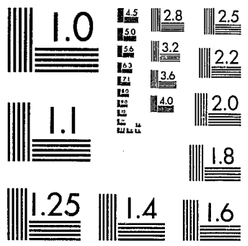
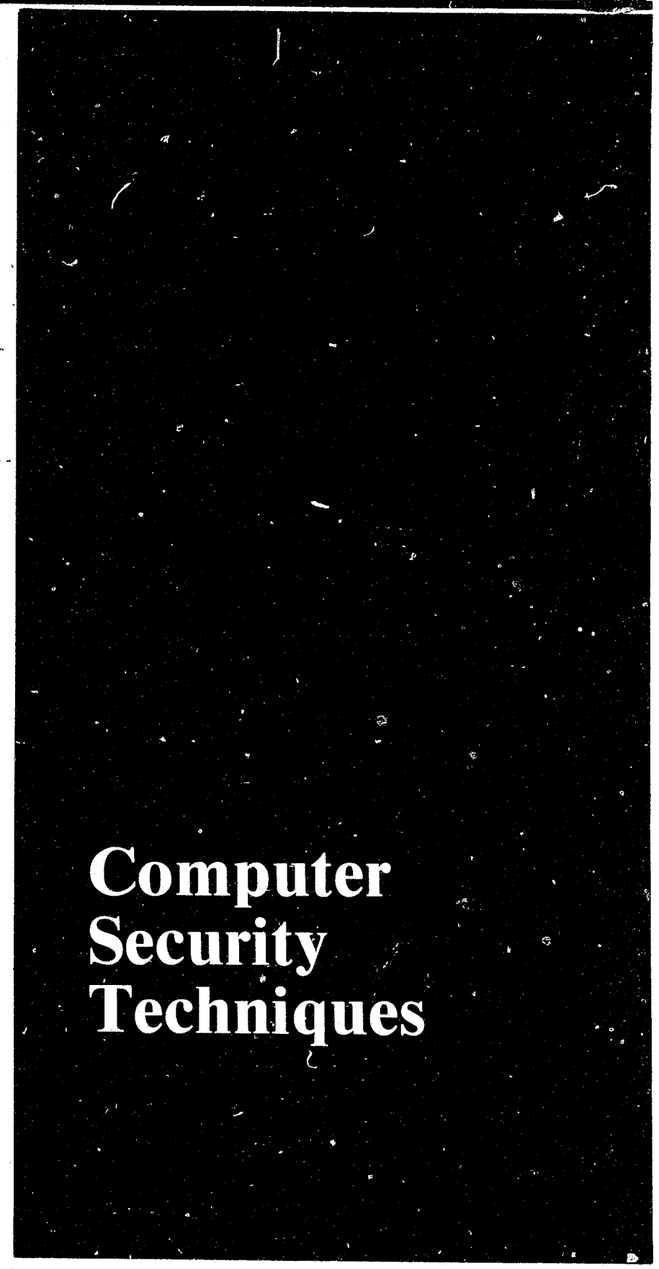


U.S. Department of Justice
Bureau of Justice Statistics

MF-1

COMPUTER CRIME



U.S. Department of Justice
Bureau of Justice Statistics

Benjamin H. Renshaw III
Acting Director

Carol G. Kaplan
Director
Division of Federal Statistics
and Information Policy

U.S. Department of Justice
Bureau of Justice Statistics

Computer Crime

Computer Security Techniques

This document was prepared for the Bureau of Justice Statistics (BJS), U.S. Department of Justice (DOJ) by SRI International under Grant No. 80-BJ-CX-0015. Points of view and opinions stated herein are those of the authors and do not necessarily represent the official position or policies of BJS, DOJ or SRI International.

Donn B. Parker of SRI International was the project leader. Other SRI project staff were Dr. Douglas Webb, Mr. Charles Cresson Wood and Mr. William Connor. Susan Nycum of Gaston Snow and Ely Bartlett conducted the legal inquiries and contributed most of the legal discussions. Dr. Rein Turn of Northridge California State University and Robert Abbott, President of EDP Audit Controls, were consultants to the project. The project was performed for the Bureau of Justice Statistics, U.S. Department of Justice, with Carol G. Kaplan acting as grant monitor.

Preface

Over the past 10 years, unprecedented advances have occurred in the development and implementation of computerized techniques for record management, information storage and data retrieval. These advances have impacted on all Americans and have made possible the performance of complex tasks which directly support the Nation's commercial activity, research and development, national defense, and fiscal operations.

Paralleling the expansion of computer activity, however, has been an increasing concern over the establishment of vast data bases which contain information identifiable to specific individuals. Concern has also arisen over the potential for criminal abuse within the computer environment. Such abuse is considered particularly threatening, both within the U.S. and the international community, in light of the possibly vast sums of money involved and the potential for disruption of international economic and security systems.

In response to these concerns major efforts have been undertaken to develop, test, and implement techniques and strategies to protect the security of computer systems and the data contained therein. Efforts have also been made to develop advanced audit techniques which are better capable of detecting and measuring computer-based crimes and security transgressions.

The Bureau of Justice Statistics, as a Federal information agency, is concerned with the development of information policies and practices which ensure the security and accuracy of data. Additionally, the Bureau of Justice Statistics, and its predecessor entity the National Criminal Justice Information and Statistics Service, has supported automation of criminal justice systems and is particularly concerned with the growing problem of computer-related criminal activity.

This document presents the result of a major review of the computer security procedures which are currently employed in the public and private sector. Over eighty techniques are described and are classified in terms of strengths, weaknesses, costs, and target vulnerabilities. The document also identifies some of the legal issues relevant to protection of computer hardware and data. It is our hope that the document will serve as a basic resource in the area of computer security and will be of value to persons involved in all aspects of computer management and operations.

Benjamin H. Renshaw III
Acting Director
Bureau of Justice Statistics

CONTENTS

EXECUTIVE SUMMARY

Indispensable to almost every form of modern business and government, the computer has become a vault for the safekeeping of electronic money, vital information, and personal data. The creation of new forms of assets and the means for processing them has given rise to the potential for misuse of computers and computer data. The security of these assets is vital. Organizations that use or provide computer services for governmental and business purposes thus have a responsibility to the users, data subjects, managers and employees, as well as society, to assure data security in legal, economic, and ethical terms to avoid loss to themselves and others. Data security encompasses the integrity, preservation, authorized use, and confidentiality of data starting with its generation, through its entry into computers, automatic and manual processing output, storage, and finally its use.

Many factors must be taken into account in planning and establishing data security. Dangers lurk not where losses have been anticipated and good controls exist, but where vulnerabilities have not been anticipated and controls are lacking. Systematic methods are needed to assure completeness of safeguarding with limited resources that can reasonably be devoted to protection in the complex and changed environments of data processing brought about by the use of computers.

Data processing and data security have advanced rapidly to the point where organizations today do not have to take safeguarding action in isolation from what other organizations are doing. Many organizations have adopted the solutions to common vulnerability problems developed by others. Applying generally used security practices and controls is attractive where the problems and needs are similar among many organizations. The 82 data security practices and controls presented in this report are the best that are used or endorsed by seven organizations that are particularly advanced in their data security, these consist of a city, a county, and state data processing service organization, a criminal justice research institute, a large insurance company, and two university data processing centers.

New approaches to reviewing, establishing the needs for, and selection of controls are emerging as concepts of data security mature. Today, the data security field is characterized by increasing top management interest and support, established specialists in the subject area, appointment of full-time computer security officers, data security products available at reasonable prices, increasing exercise of prudent care, and laws and regulations requiring security.

None of the organizations studied used a formal cost-benefit or risk analysis to evaluate data security controls. These techniques, which have been heralded in the literature, were thought to be excessively elaborate and not cost-effective. Quantified analyses were not appropriate because of a lack of valid data. Instead, each site primarily used subjective and somewhat informal piecemeal techniques for assessing the advantages and disadvantages of particular data security controls.

Most computer centers have an array of similar vulnerabili- ties consisting of common potential threats, assets subject to loss, and environments at risk, which can be addressed with generally used and accepted security controls. Special problems, however, can arise from adoption of new technology and unusual potential threats where new controls applied to new situations are needed. Moreover, some situations involve very costly controls. These special cases require detailed, quantified, vulnerability and risk assessments to justify protective action. Otherwise, generally used controls can be employed to develop a baseline of security on which specialized security for the special problems can be built to provide a consistent, comprehensive approach to data security.

The follow-the-leader strategy of employing generally used controls in data processing is motivated in part by the legal concept of standards of due care. It is becoming possible to lose more in consequential damages from a civil law action such as a stockholders' suit or citizens' suit against the government after an accidental or intentionally caused act than directly from the act itself. The legal concept of standard of due care will arise with increasing frequency in litigation over computer related loss. Data security administrators must be aware of standard of due care issues that arise and take action to conform to the outcomes through application of generally used controls.

In another area the need for protecting proprietary interests in computer programs is growing as these valuable assets proliferate. The legal counsel and data processing manager in organizations using computers should work together to understand the needs for protection of computer programs, including the value of patents, copyrights, trade secrets, trademarks, and contracts. At present, often the best alternative is to copyright computer programs and then to license or disclose the computer program using agreements that restrict use, transfer, and disclosure. This approach should not conflict with existing copyright law theory, and it achieves the same secrecy afforded by trade secret protection.

The data processing manager should understand the legal alternatives for protecting computer programs and adopt prudent controls used by others under similar circumstances. If the organization uses computer programs developed and owned by outside parties, this understanding and use of controls can prevent legal problems and can ensure that the

terms of the agreement for using the computer programs are proper. For organizations that develop computer programs in-house, a corporate policy based on a thorough knowledge of the laws is a basic control that can prevent misunderstandings between management and development personnel.

Data security reviews to identify and evaluate vulnerabilities, calculate risks, and select controls have been conducted assuming differences and uniqueness from one computer center to another because of their one-of-a-kind development. Differences in physical facilities, computer configurations, types or modes of computer usage, organization patterns, and computer application environmental factors have all been emphasized. However, similarities in the use and security of computers are appearing in many areas such as physical access control, fire prevention and protection of computer program ownership.

A new concept of baselines of security controls can be developed from these and many other similar environments and vulnerabilities. A baseline of security controls is a set of generally used controls meeting commonly desired control objectives that should be present in every well-run computer center. The justification for having them is derived from common usage and prudent management rather than from explicit identification of vulnerabilities and reduction of risk.

A control is the policy, method, practice, device, or programmed mechanism to accomplish a control objective. A control has implementation variants that are established in the detailed specifications for the control in a particular use. Baseline controls have never before been identified, and it is not known how many would qualify universally or within any specific organization. However, the baseline concept is now feasible because of the control selection experience gained as the data security field matures. The 82 controls found in the study of seven computer field sites are a preliminary step in identifying baseline controls.

A baseline of security need not be a rigid, unalterable set of control objectives and their required controls and variants. The purpose of a baseline is to specify a minimum set of controls such that if a control is omitted, there would be explicit reasons identified why it is absent or why an alternative control is equivalent. If these exceptions from a baseline are acceptable to the authority ultimately responsible for security, the baseline could still be said to be the accepted criterion. In fact, this exception-taking is the process by which baselines evolve. When enough support for an exception exists, a baseline is changed to include the exception as part of the baseline.

The success of the baseline concept lies in obtaining concurrence and acceptance of a sufficient number of generally used controls by computer security administrators and, in turn, by the management responsible

for the expenditure of resources for data security. Certainly enough controls are now identified in extensive security literature and exist as commercial products. Management must be willing to accept a recommended control justified only by having a security administrator show that it is part of a baseline. Prudent management will be motivated to do this out of trust in the security administrator, the prospect of saving time, the reduction of expenses for evaluation and study, and the contentment of knowing that the organization is protected by generally used controls.

Baseline security will allow organizations to reduce unnecessary expenditures for detailed study of already resolved problems and selection of solutions by extensive justification efforts, data gathering, and analysis. It will facilitate the comprehensive use of simple, inexpensive, effective safeguards before difficult, new problems are attacked. As computer-using organizations adopt the baseline approach for selection of controls, they will increasingly rely on the best security controls used most successfully by other organizations. This practice will further advance the baseline concept by encouraging uniformly high quality security and will stimulate and facilitate a formalized theory of computer security, putting it on a par with other theories in computer technology. The training of computer security specialists will likewise be formalized and advanced. In addition, identification of generally used controls and their variants will stablize and enlarge the security products market to stimulate a wider range of less expensive control products that require fewer model types and options.

It is hoped that baseline concepts will not be seen as alternatives to quantitative and qualitative risk assessment methods now in use. Baseline controls would be selected before such assessments take place so that the obvious, accepted, routine controls could be applied before risk assessments are used. Therefore, assessments can be started further along in the controls selection process.

The development and identification of baseline controls can be advanced by considering the 82 controls that were identified at the seven field sites where they were agreed to be desirable in most computer installations. The best controls were identified, documented, and grouped within control objective categories based on several similarities. Control objectives included prevention of modification, disclosure, or unauthorized use of obsolete or incomplete input/output data, prevention of disclosure or unauthorized use of personal information, prevention of unauthorized access to sensitive areas, detection of unauthorized activities of employees, and avoidance of violations of laws and regulations.

Five indices provide a computer security practitioner with a simple and easy means of locating all controls under a variety of types of headings: security topic, control objective, area of responsibility, mode (type) of implementation or execution, and area of control environment. In the first index, seven security topic areas for categorizing the 82 controls were identified. Each area includes 8 to 21 controls. These topic areas and some of the more significant controls are summarized below.

- Manual Assurance of Data Integrity

  Data security extends to the manual handling of data before entry into computers and after computer processing. Data and the programs that process the data must be explicitly assigned to the care of the owners, custodians, and users. Each party must be held accountable for their integrity and safekeeping through confirmation of receipt, inspection at each manual handling step, use of printed proprietary notices on documents, and proper archiving or destruction of used documents. Data representing personal information requires great care to protect privacy, including review of types of human subject data for appropriateness, need, completeness, and timeliness.

- Physical Security

  Physical security involves the buildings that house computer centers, as well as the remote computer terminals. Within the established security perimeters, access to work areas must be restricted with physical barriers, appropriate placement of equipment and supplies, and universal wearing of identification badges. Emergencies must be prepared for, alternative power sources provided in many cases to assure uninterrupted processing, and incoming and outgoing materials inspected. Access to loading areas requires special precautions.

- Operations Security

  Operation of computers requires many controls. Isolation of sensitive computer production jobs to minimize exposure to modification, destruction, exposure, or unauthorized use especially separating production and testing activities, is essential. Computer system trouble logs and activity records must be kept and used. Magnetic tapes and disks and output documents must be appropriately identified, and copies must be made and kept safe for backup. Contingency and recovery plans must be prepared and tested. Employee identification on work products and other practices to assure worker trustworthiness must be carried out.

- Management Initiated Controls

  Security requires direction and support from top management to assure adequate protection; for example, sensitive duties among employees should be appropriately separated. A data security management committee to review and approve new controls is essential. The important functions of EDP auditor and computer security officer should be established and staffed. Proper funding for security and especially for contingencies and recovery are needed. Data should be classified for properly distinguishing degrees of control. The reports and documentation dealing with security are particularly sensitive and must be held at the highest level of protection.

- Computer Program Development and Maintenance

  Computer programs must contain adequate controls; responsibility for the controls and program changes must be assigned to assure compliance with laws and regulations as well as overall quality. This also requires participation by computer users and EDP auditors at critical times during program development. Access to computer programs must also be closely controlled.

- Computer System Control

  Controls in the computer operating programs and other major program subsystems used in many applications are essential. Outside vendor supplied programs and changes to them require special care. Data bases of personal information must conform to privacy constraints. Input data validation, exception reporting, and possible use of cryptographic protection using secret keys are important controls that can be provided by the system for many applications.

- Computer System Terminal Access Controls

  Access to computers from remote terminals changes the nature and extent of potential losses, especially when dial-up access from any telephone is possible. Transaction privileges, output display restrictions, terminal identifiers, log-in protocols and password access by authorized users are essential. Data file access controls and logging such activities are also important. Finally it is essential to have a terminal user's agreement document to assign accountability properly.

The indexing procedure and the 82 controls described in this document are meant to add materially to new concepts in data security that take advantage of commonly used solutions to common problems without elaborate justification, thus conserving limited security resources to deal with the new and costly controls necessary as new potential threats, vulnerabilities, forms of assets, and technology emerge.

SECTION I INTRODUCTION

The "Dawn of the Age of Aquarius" has also ushered in the "Age of the Computer." It is no secret that computers have become indispensable to almost every form of modern business and government. The rapid expansion of computer use has created an electronic marketplace where goods and intellectual products are transferred and paid for entirely by electronic means. Computers have also created a new method of storage and representation of assets through electronic data processing systems that record everything from bank balances to shares of securities. The use of computers has even advanced to the stage where electronic signatures can be given unique characteristics making them more easily identifiable and reliable than human handwriting in many respects.

The new form of assets consists of pulses of electricity, states of electronic circuits, and patterns of magnetic areas on tape and disks. The pulses can be converted to the form of checks by a computer printer or to monetary currency by computer-printed reports that authorize cashiers to transfer cash from boxes to people or to other boxes. The pulses can also be converted to printed reports or mechanical functions that cause actions either manually or automatically involving goods and services. These negotiable assets, as well as personal information, now are stored as data in computers, saved on magnetic tape and disks, and sent through wires and microwave carriers in electronic, electromagnetic wave, and magnetic forms.

The creation of these new forms of assets, however, has been accompanied by an increase in the potential for misuse of computers and computer data. Some of the people who create and work with computer products have the capability to alter or delete assets stored in computers or to create totally new assets. The security of these assets, as well as other data stored in computers, is vital. In this document, computer security encompasses the integrity, preservation, authorized use, and confidentiality of data starting with its generation, through its entry into computers, automatic and manual processing, output, storage, and finally its use.

One of the primary motives for computer security is protection from intentionally caused loss. Computer crime is highly publicized and its nature frequently distorted in the news media. Although there are no valid representative statistics on frequency or loss, enough loss experience has been documented (more than 1000 reported cases since 1958) and even more conjectured to make it clear that computer crime is a growing and serious problem. Broadly defined, known experience indicates a high incidence of false data entry during manual data handling before computer entry. Most losses of this kind are small, but several large losses of

$10 to $20 million have occurred. Unauthorized use of computer services has also proliferated, especially with increasing use of dial-up telephone access to computers. A few sophisticated programmed frauds inside computer systems or using them as tools for frauds have been found where detection was mostly accidental. Reported computer crime is committed mostly by people in positions of trust with special skills, knowledge and access. The results of known experience indicate the need for a wide range of basic controls that reduce the likelihood of violation of trust by these people. Many of these controls are represented in this report.

Reliance on Computers Requires Computer Security

Although computer security has always been needed, even before computers, interest in it became widespread only after computers came into use, especially for processing financial and personal data. Computers facilitate the great concentration of data for powerful means of processing, and for the first time since the days of manual data processing computers provide an opportunity to apply computer security in effective, uniform, and low-cost ways. At the same time computer use increases the dangers of large losses from the concentration of intangible assets in electronic forms and changes the nature of exposures to losses with assets in these new forms.

Use of computers changes the patterns and degree of trust put in people who work with data. New occupations staffed by fewer, technology-oriented people, each with greater capacity to do good or harm using computers as tools have emerged. There is now one computer terminal for every three white-collar workers.

Computers remove processing and storing of data in their electronic form from direct human observation. Thus, computer programs that direct the processing of data whose integrity and correctness must be assured are necessary tools to see the results of data processing and check the correctness of data stored in computer media. The procedures by which data are processed and stored are created by programmers at a different time and place than when the actual processing occurs. Processing takes place so rapidly as to be incomprehensible to humans until it is complete, and intervention is impossible except in preprogrammed ways that were developed without the possibility of foreseeing all future conditions and needs.

Organizations that use or provide computer services for governmental and business purposes have a responsibility to the users, data subjects, managers and employees, as well as society, to assure computer security in legal, economic, and ethical terms to avoid loss to themselves and others. Thus, contractual commitments that specify trade secret protection of commercial computer program and data file products require that users of the products apply safeguards. Top management, of course, wants to continue the success of their organizations and avoid data-related losses. Data processing employees abide by the computer security

policies and procedures to please management and receive advancements in their jobs. Society demands responsible treatment of data; the U.S. government, for example, has attempted to obtain voluntary adherence by business to the Organization for Economic Cooperation and Development Guidelines on Protection of Privacy and Transborder Flows of Personal Data. In addition, professional societies and trade associations apply peer pressure to meet ethical standards.

Data-related losses from errors, omissions, bad judgment, intentional acts, and natural events motivate the victims to avoid further loss. Some controls on loss result in more efficient data handling, reduced insurance premiums, and lower costs. Compliance with laws and regulation such as the Privacy Act of 1974, Foreign Corrupt Practices Act, criminal statutes, and the U.S. Office of Management and Budget Circular A-71 on Computer Security is required for an orderly society.

All of these factors and more must be taken into account in planning and establishing computer security. Dangers lurk not where losses have been anticipated and good controls exist but where vulnerabilities have not been anticipated and controls are lacking. Systematic methods are needed to assure completeness of safeguarding with limited resources that can reasonably be devoted to protection in the complex and changed environments of data processing brought about by the use of computers.

Commitment to Computer Security

Management is eager to allocate resources that directly increase the productivity of their organizations. Security seldom adds directly to productivity; it only assures protection from loss of productivity and avoids violation of rights, laws and regulations. Therefore, security is only productive in the relatively rare cases when losses might have occurred. If security is effective, it usually goes unnoticed because loss is averted. Otherwise, security is sometimes seen as costing money without visible, direct contributions to performance. This makes security expenditures particularly important to justify and understand.

Fortunately, enlightened management will react rationally to assure security in their organizations when given reasonable options and adequate justification for doing so. Employees will support and carry out security when they understand its purpose, receive clear directives, understand that it is part of their job performance, and are judged on their adherence to secure practices. Therefore, recommendations for cost-effective controls must be properly justified and generally accepted.

Methods for conducting security reviews based on risk assessment to determine vulnerabilities and identify needed controls have been developed and used to some extent. However, many controls are still selected on a piecemeal basis when individual needs become evident without comprehensive review of all needs. This leads to inconsistent security

buildup that leaves serious vulnerabilities and gaps. Security must be measured by the weakest links; losses occur where adequate controls are lacking. Therefore, methods of review must be developed that are comprehensive as well as sufficiently practical and low in cost to attract their use.

Data processing and computer security have advanced rapidly to the point where organizations today do not have to take action in isolation from what other organizations are doing. Many organizations have adopted the solutions to common vulnerability problems developed by others. Applying generally used security practices and controls is attractive where the problems and needs are similar among many organizations.

Contribution of This Report to Computer Security

The study results reported in this document are meant to add materially to new concepts in computer security. The computer security practices and controls presented here are those used or endorsed by seven organizations that are particularly advanced in their computer security. In addition, the organizations were chosen from among those heavily involved in manipulating personal data to emphasize the application of security to issues of privacy. Thus, several of the organizations are processors of criminal justice data and one is a processor of life and medical insurance. The seven participating field site organizations are:

(1) A state law enforcement data center

(2) A county EDP services department

(3) A city data services bureau

(4) A research institute specializing in criminal justice research

(5) A life and casualty insurance company

(6) A center for political studies, which does extensive research on sensitive topics linked to individuals

(7) A state information services department.

A project team of experienced computer security consultants examined the seven field site organizations to determine the best controls and practices in use, as well as the methods of review and selection of controls and practices that organizations use. This document describes the 82 controls and practices that were judged as generally acceptable for good computer security by computer security administrators from all seven organizations along with two independent security consultants.

In Section II of this report, the background and maturation of computer security methods, particularly as a basis for new approaches to evaluating and selecting controls, are described. Common, selective, and special vulnerabilities are identified. Section III describes presently used security review methods and the legal concepts of standards of due care and protecting proprietary interests in computer programs which contribute to computer security practices and the law.

Section IV, along with more detailed descriptions in Appendix B, presents a new, baseline concept that can be used along with other methods for selecting controls and security practices. The principles and benefits of baseline controls are stated and future baseline development is considered.

Section V explains the method of investigation, the format used to describe the controls found in the study, and the five indices of the 82 controls that are described in the last section. The five indices are identified by topic, objective, area of responsibility, mode, and environment to facilitate location of specific controls. An overview summarizing the controls by topic completes Section V.

In Section VI, the controls are presented in ways quite different from that found in other security literature. A title, control objective, and general description based on actual usage experience are presented. The control variants are identified. Strengths and weaknesses found in usage are stated. These items are followed by advice on how to audit the controls, and five more characteristics are briefly identified to complete the description. Appendix A presents three case studies of actual selection and approval of controls and a step-by-step method of how a baseline review could be conducted.

SECTION II BACKGROUND

Computer Security Beginnings

Although computer security has been an important requirement in the military since computer use began, it has been only explicitly recognized in nonmilitary government and business since the late 1960s. The 1967 American Federation of Information Processing Societies, Spring Joint Computer Conference session, "Security and Privacy in Computer Systems" chaired by Dr. Willis Ware of the Rand Corporation, generated new interest in computer security. Rapid development, stimulated by the privacy issues and notorious computer crimes in the 1970s, has followed. Formalized methods for evaluating the adequacy of security soon followed.

On July 27, 1978, the U.S. Office of Management and Budget issued to all agency heads the Transmittal Memorandum No. 1 under Circular No. A-71 on Security of Federal Automated Information Systems. This memorandum presents a comprehensive policy regarding establishment of computer security programs in all nondefense computer centers. It contains a procedure for adopting security standards, a requirement for security in all hardware and software procurements, plus guidance on conducting risk analyses, performing security audits, developing contingency plans, and establishing personnel security policies. Various roles for the National Bureau of Standards, General Services Administration, and Civil Service Commission are specified. This memorandum, a significant milestone for computer security in the federal government, is a well-conceived document worthy of general use.

Maturing Computer Security

New approaches to reviewing, establishing the needs for, and selecting computer security controls are emerging as concepts of computer security mature. Maturation is evident from the routine acceptance of security and from the type of controls typically used today at the seven sites visited. At present, the computer security field is characterized by:

- General management recognition and support.

  Top management at the sites were interested enough in computer security to fully cooperate with the project field teams. Corporate and agency policies reflecting top management's concern have been formulated.

- Established specialists in the subject area.

  Full-time security researchers and designers in computer science and technology are developing concepts of trusted computer systems that will be significantly more secure than current computers. Many consultants are active in the field. Computer security job titles and positions have been developed, and hiring by these titles is practiced.

- Appointment of full-time or part-time computer security officers in large, well-run computer installations.

  The larger organizations visited had full-time or part-time computer security officers. National conferences on computer and computer security and privacy are currently drawing 700 to 800 computer security-related specialists and administrators.

- Computer security products available at reasonable prices.

  Physical access control systems for computer centers, password access terminal systems, file access control computer programs, fire detection and suppression equipment, cryptographic systems, audit program tools and uninterruptible power supplies for continuous operation of computers are examples of reasonably priced products (see also Section VI). In addition, the products' salesmen provide a new source of information and assistance for security practitioners.

- A precedent-setting federal standard for cryptographic protection.

  The first federal information processing standard, the Data Encryption Standard, was approved by the National Bureau of Standards and is used in more than 25 products.

- Increasing numbers of effective controls found in well-run computer installations and well-designed systems.

  Section VI identifies 82 generally used controls based on field investigation of the seven computer sites.

- Practice of formal security review methods.

  Task group reviews of computer centers are becoming more common. The U.S. Office of Management and Budget requires that risk assessments be performed in all federal agency computer centers at least once every 3 years. The National Bureau of Standards has published several reports on conducting risk assessments.

- A body of information documenting loss experience.

  Conference proceedings, books, and trade journals include detailed descriptions of loss cases. Mr. Donn B. Parker at SRI International, Professor Brandt Allen at the University of Virginia, The American Institute of Certified Public Accountants, Mr. Robert Courtney in New York, and Mr. Jay Bloombecker in Los Angeles have extensive files of reported computer abuse and crime cases.

- Laws and regulations requiring security.

  The Federal and State Privacy Acts, Foreign Corrupt Practices Act, 16 state computer crime statutes, and numerous regulations require or directly imply the need for controls.

- Special insurance policies.

  Numerous insurance companies offer policies for protection against data processing business interruption, errors and omissions, and crime.

- Numerous books, journals, news publications, and other writings on the subject.

  The National Bureau of Standards has published more than 40 computer security reports. The Bureau of Justice Statistics, Department of Justice, has published a series of manuals and guides on privacy and security. At least four monthly commercial newsletters and journals, as well as many books on computer security, are published.

- Specialized audit capabilities.

  The Institute of Internal Auditors published the SRI International Systems Auditability and Control Reports identifying 30 audit techniques and more than 300 controls. EDP auditing has become an accepted specialty in audit, and EDP auditors are certified by the Institute of Internal Auditors and soon also by the EDP Auditors Association.

Vulnerabilities

Admittedly, some potential threats and assets subject to loss are different from one computer center to another depending on organizational characteristics and purposes. Some vulnerabilities of a U.S. Department of Justice computer center will be different than a toy manufacturer's computer center. However, similar problems among even diverse kinds of computer centers can lead to adoption of commonly used controls. The potential threats, the assets at risk, and the vulnerable facilities that are similar among all computer centers include:

- Potential Threats

  - Disgruntled or error-prone employees causing physical destruction and destruction or modification of programs or data.
  - Natural disaster such as fire, flooding, and loss of power and communications.
  - Outsiders or employees making unauthorized use of computer services.
  - Outsiders or employees taking computer programs, data, equipment or supplies.

- Assets Subject to Loss

  - Facilities
  - Systems equipment
  - People
  - Computer programs
  - Data
  - Data storage media
  - Supplies
  - Services
  - Documents
  - Records
  - Public respect and reputation.

- Common Environments at Risk

  - Computer rooms containing computers and peripheral equipment
  - Magnetic media (tapes and disks) libraries
  - Job setup and output distribution stations
  - Data entry capabilities
  - Program libraries
  - Program development offices
  - Utility rooms
  - Reception areas
  - Communications switching panels
  - Fire detection and suppression equipment
  - Backup storage
  - Logs, records, journals.

In addition to the vulnerabilities common to all computer centers, some types of computer centers such as criminal justice operations, research institutes, insurance companies, and banks have environments, applications, and types of data that create similar potential threats and types of asset loss. The vulnerabilities endemic to subsets of similar computer centers lead to the need for selective controls such as separation or deletion of names from personal data, batch check summing of inventory data and possibly data encryption. Some examples of computer applications and associated risks that are not common to all computer centers are as follows:

- Processing and storage of personal data

  - Intentional or accidental disclosure, modification, destruction or use of personal data or records of their use.
  - Violation of confidentiality rules, personal data regulations, or privacy laws.

- Processing and storage of secret data (e.g., investigative, intelligence, trade secret, marketing, competitive).

  - Intentional or accidental disclosure, modification, destruction, or use of trade secret or sensitive data or records.
  - Violation of rules, regulations, or laws.

- Processing and storage of financial data (e.g., account balances, negotiable instruments input/output, general ledger, accounts payable/receivable, payroll).

  - Financial fraud or theft.
  - Accidental financial loss such as lost interest.
  - Failure to meet financial report filing dates and other fiduciary obligations.

- Process control (e.g., controlling manufacturing processes, transportation, meal processing, inventory control, patient monitoring).

  - Intentional or accidental modification, failure, or destruction of processes.

In addition, special or unique problems can arise in a single computer center where new technology is adopted and commonly used controls have not yet emerged. Examples of the new technology include voice data entry, voice output, fiber optics communication, satellite data communications, and automated offices.

Lastly, several potential sources of unusual threats requiring special controls have been identified: a computer center built over a burning underground coal mine, violent labor strife, a computer center in an airport glide path, rodent or insect infestation, and contract programming performed by prison inmates.

Current Security Review and Control Selection Practices

The process of identifying security needs and selecting and justifying controls is called a security review when carried out in an organized set of scheduled and budgeted tasks. It is sometimes incorrectly called an audit. An audit implies independent review by auditors for top management and owners of an enterprise to discover problems and lack of compliance with law, regulations, and policy.

The security review method described below is based on identification of assets, potential threats, and lack of controls. A zero-based method, it begins by assuming that potential threats and controls have not been adequately addressed previously. Its purpose is to comprehensively and exhaustively identify problems in the form of specific vulnerabilities, their risk, and compensating controls. This approach is thoroughly justified; losses tend to occur where effective controls are absent.

The control selection methods as they are currently practiced are also described below. The commonly recommended approach has been combined with techniques in actual practice to provide a new security review and control selection methodology (see Appendix B). Although this new baseline review and selection method has not been fully tested, it is readily usable; it employs the most successful practices found among the seven field sites in the study, as well as components of other recommended methods.

A Commonly Recommended Review Method

The usual method of security review often described in the literature and in seminars includes combinations and various orderings of the following steps:

(1) Organize a task group to conduct the review; establish plans, assignments, schedules, budgets, and scope; obtain management approval and support of the plan.

(2) Identify the assets subject to loss; either determine their value, consequences of loss, and replacement value or rank their importance.

(3) Identify potential threats to the identified assets.

(4) Identify the controls in place or lack of controls that mitigate or facilitate the potential threats to the assets.

(5) Combine associated potential threats, assets subject to loss, and lack of mitigating controls; each triple of items constitutes a vulnerability.

(6) Evaluate and rank the vulnerabilities in terms of greatest to least expected potential loss; alternatively quantify risk for all or only the major vulnerabilities in terms of annual frequency of loss and single case loss in dollars to obtain annualized loss exposure.

(7) Identify actions and controls that would reduce the risks of losses to acceptably low levels.

(8) Recommend an implementation plan to reduce risk to an overall acceptably low level.

(9) Carry out the plan and establish ongoing security maintenance and improvements.

Several steps may be combined or overlapped for task group operating efficiency. Various methods such as use of questionnaires and loss and frequency data forms or scenarios can aid in accomplishing the tasks and documenting the results. Some steps may involve a high volume of data to warrant use of computer-aided methods. For example, quantified risk assessment requires expected frequency of loss and dollar value of single incident loss from both intentional and accidental modification, destruction, disclosure, use and denial of use (for various periods of time) for all computer-related threats and assets.

In practice, however, this formalized review approach is rarely taken, or only severely limited versions are adopted. More likely, only piecemeal discoveries of vulnerabilities and their solutions happen. These events are occasioned by other information processing activities such as audits, loss events, new applications, new or newly enforced requirements, contracting, or budget studies. If a specific study is conducted, often obvious, significant vulnerabilities are identified early and actions taken to reduce their risk even before the final recommendations are made.

Security Methods in Practice

A survey of management practices was conducted at the seven field sites. Managers were asked to describe the process currently used to select, justify, and install computer security controls. Both methodology and organizational factors were studied. Three typical case studies for a government agency, a research organization, and a private sector firm are included in Appendix A.

None of the organizations studied used a formal cost-benefit or risk analysis to evaluate computer security controls. These techniques, which have been heralded in the literature, were thought to be excessively elaborate and not cost-effective. Quantitative analyses were considered not appropriate because of a lack of valid data. Instead, each site primarily used subjective and somewhat informal piecemeal techniques for assessing the pros and cons of particular computer security controls.

These subjective techniques can be described as the exercise of prudent care or subscribing to generally used controls. The words "prudence" and "common sense" were frequently used in describing what went into these subjective assessment approaches. Generally used approaches were defined in terms of the practices of other organizations in similar environments. Management essentially asked, "If another manager were in my place, would he install and operate the proposed control?" Factors considered in answering this question include:

- The controls actually being used by other organizations with similar applications and equipment.
- Reported loss experience.
- The perceived needs of the organization's own operating environment compared to other organizations with similar environments.
- The increased level of security to be achieved
- Laws and regulations.

Definitions of generally used controls typically consider a wide-ranging control environment. Policies and professional ethical mores, personnel procedures, and manual procedures can be used to make up for the possible lack of computer-based controls, especially in computer systems where security has not been a design and implementation criterion.

Another important factor in the decision to use a particular control was the influence of outside parties. Clients served by the organizations specified requirements that had to be met before certain work could be performed and data could be obtained. These requirements mirrored requirements that in some instances came from within the organization. External and internal auditors were other sources of relevant information. Quantitative information such as the cost to install and operate a control, money to be saved, or the losses to be prevented (from catastrophes, lawsuits, or public embarrassment) were rarely considered.

Management in most cases did not actively seek information about what is done elsewhere. Although they used this information when made available to them and found it to be of great interest and potentially useful, they did not believe that contacting similar organizations and asking questions were cost-effective. The exception to this occurred when very costly controls, such as vaults or electronic lock access systems, were considered. Management then directed technical personnel to study alternative products and survey users of the products. Sometimes prioritized lists of desirable controls were prepared as wish lists that could be reviewed whenever budgets were prepared. The lists were helpful in matching high-priority controls with limited resources. Controls were viewed as necessary resource-consuming items rather than revenue generating or cost-saving items. The time frame was typically 3 to 5 years.

The source of the funds to be used for a control largely dictated the approval process; if funds were to come from a government grant, from organizational overhead, or from a client project, then the approval channels were markedly different in each case. The approval process also varied depending on the time of year when the need for a control was

noticed. If a need was perceived shortly before budgets were prepared, and installation could be delayed until the next fiscal year, then it was included in the budget. If installation of a control could not be delayed until the next fiscal year, special procedures were required to rearrange currently budgeted funds to obtain additional funds.

Documentation of the decision process was often sparce. Purchase requisitions and budgets on the proposed control were sometimes the only formal documents produced. Explicit management approval in these cases was given when these forms were approved. Larger organizations were more likely to require formal documentation that included proposals, signoff sheets, memos, impact statements, and in rare instances cost-benefit analyses. Systems development and modification methodologies in some cases included requirements for considering computer security. Security was reviewed when a system was designed, redesigned, or modified, but not otherwise. The concern for security was not dealt with in isolation from other activities. Typically, a control that was retrofitted to an existing system was evaluated in the same manner as a control that was originally designed into a system. Both were subject to the system development and modification methodology.

Documentation of control decisions and the resulting changes to be made were more extensive whenever a control was going to affect people outside the organization. One organization wrote and maintained a specialized secure operating system; another developed and installed a security program package. For these products, strict requirements for system change justification and documentation existed.

Decision-Making Factors

Typically, the decision to adopt a control was made by the line managers from the area primarily involved; for example, if an electronic lock access system would restrict the activities of computer operators, then computer operations management would make the decision.

In some instances, security committees that had an advisory role in the decision to adopt computer security controls were formed. These committees were composed of higher level managers who represented the following organizational areas: the legal department, user organizations, applications development, computer operations, and industrial security. These committees monitored legal and regulatory requirements, current events, and the current security systems. In rare cases, the committee had approval authority.

When a proposed control affected several parts of the organization in a significant monetary or operational way, then management approval of each of these areas was usually obtained. Approval by industrial security, legal counsel, audit, personnel, users, as well as other departments of a computer center besides the one proposing a control was thus sometimes required. For example, if a control would increase the

rates for computing services charged to users, or if it would change the user's interaction with a computer system, then the users would typically be involved in the decision process. Occasionally, if many areas were involved, then a higher level manager who had each of these areas reporting to him decided whether to adopt a proposed control.

The computer service provider may play different roles in the identification and approval of the need for a control. The service provider in some cases was responsible for telling the user what was needed, while in other organizations the user was responsible for telling the service provider what was required. In either case, expertise within the computer service provider's organization was relied on. In some organizations, other departments such as audit and legal counsel were supposed to alert involved parties to the need for additional controls, but the approval of the changes still rested with the service provider and the user.

Audit departments were seldom involved in the control requirements and specification process. Although many authors of computer security works advocate that auditors be involved in systems design work, this participation did not generally occur. Some say that this system is adequate--auditors are not supposed to directly participate, which specification of controls would imply. Auditors were said to only infrequently review computer controls. Others state that auditors should be more active in the review of controls, informing management of the need for improvements. Larger organizations were more likely to have auditing staff involved in these activities.

Many installations have noted that finding security experts in the computer field to hire is a problem. In some cases controls were not evaluated or implemented because of the lack of qualified personnel. The shortage of experts in the computer security field is particularly acute.

Evidence of the maturing of computer security and the findings from experience about selection of controls provide the background to consider the motivation and need for adopting generally used controls. The next section provides two specific examples of common sources of this motivation and need and how they may be satisfied by generally used controls.

This section has described the increased recognition of the need for security controls and the maturation and status of the process of control selection. A major factor relevant to decision making regarding computer security is the legal framework surrounding data and related computer violations and liabilities. These issues are addressed in the next section.

SECTION III COMPUTER SECURITY CONTROLS AND THE LAW

Standards of Due Care

The follow-the-leader strategy of employing generally used controls in data processing is motivated in part by the legal concept of standards of due care. It is becoming possible to lose more in damages from a civil action such as a stockholders' suit or citizens' suit against the government after an accidental or intentionally caused act than directly from the act itself. Liability for the violation by a provider of computer services towards any other (customer, data subject, affected third party, stockholder) can arise through a conscious act of malice with intent to cause harm, through reckless disregard of the consequences to the person harmed or through negligent performance or failure to perform. For such liability to attach, a duty of care must be owed to the victim of the act. Once responsibility is established, the provider having the responsibility is required to act as a prudent person.

The actions of another person in the same position or the general practice of the computer services industry are useful in establishing the standard of care against which individual performance will be measured. However, industry practice is not a complete answer. In the T. J. Hooper case, which concerned the failure of a large tug boat operator to use radio receivers in 1932 to avoid inclement weather, Judge Learned Hand stated:

> Is it then a final answer that the business had not yet adopted receiving sets? There are, no doubt, cases where courts seem to make the general practice of the calling (industry) the standard of proper diligence;... Indeed in most cases reasonable prudence is in fact common prudence, but strictly it is never its measure; a whole calling (industry) may have unduly lagged in the adoption of new and available devices. It (the industry) may never set its own tests, however persuasive be its usages. Courts must in the end say what is required; there are precautions so imperative that even their universal regard will not excuse their omission...(60 F.2d. 737,730) (2nd Cir. 1932, Cert, denied 287 U.S. 662 (1932).

No definitive answer or test can establish a standard of due care on grounds of common practice in an industry or on prudence based on use of available devices whether generally adopted or not. In 1955, the Circuit Court of Appeals for the Sixth Circuit held that the failure to use radar by an aircraft in 1948 was excusable because no commercially feasible aircraft radar system was available (Northwest Airlines v. Glenn L. Martin Co. 224, F.2d 120, 129-130). In 1977, the U.S. District Court

for the Southern District for New York held an airline liable for a robbery for failure to take appropriate precautions, despite the provision of an armed guard in front of the locked unmarked storage area and the argument that the airline had taken the same degree of precautions that other airlines had. (Manufacturers Hanover Trust Co. v. Alitalia Airlines, 429 F.Supp. 964(1977)). Further, professionals may not always rely on generally accepted practices. In U.S. v. Simon (425 F. 2d. 796 [2nd Cir. 1969]) the United States Court of Appeals for the Second Circuit held that, even in a criminal case, generally accepted accounting principles were not necessarily the measure of accountants' liability for allegedly misleading statements in a footnote to the financial statements.

The concept of standard of due care will arise with increasing frequency as disputes over computer-related loss end in litigation. Computer security administrators must be aware of standard of due care issues that arise and take action to conform to the outcome.

Applying Legal Concepts to Computer Services

One area where the courts have had some difficulty in applying legal concepts to computers is in determining exactly how to characterize computer services from a legal point of view. The courts have generally held that basic legal principles requiring a person to exercise reasonable care do not change simply because a computer is involved. The courts have generally stated that those who use computers must do so with care, and they have not been sympathetic to defenses asserting good faith mistakes resulting from reliance on faulty computer data. In Ford Motor Credit Co. v. Swarens (447 S.W. 2d. 53 [Ky. 1964]), for example, a finance company wrongfully repossessed the plaintiff's car after he had proven on two occasions that he was current in his payments by showing cancelled checks to agents of the defendant. The finance company defended on the basis that an admitted error with respect to the plaintiff's account had occurred as a result of a com- puter error. The court rejected this defense stating:

> Ford explains that this whole incident occurred because of a mistake by a computer. Men feed data to a computer and men interpret the answer the computer spews forth. In this computerized age, the law must require that men in the use of computerized data regard those with whom they are dealing as more important than a perforation on a card. Trust in the infallibility of a computer is hardly a defense, when the opportunity to avoid the error is as apparent and repeated as was here presented.

It is clear, therefore, that excessive reliance on computer data without proper safeguards to ensure the reliability and accuracy of the information may constitute the failure to exercise due care, and in some cases may even result in the award of punitive damages.

Professional Standard of Care

There is clearly a duty to exercise reasonable care in using computers. Depending on the legal characterization given to contracts to supply computer equipment and services, a higher standard of care may be required of suppliers of computer services. Such an argument would be based on the theory that programmers and others who provide computer services hold themselves out as professionals with special expertise. As such professionals, they arguably should be held to the level of care that would be exercised by a reasonable member of the profession under similar circumstances.

In Triangle Underwriters v. Honeywell, Inc. (604 F. 2d. 737 [2nd Cir. 1979]) for example, the court found that Honeywell agreed to deliver a completed computer system to Triangle and not to run a continuous data processing service. Triangle tried to argue not only that Honeywell had been negligent in failing to design and deliver a workable system, but also that the wrong continued during the period in which Honeywell employees attempted to repair the malfunctioning system. Triangle argued that Honeywell had engaged in professional malpractice, and that the continuous treatment theory should apply so that the statute of limitations would not commence to run until the professional relationship had ended. The district court noted that the continuous treatment theory had been applied by New York courts to nonmedical professionals such as lawyers, accountants, and architects, but it declined to apply the theory to Honeywell. "In the case at bar ... the necessary continuing professional relationship did not exist. Honeywell was not responsible for the continuous running of a data processing system for Triangle."

Although the court thus refused to accept the plaintiff's theory of professional malpractice on the facts of that case, the decision leaves open the possibility that the doctrine might be applied in a future case to persons who provide computer services for a client on an ongoing basis.

Strict Liability

There is a further issue of whether those who provide computer services should be strictly liable in tort for injury to others due to malfunctions of the equipment. The doctrine of strict liability arose out of cases involving the sale of goods, and it has been said that:

> Professional services do not ordinarily lend themselves to the doctrine of tort liability without fault because they lack the elements which gave rise to the doctrine. There is no mass production of goods or a large body of distant consumers whom it would be unfair to require to trace the article they used along the channels of trade to the original manufacturer and there to pinpoint an act of negligence remote from their knowledge and even from their ability to

inquire. Thus, professional services form a marked contrast to consumer products cases and even in those jurisdictions which have adopted a rule of strict products liability a majority of decisions have declined to apply it to professional services. The reason for the distinction is succinctly stated by Traynor, J., in Gagne v. Bertran, 43 Cal. 2d 481, 275 P. 2d 15, 20-21 (1954): "[T]he general rule is applicable that those who sell their services for the guidance of others in their economic, financial, and personal affairs are not liable in the absence of negligence or intentional misconduct. . . . Those who hire [experts] . . . are not justified in expecting infallibility, but can expect only reasonable care and competence. They purchase service, not insurance (CT/East, Inc. v. Financial Services, Inc., 5CLSR 817 [1975]).

Under this traditional approach, a finding that an agreement to provide computer equipment constituted either a sale of goods on the one hand or a contract for professional services on the other would appear to decide the issue of whether the doctrine of strict liability would apply. Following this line of reasoning, if an agreement to provide a computer package was construed as an agreement for professional services, then the provider could not be strictly liable in tort for any malfunction.

Traditional legal theories, however, cannot always be applied without difficulty to novel concepts such as computer agreements. It may be more appropriate, therefore, to adopt the approach used by a federal court in Wisconsin in Johnson v. Sears, Roebuck & Co. (355 F. Supp. 1065 [E.D. Wis. 1973]). In Johnson, the plaintiff argued that the hospitals that treated her for injuries had done so negligently and that they were strictly liable in tort. The court decided the issue of the applicability of strict liability to the sale of services by analyzing blood transfusion cases that held hospitals strictly liable in tort for providing blood containing impurities to patients. The court rejected the sales/service analysis and stated that the decision to impose strict liability should be made on an ad hoc basis by examining the facts involved in each particular case. The court reasoned that the ". . . decision should not be based on a technical or artificial distinction between sales and services. Rather, I must determine if the policies which support the imposition of strict liability would be furthered by its imposition in this case."

Statutory Sources of Liability for Reliance on Inaccurate Computer-Based Data

Regardless of whether suppliers of computer services should be held to a higher standard of care or subject to strict liability in tort, clearly the common law duty exists to exercise reasonable care to ascertain the accuracy of information furnished by a computer before relying on such data. This duty becomes particularly important when computer data are relied on in making periodic reports required by the federal securities laws. Management has a duty to maintain accurate records and third parties have the duty to verify the accuracy of information supplied by management.

Management's Responsibilities--Various provisions of the Securities Act of 1933 (the 1933 Act) and the Securities Exchange Act of 1934 (the 1934 Act) impose liability for making false or misleading statements of a material fact or for failing to state a material fact necessary to make statements made not misleading, in the light of the circumstances under which they were made. These provisions create a duty on the part of reporting companies to file accurate reports and to maintain accurate records. The Foreign Corrupt Practices Act of 1977 (FCPA) codified this duty to maintain accurate records.

A recent bank embezzlement of $21.3 million illustrates the importance of complying with the FCPA's requirement of establishing a system of internal accounting controls. The management of an entity is responsible for establishing and maintaining adequate internal controls, and it is worth noting that the complaint in a shareholder's derivative suit now being argued before the United States District Court for the Southern District of Texas relies partly on an allegation that management failed to do so. Management risks exposure to significant potential liability, therefore, if it fails to institute and enforce internal controls sufficient to comply with the FCPA.

Internal controls should ensure that data produced by a computer are accurate and reliable. This means that restrictions should be put on access to computer records and on who has the capability to enter information or alter data in the computer. "Audit trails" should also be used to create documentary evidence of transactions and of who made a particular data entry. Finally, electronic record keeping systems are only as trustworthy as the people who use them, and it is imperative that a security system be established to help preclude unauthorized persons from gaining access to the computer or altering information in the system.

Accountants' Responsibilities--The $21.3 million bank embezzlement raises substantial questions about the sufficiency of the auditing procedures of a bank or other company that uses an electronic data processing system for the storage and representation of assets. The role of an accountant performing an independent audit is to furnish an

opinion that the accounts of the company being audited are in proper order and that they fairly present the company's financial position. It seems obvious, therefore, that an independent accountant performing an audit of a company that uses an EDP system should examine the reliability of the system and the controls on it before issuing an opinion. Otherwise, the accountant's certification of the company's financial statements would have no reliable basis. The Second Standard of Field Work of the Generally Accepted Auditing Standards approved and adopted by the membership of the American Institute of Certified Public Accountants (AICPA) states that "[t]here is to 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" (American Institute of Certified Public Accountants, Statement on Auditing Standards No. 1, Sec. 150.02. [1973]). This Standard of Field Work requires an auditor to study and evaluate a corporation's system of internal control to establish a basis for reliance thereon in formulating an opinion on the fairness of the corporation's financial statements, and this basic duty does not vary with the use of different methods of data processing as the Standard states:

> Since the definition and related basic concepts of accounting control are expressed in terms of objectives, they are independent of the method of data processing used; consequently, they apply equally to manual, mechanical, and electronic data processing systems. However, the organization and procedures required to accomplish those objectives may be influenced by the method of data processing used.

The AICPA has recognized that "[t]he increasing use of computers for processing accounting and other business information has introduced additional problems in reviewing and evaluating internal control for audit purposes," and it has issued a Statement on the Effects of EDP on the Auditor's Study and Evaluation of Internal Control. This Statement provides that:

> When EDP is used in significant accounting applications, the auditor should consider the EDP activity in his study and evaluation of accounting control. This is true whether the use of EDP in accounting applications is limited or extensive and whether the EDP facilities are operated under the direction of the auditor's client or a third party.

When auditing a corporation with an EDP system, therefore, an auditor should thoroughly examine the system to evaluate its control features. To conduct his examination properly, however, the auditor must have sufficient expertise to enable him to understand entirely the particular EDP system involved.

Conclusions on Applying Legal Concepts

Everyone who uses or supplies computer services has a common law duty to exercise reasonable care to ensure that information supplied by the computer is accurate and reliable. The federal securities laws impose additional duties on management to keep accurate records and to devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances that transactions are executed in accordance with management's authorization and are accurately recorded. Finally, accountants who audit companies with EDP systems have a duty to review the company's system of internal controls and to disclose any material deficiencies to management and possibly to the public through notes to its certification of financial statements.

These various duties illustrate the necessity of taking steps to ensure the reliability of computer systems. A well-designed system of internal control is crucial to safeguard against the improper use of the computer. Internal control begins with the computer equipment itself. When converting to an EDP record keeping system, management should get outside advice on the type of system required and on the controls that should be built into the system. Management should fully understand what the computer programs in the system are designed to do and that the computer can do only what it is told and nothing more. This can be an important method of preventing fraud, and management should demand that internal controls be put into the system, because otherwise the programmer may not do so.

Once controls are built into the computer system itself, internal controls should be established and maintained to prevent unauthorized access to the system. The internal controls should cover all phases of EDP and include input, processing, and output controls. An overall plan of organization and operation should be devised containing controls over access to EDP equipment, as well as provisions for effective supervision and rotation of personnel, and the plan should be strictly enforced. Finally, an internal auditing process should be established to provide independent document counts or totals of significant data fields.

The independent accountant plays a major role in preventing unauthorized persons from gaining access to the computer system. Through his review of a company's internal controls, an accountant can detect possible weaknesses and recommend useful changes. It is very important, therefore, that outside auditors closely scrutinize a company's internal control system. A rigorous independent audit makes up the final stage of an overall plan to help prevent the production of inaccurate computer-based data.

Protecting Proprietary Interests in Computer Programs

Discussions with legal counsel at several of the field sites revealed considerable concern about proprietary interests in computer programs. Little communication exists between lawyers and data processing

managers, and areas of their mutual concerns are not often addressed. Communication is even more important today as programs and data files are increasingly viewed by management as valuable, intangible assets of their organizations. In addition, government and business organizations are increasingly acquiring commercially available computer programs where proprietary interests of providers and users must be protected. Selection of generally used controls will be strongly influenced by the need to preserve proprietary rights to computer programs.

Problems Addressed

Protecting proprietary interests in computer programs is a multifaceted task that requires knowledge of the law, computer programs, and security. Few data processing managers have this expertise in-house, but all owners and custodians of computer programs can and should add to their skills and knowledge from other sources of expertise.

Those involved with computer programs--owners, users, custodians, employees, and competitors--have two conflicting goals; sometimes the same party pursues both goals simultaneously for different products. One goal is to protect the computer program, either to ensure a competitive advantage by preventing others from using the computer program or to charge for its use or disclosure. The other goal is to ignore protection so that the computer programs can be used and transferred at will and without cost. The particular goal sought by an organization depends on its values, purposes, and policies; however, the data processing manager should understand the boundaries of fair and legal business practice that apply to users, custodians, and owners of computer programs, as well as to competitors.

The Nature of Computer Programs

Before the types of computer programs involved are identified, it is helpful to know why the laws differentiate computer programs from other parts of computer systems. A computer program is a form of intellectual property (a valuable, intangible asset consisting of ideas, processes, and methods) that is relatively new and eludes analogy to previously existing products. Debate continues as to whether computer programs are products, technical processes, or professional services. Computer programs are thus unique as a subject of treatment under existing law, and applying the law requires adapting current legal concepts of particular forms of computer programs. Computer programs are developed to run in specific types of computers (such as operating systems) or are machine-independent (such as many application programs). They may be in human-readable form or machine-readable form. Some computer programs are translated into different programming languages or converted to run on different computers.

Forms of Legal Protection

The five forms of legal protection that can apply to computer programs are patent, copyright, trade secret, trademark and contract.

Patents--Patent protection is a federal statutory right giving the inventor or his assignee exclusive rights to make, use, or sell a product or process for 17 years. An invention must meet several criteria to receive patent protection. First, it must involve statutory subject matter (i.e., physical methods, apparatus, compositions of matter, devices, and improvements). It cannot consist merely of an idea or a formula. Furthermore, the invention must be new, useful, not obvious, and must be described according to patent regulations in a properly filed and prosecuted patent application.

The status of patent protection for computer programs until 1981 was ambiguous. In three decisions the U.S. Supreme Court held that particular computer programs were unpatentable because of failure to meet one or more of the tests described previously. The Court declined to patent what it felt was merely a formula, it had held a process nonpatentable for obviousness, and it had refused a patent when the only novelty involved was the form of carrying out a nonpatentable step.

In 1981, however, the Supreme Court handed down two decisions that may have some effect on future patentability claims. These cases involved computer programs that are part of inventions otherwise eligible for patent. In one case, the Court decided that a process control computer program for curing synthetic rubber should not be denied a patent simply because it uses an algorithm (an ordered set of instructions) and a computer. The U.S. Patent Office must still determine whether the entire process is novel enough to warrant issuing a patent.

In a companion case, the Court let stand a lower court ruling that a module of the Honeywell Series 60 Level 64 computer system should be considered for patent. The module, which includes electronic circuits and a computer program fixed in the circuits, is a storage and retrieval device using internal storage registers. Again, the device must meet the novelty requirement before a patent is issued. Note that these decisions involve computer programs that are part of a patentable device or process; these decisions do not reverse past rulings that computer programs are not patentable.

Even if there were a major change in computer programs patent policy, few owners would seek patent status for their computer programs. The patent process is lengthy and expensive and requires full disclosure of the idea. Furthermore, a patent has only a 50% chance of surviving a challenge to its validity in the courts. For those few programs that really do represent technological breakthroughs, however, a patent would provide the exclusive right to use or sell the program for 17 years (patents are nonrenewable).

Copyrights--Copyright is the federal statutory protection for an author's writings. Written works created since January 1, 1978 are protected by the new copyright law, which provides exclusive rights to the author or his assignee for the copyright, publication, broadcast, translation, adaptation, display, and performance of the idea contained

in the work from the time it is embodied in tangible form. This protection is lost if the writing is published without copyright notice, which consists of the word copyright (or ©), the date, and the author's name. This notice must be affixed so that it attracts the attention of third parties (i.e., on the first or inside front page of a book or pamphlet). In late 1980 a federal copyright bill was enacted explicitly to cover computer programs and data bases.

Copyright is inexpensive and can be obtained quickly. One required and one optional copy along with minor filing fees must be submitted to the Copyright Office. The second copy can be the first and last 25 pages of the program. Although optional, the second copy is a prerequisite for bringing an infringement suit and for some remedies such as statutory damages and the award of attorney fees. The copyright remains in effect for 50 years beyond the death of the author and is nonrenewable.

Because copyright protects only against copying and requires disclosure of the idea, its usefulness is limited for some programs. However, it can be adequate protection for inexpensive package programs sold in the multiple copy market. The function of such programs is not unique; the value to the owner lies in selling thousands of copies.

Trade Secrets--A trade secret is a right protected by state rather than federal law. It is defined in many states as a secret formula, pattern, scheme, or device used in the operation of a business that gives the organization a competitive advantage over those who do not know it. Computer programs have qualified as trade secrets in a number of court cases.

The requirement for trade secret status is that the item must remain secret. Absolute secrecy is not required; for example, if the secret is disclosed only to people bound (by virtue of their relationship or by contract) to keep it confidential, trade secret status is maintained regardless of how many people know it. Confidential relationships include employees, agents in a fiduciary or trust relationship, and thieves. To prevent thieves from profiting from ill-gotten knowledge, the laws hold that they are in a constructive trust relationship. A contract is used to bind licensees and joint venture partners or investors. In some states these people are bound even without a contract.

Once the secret is disclosed without a requirement of confidentiality, or is disclosed to someone who does not know its secret character, the trade secret status is lost forever. (Trade secrets are often disclosed carelessly to user groups and at technical meetings.) If the secret is not disclosed, however, the protection can last forever.

Employees who learn the secret in the course of their duties are bound not to misappropriate it because of their trust relationship. Many employees do not realize the comprehensive nature of that trust and

should be educated by their employers before they injure both the employer and themselves by using computer programs developed for an employer for their own purposes.

Trademarks--Trademark protection provides the exclusive right to use a symbol to identify goods and services. Trademark rights take effect upon use in commerce. Registration with the U.S. Patent Office or a state agency is not necessary to obtain trademark status, but it helps greatly in exercising trademark rights. Trademark protection exists at both the federal and state levels. The protected symbol can be both a trade name and a logo (e.g., XYZ). The protection afforded by the trademark is limited to the name or logo. The program content itself is not protected. Because the major benefit of trademark protection is to prevent another product from being given the same name, this protection is useful only for programs that will be marketed.

Contracts--Copies of computer programs are ordinarily transferred to others in the course of doing business (sometimes in source language form); therefore, transfer is frequently accompanied by an agreement to keep the computer program confidential. Patented and copyrighted computer programs can be transferred using contracts that have more restrictive provisions than the patent or copyright law requires. The owner can, for example, contract with another not to disclose copyrighted computer programs. In addition, damages for disclosure or unauthorized copying, complex formulas for royalty payment for legitimate use, and the ownership of enhancements and changes to the computer program can also be delineated in a contract.

Selecting the Right Protection

The type of protection that is best for a particular computer program depends on several factors:

(1) The longer the lifespan of the program, the more likely that the expensive investment of patent protection will be worthwhile.

(2) The higher the value of the program, the more money that can reasonably be spent on protection.

(3) Algorithms that must be disclosed widely are (if otherwise worth the investment) best protected by patent, which precludes use as well as duplication. Copyright protects only against copying, and trade secret protection is irrevocably lost if the algorithm is inadvertently disclosed outside a confidential relationship.

(4) The most expensive protection is patent; the least expensive is copyright.

(5) Patents take the longest time to obtain; the other forms offer almost immediate protection.

(6) A patent protects against recreation; trade secret protection is lost if the program can be recreated.

These factors are summarized in Table 1.

Unresolved Legal Issues

Two unresolved but important legal issues affect the analysis summarized in Table 1. The first is the patentability of computer programs discussed previously. The data processing manager and corporate counsel should keep track of the continuing legal debate in this area. The second unresolved issue is the legal relationship between copyright and trade secret protection when both are used for the same product. Trade secret protection has been held by the U.S. Supreme Court to be compatible with patent protection, but the Court has yet to decide whether a trade secret can be copyrighted to protect the secret in case it is disclosed.

Table 1

DECISION TABLE FOR TYPES OF LEGAL PROTECTION

Decision Factor	High	Medium	Low
Estimated lifespan of the program	C or TS	P	C or TS
Value of the program to the owner	P, C, TS	P, C, TS	C, TS
Need to disclose the program to others	P, C	TS, C	TS
Owner's expense budget	P, TS, C	TS, C	C
Time sensitivity	TS, C	P, TS, C	P, TS
Susceptibility to reverse engineering	P	P, TS	TS, C

Notes: C = Copyright, P = Patent, TS = Trade secret.

The policies underlying the two forms of protection conflict: federal copyright protection contemplates disclosure, while state trade secret protection requires nondisclosure without an obligation for further disclosure. According to some legal scholars, a court could rule that a copyrighted program is not eligible for trade secret protection. Other legal scholars argue that since the disclosure requirement for federal patent protection has not preempted trade secret protection, the Supreme Court should also uphold the right of computer program owners to receive both trade secret and copyright protection.

Suggested Controls

Because of these critical and unresolved legal issues, developers should carefully evaluate the types of protection and remain alert to changes in the laws. At present, often the best alternative is to copyright computer programs and then to license or disclose the computer program using agreements that restrict use, transfer, and disclosure. This approach should not conflict with existing copyright law theory, and it achieves the same secrecy afforded by trade secret protection.

Embodying the program in electronic circuitry is another alternative that should be considered. It cannot be altered by the user and inhibits copying and user enhancements. In addition, the recent Supreme Court decision suggests that programs in such form can receive patent protection if they are parts of patentable devices. Without patent protection, they are susceptible to recreation and thus to loss of trade secret status.

To provide notice of the proprietary rights of computer-related materials, the owner should put a human-readable notice on all materials a user will see. The notice can be placed on a computer terminal that displays the program, on listings, on manuals, on containers of machine-readable material, and in the program itself. A suggested form of notice is:

> This is an unpublished work protected under the copyright law of 1976. It is owned by XYZ company, all rights reserved. Any unauthorized disclosure, duplication, or use is a violation of civil and criminal law.

If licensed, a reference to the license can be included in the notice.

If the work is published, it should have the formal copyright notice attached in lieu of the above statement. The intentional omission of the copyright will cause the owner to lose his copyright; an unintentional omission can be remedied.

Employer-Employee Relationships

Many problems covering computer programs protection arise from the employer-employee relationship, where two philosophies often conflict. One philosophy is that the products of the employee belong to the employer; the other is that employees should be free to change jobs during their careers and to use the expertise gained in one job in new work situations.

Although some employers might argue that all work done during employment belongs to them, and some employees might claim that their creations are theirs exclusively, the laws do not generally support either claim. State laws vary on this question; however, the prevailing view is that programs written or developed as a specific task assigned by the employer belong exclusively to the employer, and that programs written or developed solely by the employee, using the employee's own time and resources, belong exclusively to the employee. Most controversy over computer program ownership falls in the gray area between these two positions.

The following discussion centers on trade secret law since patent and copyright protection are less helpful. Patent protection for computer programs is ambiguous and hence rarely used, and most companies have a well-established patent assignment policy. On the other hand, the new copyright law is explicit regarding work for hire:

> In the case of a work made for hire, the employer or other person for whom the work was prepared is considered the author for purposes of this title, and, unless the parties have expressly agreed otherwise in a written instrument signed by them, owns all of the rights comprised in the copyright.

Conflicts of trade secret ownership between employers and employees for other than assigned work are usually resolved based on the resources used. Employees who develop new computer programs on their own time, at home, on a personally owned terminal, but using employer computer time may be found to own the programs; however, the employer may be given a royalty-free license to use the programs in its business. A more complex question concerns employees working at home on flextime or with an employer-owned terminal or microcomputer. In such cases, proof of whose resources are used in development is more difficult to establish.

Legal battles over program ownership are very costly to both sides and consume enormous amounts of time and energy. Often a court formulates a compromise so that neither side actually wins. To avoid going to court over program ownership, employers should have an explicit policy regarding employee-developed programs. This policy can be part of an organization-wide trade secret protection plan developed by management and legal counsel.

A basic control requires that each employee involved in developing computer programs should be required to sign an agreement concerning ownership of computer programs at the time of hire. A formal employment or secrecy agreement or an informal letter to the employer can be used. Since both types of agreement are legally effective, management style should determine which approach is used. The informal letter is friendlier, but the awesome contract form may make a more lasting impression on the employee.

If a simple letter is used, the following format is recommended for the key paragraph:

> All computer programs written by me, either alone or with others, during the period of my employment, commencing on _____, 19__, and up to and including a period of _____ after termination, whether or not conceived or made during my regular working hours, are the sole property of the company.

This important control prevents misunderstanding and protects the employer against legal action.

Employees may use skills developed during previous jobs; however, they may not use trade secrets disclosed to or produced by them during those jobs. This is enjoinable behavior and may result in the award of damages to the former employer. Departing employees should take nothing tangible from the old job--listings, notebooks, tapes, documents, or copies of any kind, including lists of specific customers. Prospective employers should carefully avoid crossing the fine line between hiring someone to provide expertise in a particular area and hiring someone to provide knowledge of a competitor's proprietary products or business plan. Special care is required when more than one employee is hired from the same company.

Another essential control requires that departing employees should be reminded during the exit interview that no materials or proprietary concepts received during employment can be used at the new job. They should be asked to read and sign a statement that acknowledges their understanding of this point. The statement should also affirm that no materials have been removed from the employer's premises and that all those previously in the employee's possession have been returned. Employers should obtain the employee's new address in case later contact is necessary.

During the exit interview, employees should have the opportunity to clarify gray areas--programs they wrote on their own time using company terminals and company computer time, innovations they developed that the company never used, and so on. Permitting a departing employee to use an invention that will not cause loss of competitive advantage can

ensure a friendly and loyal colleague in the marketplace. In any case, legal counsel should be involved in these sessions, because an attorney experienced in trade secret law can interpret the nuances of the interview more effectively and can emphasize the consequences of unfair competitive conduct.

Guidelines for Computer Program Users

Users who obtain computer programs outside of contractual or other confidential relationships that preclude competitive action can legally recreate the programs and use them freely even if they know they are trade secrets. In addition, users who obtain computer programs from third parties without any knowledge that they are proprietary are free to use them. In such cases the third party may be liable to the owner for misappropriation. Computer program users should note, however, that intentional wrongful use in this situation may lead to criminal and civil liability for infringement or misappropriation.

Patented inventions can only be used with the owner's permission. The alleged infringer, however, can challenge the validity of the patent in court and, if successful, can defeat the patentee's exclusive right to use the invention.

Another problem concerns the ownership of a user-made change or enhancement that significantly alters the constitution of the computer program. Neither copyright nor trade secret law is explicit on this point. Many vendor-user agreements require the user to return all copies of the computer program at the end of the term; however, few vendors forbid user changes and enhancements or ask for royalties from new works embodying or based on their computer programs. Some agreements contain provisions that any and all changes belong to the vendor. Thus, the computer program user should pay special attention to contract provisions regarding changes and enhancements. In the absence of a specific agreement, the user takes some risk but has a fair chance of surviving a challenge that user-made changes infringe on the vendor's rights.

Recommended Course of Action

The data processing manager should understand the legal alternatives for protecting computer programs and adopt prudent controls used by others under similar circumstances. If the organization uses computer programs developed and owned by outside parties, this understanding and use of controls can prevent legal problems and can ensure that the terms of the agreement for using the computer programs are proper. For organizations that develop computer programs in-house, a corporate policy based on a thorough knowledge of the laws is a basic control that can prevent misunderstandings between management and development personnel.

Such a policy can also ensure that the company does not lose a competitive advantage because of unauthorized disclosure or copying of programs. Because the laws in this area are subject to change, the data processing manager should stay in close touch with the organization's legal counsel to keep pace with the latest developments.

Meeting standards of due care and protecting proprietary interests in computer programs are examples of common sources of motivation and need to adopt generally used controls. Consideration of these common sources of motivation and need, as well as the generally used controls (many found in the study of the field sites), leads to a new computer security concept presented in the next section.

SECTION IV NEW COMPUTER SECURITY CONCEPTS

The Baseline Concept

Computer security reviews to identify and evaluate vulnerabilities, calculate risks, and select controls have been conducted assuming differences and uniqueness from one computer center to another because of their one-of-a-kind development. Differences in physical facilities, computer configurations, types or modes of computer usage, organization patterns, and computer application environmental factors have all been emphasized. However, similarities in the use and security of computers are appearing in many areas:

- Almost every computer center has secure area needs for housing of at least one computer in one room and peripherals in the same or adjacent room.
- Almost every well-run computer center has a procedure for physical access control to facilities.
- Every well-run computer center has a procedure to assure secure backup copies of data files and computer programs stored on computer media, documentation, and computer supplies.
- Every computer center has logs and journals of computer usage and performance that have importance for security.
- Every computer center has computer programs that contain controls to prevent erroneous processing.
- Every computer center has computer programs requiring legal ownership protection as indicated in Section III.
- Every well-designed computer center has some form of fire detection and suppression capabilities.
- Every computer center has staff in positions of trust.

A new concept of baselines of security controls can be developed from these and many other similar environments and vulnerabilities. A baseline of security controls is a set of generally used controls meeting commonly desired control objectives that should be present in every well-run computer center. The justification for having them is derived from

common usage and prudent management rather than from explicit identification of vulnerabilities and reduction of risk. If a baseline control is not selected for use, its absence should be recorded or alternatives should be selected and justified.

A control objective is a condition or event that is to be avoided, deterred, detected, prevented or recovered from. Examples are as follows:

- Avoid violations of laws and regulations
- Detect unauthorized system use
- Prevent unauthorized access to sensitive areas.

A control is the policy, method, practice, device, or programmed mechanism to accomplish a control objective. A control has implementation variants that are established in the detailed specifications for the control in a particular use. Baseline controls have never before been identified, and it is not known how many would qualify universally or within any specific organization. However, the baseline concept is now feasible because of the control selection experience gained as the computer security field matures. The 82 controls found in the study of seven computer field sites are offered in Section VI as a preliminary step in identifying baseline controls.

A baseline of security need not be a rigid, unalterable set of control objectives and their required controls and variants. The purpose of a baseline is to specify a minimum set of controls such that if a control is omitted, there would be explicit reasons identified why it is absent or why an alternative control is equivalent. If these exceptions from a baseline are acceptable to the authority ultimately responsible for security, the baseline could still be said to be the accepted criterion. In fact, this exception-taking is the process by which baselines evolve. When enough support for an exception exists, a baseline is changed to include the exception as part of the baseline.

A single, clear-cut baseline is improbable. As espoused by different experts and organizations, baselines may be different. For example, differing baselines may be established by insurance companies, banks, and manufacturers. Security experts, auditors and consultants may have differences of opinion over inclusion of a control in a baseline but little disagreement about control objectives. In addition, some controls and even some control objectives will become obsolete as technology changes and advances. For these reasons, a baseline is not identified as a standard. Whereas a baseline may be called a standard within any one domain (e.g., federal standards established by the U.S. the U.S. Department of Commerce, National Bureau of Standards, or a particular company), the acceptance of general standards should be reserved for American National Standards Institute adoption.

Benefits of Baseline Controls

The success of the baseline concept lies in obtaining concurrence and acceptance of a sufficient number of generally used controls by computer security administrators and, in turn, by the management responsible for the expenditure of resources for computer security. Certainly enough controls are now identified in extensive security literature and exist as commercial products. Management must be willing to accept a recommended control justified only by having a security administrator show that it is part of a baseline. Prudent management will be motivated to do this out of trust in the security administrator, the prospect of saving time, the reduction of expenses for evaluation and study, and the contentment of knowing that the organization is protected by generally used controls.

Baseline security will allow organizations to avoid unnecessary expenditure of resources to engage in detailed study of already resolved problems and selection of solutions by extensive justification efforts, data gathering, and analysis. It will facilitate providing simple, inexpensive, effective safeguards comprehensively before difficult, new problems are attacked. As computer-using organizations adopt the baseline approach for selection of controls, they will increasingly rely on the best security controls used most successfully by other organizations. This practice will further advance the baseline concept by encouraging uniformly high quality security. In addition, this will stimulate and facilitate a formalized theory of computer security, putting it on a par with other theories in computer technology. The training of computer security specialists will likewise be formalized and advanced.

Identification of generally used controls and their variants will stabilize and enlarge the security products market to stimulate a wider range of less expensive control products that require fewer model types and options. For example, when procedures are developed and accepted for cryptography use, then cryptographic products will become more uniform and cost less.

Future Development of Baseline Concepts

This report alone is not sufficient to assure the feasibility of baseline concepts. The control objectives and controls identified from the seven field site visits may form a baseline nucleus because they are explicitly documented as currently in use in several computer centers, and representatives of all seven sites agreed on their common usage. The literature abounds with descriptions of controls, each usually recommended by one or two authors and not necessarily supported by widespread use. The Systems Auditability and Control Reports from the Institute of Internal Auditors identifies 300 controls and a set of control objectives based on a survey of 1,500 computer-using enterprises. However, one conclusion of these 1977 reports was a significant lack of common usage. Only a few organizations were found to be using any particular control.

It is hoped that the baseline concepts will not be seen as alternatives to quantitative and qualitative risk assessment methods now in use. Baseline controls would be selected before such assessments take place so that the obvious, accepted, routine controls could be applied before risk assessments are used. Therefore, assessments can be started further along in the controls selection process.

When protection from intentionally caused losses is of concern, a game strategy must be used. The intelligent opponent will normally not attack where effective controls are in place but will seek vulnerabilities resulting from a lack of controls. In other words, losses will tend to occur where victims have not thought to put controls. It must be assumed that an intelligent opponent will know as much about published baselines as their originators do and will take advantage of any deficiencies. Therefore, the baseline concepts are essentially forced on potential victims. These vulnerable organizations must establish full baseline protection as routine, prudent operation to be able to concentrate on those vulnerabilities created by the special circumstances and new environmental factors brought about by use of new technology and new applications. After all, that is what intelligent opponents will also be concentrating on after being rebuffed by baseline controls.

The baseline concepts have a solubrious effect on errors and omissions; they can mitigate unintentional threats. Unlike intentional acts, sources of errors and omissions can only affect specific vulnerabilities. Therefore, an escalated game strategy is not required. Prevention of accidental loss results mostly from control of intentionally caused loss.

Formal bodies for identifying baseline controls might include the American National Standards Institute, but based on its historical practice the institute would probably standardize only a few of the most significant controls such as cryptographic algorithms or uninterruptable power supplies. The Generally Accepted Accounting Practices adopted by the American Institute of Certified Public Accountants might be an interesting model to build on. However, this would require a publicly and legally recognized professional body in a narrowly defined, highly controlled (certified) practice. The computer field is probably too highly diversified and changing too fast for the necessary stability and consolidation of professionalism for a similar concept to work for adoption of baselines in the near future.

The baseline concepts must therefore evolve slowly over a long period to achieve a state close to general concurrence. Recognition of the baseline concepts at this early stage should facilitate their development. It can be argued that the number of generally used controls is insufficient to form good baselines. However, the similarity of control needs has never been tested. In fact, all current methods for selection of controls have been based on the opposite assumption that every situation is unique. Assuming at least some commonality of needs and controls, a beginning based on potential benefits of baseline concepts may produce sufficient results to counter such arguments.

The types and number of control objectives and controls in each category described in this report will change as the computer security field matures, new potential threats arise, and the technology changes. Control objectives and controls will be moved from special to selective to baseline categories, some controls will be dropped or replaced, and new controls will be developed. Today, few control objectives and controls have achieved explicit, generally used, baseline status because the concept is new and differences rather than similarities have been emphasized at computer centers. In the future, baselines should grow and become more strongly accepted. Special controls could decrease; many will become baseline controls as security needs become more commonly known. This could occur as selection of controls becomes more strongly based on what others are doing under similar circumstances. Justification for recommendations will increasingly be based on the concept that "we should do this, because company X is doing it."

SECTION V GENERALLY USED CONTROLS

Method of Investigation

A small range of types of computer-using organizations was chosen for study of common security needs and controls to limit study to seven field sites. Organizations in the criminal justice community and one insurance company were chosen to focus on common security needs for confidentiality of personal information. One large business was selected to contrast the six organizations in the criminal justice area with at least one very different organization but one that had a similar need. The types of organizations chosen are listed below:

- A state department of administration
- A private law research institute
- A county government
- A state department of justice
- A city government
- An insurance company
- A university institute for social research.

Teams of two experienced computer security consultants spent 3 or 4 days at each of the seven sites. An attorney specializing in the computer field accompanied teams to three of the sites.

Managers at each site were asked to identify the best controlled activities and most effective controls they had in place. The purpose was to find the most exemplary security measures and not the deficiencies. Managers were also asked to specify how they would like to improve or add to controls and to indicate their plans for future enhancements of controls. Teams concentrated on activities and areas where personal data existed. In this sense the identified control objectives, controls, and control variants can be considered to fall mostly within a selective baseline for computer centers that process significant amounts of sensitive personal data. Even so, most controls found fit general baselines rather than only selective baselines.

Project teams returned from field sites with extensive rough field data. They prepared detailed descriptions of controls using several models that led to the subject headings shown in Table 2 for each control description presented in Section VI.

Table 2

SUBJECT HEADINGS

Type of Baseline: Baseline, Selective Baseline, or Special

1. Control Title: A descriptive name for the control.

2. Objective: Control objective stating the type of adversity dealt with.

3. Description: A paragraph describing the idealized control function but based on observations at the field sites.

4. Variables: Variant specifications to be determined in particular cases.

5. Strengths: The particular positive values of the control in the field sites.

6. Weaknesses: Undesirable effects of the control such as creation of additional vulnerabilities or failure to reduce target vulnerabilities.

7. How to audit: Role of the auditor in testing and reporting the effectiveness of the control.

8. Purpose: Which security functions are performed, namely, deterrence, detection, prevention, or recovery.

9. Control area: Indicates the particular area of EDP environment in which the control is implemented, namely, computer center, application system, system development and maintenance, computer system and management.

10. Mode: Type of control and way in which the control is implemented or executed, namely, manual procedures, hardware, computer operating system, computer application programs, or policy.

Table 2 (concluded)

11. Area of responsibility: Functional activity in an organization having responsibility and accountability for assets that the control protects, namely, user, security, legal counsel, audit, management, insurance, safety, personnel, computer security, quality assurance, computer program development and maintenance, computer operations, input control and output control.

12 Cost: Cost of the control and its operaton on a scale of low, medium, and high. A low cost control would probably not appear as a line item in an annual budget. A medium cost control would be a line item, and a high-cost control would have a material effect on a computer center budget.

13. Principles of note: Strongly exemplified control principles, namely, cost-effectiveness, simplicity, override capability, independence from need for secrecy, least privilege, entrapment, independence of control and subject of control, minimal exceptions, compartmentalization and defensive depth, minimal dependency on shared mechanisms, completeness and consistancy, instrumented, accepted and tolerated by personnel, sustainable, auditable, and facilitation of accountability.

At the completion of the field work and documentation of controls, a two-day workshop attended by the project teams, field site representatives and project consultants was held at SRI International. Each finding at each field site was reviewed. Duplicates and overlapping controls were identified, and each control was classified as baseline, selective, special, or rejected. Rejection occurred because of inconsequential effectiveness, inappropriateness, or poorly or confusingly documented reports. Duplicated or overlapping controls at the field sites indicated common usage and reinforced their classification as baseline or selective.

The control objectives were selected after the controls were collected. The controls found determined the control objectives, the reverse of usual practice which starts with determining vulnerabilities and needs to reduce them in terms of control objectives. The reverse process here of finding the best controls first again emphasizes the baseline concept of identifying the best controls in use for reducing common vulnerabilities without particular regard to specific vulnerabilities.

Letting natural groupings of controls determine the control objectives has resulted in less than comprehensive treatment of vulnerabilities. Important control objectives are missing from the study because no commonly used controls were found to satisfy them. Such control objectives are left for treatment as special categories or for further search of common controls in a wider range of computer centers. Therefore, the control objectives, controls, and variants presented in this report must not be taken as comprehensive or complete for all needs. In fact, the controls presented in this report are not necessarily endorsed by field site organizations, the project team, or its sponsors.

Indices of Controls Found

Section VI contains descriptions and specifications of the 82 controls analyzed in this study. The titles and Section VI page numbers of the controls have been grouped according to the five indices presented at the end of this section. Each control is identified at least once in each index. The first index, a list of controls by security topic, identifies controls in the order presented in Section VI and thus represents a table of contents for the section. Each control is located by a two-part page number; the first identifies the security topic number and the second (after a decimal point or space) identifies the first page of the control within each security topic subsection.

The indices provide a computer security practitioner with a simple and easy means of locating all controls under a variety of types of headings: security topic, control objective, area of responsibility, mode (type) of implementation or execution, and area of control environment. For example, if a practitioner is considering controls that would

be of interest to computer users, legal counsel, or audit management, then the list of controls by area of responsibility would be useful. If a practitioner is considering computer application program controls or manual procedure controls, then the list of controls by mode of implementation or execution would be useful.

Overview of Controls by Topic

In the first index, seven computer security topics were identified for categorizing the 82 controls. Each topic includes 8 to 21 controls. These topic areas including some of the more significant controls are summarized below.

1. Manual Assurance of Data Integrity

Computer security extends to the manual handling of data before entry into computers and after computer processing. Data and the programs that process the data must be explicitly assigned to the care of the owners, custodians, and users. Each party must be held accountable for their integrity and safekeeping through confirmation of receipt, inspection at each manual handling step, use of printed proprietary notices on documents, and proper archiving or destruction of used documents. Data representing personal information requires great care to protect privacy, including review of types of human subject data for appropriateness, need, completeness, and timeliness.

2. Physical Security

Physical security involves the buildings that house computer centers, as well as the remote computer terminals. Within the established security perimeters, access to work areas must be restricted with physical barriers, appropriate placement of equipment and supplies, and universal wearing of identification badges. Emergencies must be prepared for, alternative power sources provided in many cases to assure uninterrupted processing, and incoming and outgoing materials inspected. Access to loading areas requires special precautions.

3. Operations Security

Operation of computers requires many controls. Isolation of sensitive computer production jobs to minimize exposure to modification, destruction, exposure, or unauthorized use especially separating production and testing activities, is essential. Computer system trouble logs and activity records must be kept and used. Magnetic tapes and disks and output documents must be appropriately identified, and copies must be made and kept safe for backup. Contingency and recovery plans must be prepared and tested. Employee identification on work products and other practices to assure worker trustworthiness must be carried out.

4. Management Initiated Controls

Security requires direction and support from top management to assure adequate protection; for example, sensitive duties among employees should be appropriately separated. A computer security management committee to review and approve new controls is essential. The important functions of EDP auditor and computer security officer should be established and staffed. Proper funding for security and especially for contingencies and recovery are needed. Data should be classified for properly distinguishing degrees of control. The reports and documentation dealing with security are particularly sensitive and must be held at the highest level of protection.

5. Computer Program Development and Maintenance

Computer programs must contain adequate controls; responsibility for the controls and program changes must be assigned to assure compliance with laws and regulations as well as overall quality. This also requires participation by computer users and EDP auditors at critical times during program development. Access to computer programs must also be closely controlled.

6. Computer System Control

Controls in the computer operating programs and other major program subsystems used in many applications are essential. Outside vendor supplied programs and changes to them require special care. Data bases of personal information must conform to privacy constraints. Input data validation, exception reporting, and possible use of cryptographic protection using secret keys are important controls that can be provided by the system for many applications.

7. Computer System Terminal Access Controls

Access to computers from remote terminals changes the nature and extent of potential losses, especially when dial-up access from any telephone is possible. Transaction privileges, output display restrictions, terminal identifiers, log-in protocols and password access by authorized users are essential. Data file access controls and logging such activities are also important. Finally it is essential to have a terminal user's agreement document to assign accountability properly.

LIST OF CONTROLS BY SECURITY TOPIC

LIST OF CONTROLS BY CONTROL OBJECTIVE

LIST OF CONTROLS BY AREA OF RESPONSIBILITY

This list of titles of controls indicates the areas of functional activities in an organization that has responsibilities for the controls. Some controls are listed more than once if they are the responsibility of more than one functional area. The areas are: user, security, legal counsel, audit management, insurance, safety, personnel, computer security, quality assurance, computer programs development and maintenance, computer operations, input control, and output control.

LIST OF CONTROLS BY MODE OF CONTROL IMPLEMENTATION OR EXECUTION

This list of titles of controls indicates the modes in which the controls are implemented or executed. Some controls are listed more than once when they are implemented or executed in more than one way. The modes are manual procedures, hardware, computer operating system, computer application programs, and policy.

LIST OF CONTROLS BY AREA OF CONTROL ENVIRONMENT

This list of titles of controls indicates the area of particular EDP environment in which the controls are implemented. Some controls are listed more than once when they overlap functions. The areas are: computer center, application system, system development and maintenance, computer system, and management.

SECTION VI CONTROLS FOUND IN PRACTICE

Control Section 1

MANUAL ASSURANCE OF DATA INTEGRITY

1. Control Title: Assets Accountability Assignment

2. Objective: Prevent asset responsibility loss.

3. Description: Specific data producers, computer users, and computer center staff are assigned explicit ownership or custodial accountability and usage rights for all data, data handling and processing capability, controls, and computer programs. This can be done by establishing policy; establishing meaning of ownership, usage, and custodianship; and requiring that forms be completed and logs made designating and recording such accountability for data and programs and copies of them in all locations and for specified times. For example, one organization has a set of booklets for each data activity area stating ownership, usage, custodial, and control requirements. Another organization has this information as part of its policy manual.

4. Variables: Owners, users, custodians, data, programs, responsibilities, accountability, sanctions.

5. Strengths: Accountability for assets is basic to their security. Accountability assignments also make clear who is responsible and accountable for each control and its effectiveness and overall adequacy of protection.

6. Weaknesses: If accountability assignments are not kept up to date with changes in assets and organizations, confusion and a loss of accountability can occur. Strict accountability can result in a structure that inhibits one owner from assuming responsibility for another's assets when emergencies or sudden changes occur.

7. How to Audit: Questionnaires and interviews should be used to assure accountability of all assets and discover any inconsistencies or lack of awareness of assignments in compliance with policy.

8. Purpose: Prevention

9. Control Area: Management

10. Mode: Policy

11. Area of Responsibility: Management

12. Cost: Medium

13. Principles of Note: Accountability

1. Control Title: Confirmation of Receipt of Documents

2. Objective: Prevent disclosure, taking, or unauthorized use of documents.

3. Description: The confirmation process consists of verification of receipt of documents. Confirmations of delivery can be made by obtaining master files of names of input/output documents and their addressees, performing a selection of a sample of addressees by running the master file on a computer separate from the production computer or at least at a time different from normal production work. Confirmation notices and copies of the documents are then sent to the addressees to confirm that the documents are correct and that they received the documents as expected. Confirmation of smaller volumes of documents can be easily done on a manual basis. Receipt forms are used by recipients of particularly sensitive documents and returned to the sender to confirm correct report distribution and encourage accountability.

4. Variables: Area of responsibility, type of reports, frequency, sample type and size, acceptable percentage of response, exception action, forms design.

5. Strengths: An audit department's use of confirmations to determine the correctness of customer's balances in banking is well known. The use of confirmations in the insurance industry is also occasionally practiced. This suggests the possibility of extending the confirmation techniques as a general control to be used in a wide range of applications. Receipts increase assurance of confidentiality. Printing receipt forms embedded in computer output to be returned to senders may be more efficient.

6. Weaknesses: The possibility of building the confirmation process into the application may not be desirable since it might compromise the independence of confirmation control. Return of forged receipts can be accomplished. Failure to trace and recover missing receipts can cause rapid deterioration of control.

7. How to Audit: This control is used as an audit tool. Review number and nature of confirmation-related activities for costs and benefits. Sampling of receipts and sensitive report deliveries can confirm correct procedures.

8. Purpose: Detection

9. Control Area: Application system, computer center

10. Mode: Manual procedures

11. Area of Responsibility: Audit, output control

12. Cost: Medium

13. Principles of Note: Auditability, accountability, instrumentation.

1. Control Title: Data Accountability Assignment to Users

2. Objective: Prevent asset responsibility loss.

3. Description: Users are formally assigned the responsibility for the accuracy, safekeeping, and dissemination of the data they handle. If the data processing department does not handle data properly, then it is up to the users to require corrections. Organizationally, users provide a data processing department with the resources to assist them with their functions. In terms of controls, users should be able to tell data processing what is required in terms of data accuracy, relevance, timeliness, handling procedures, etc.

4. Variables: Identification of users, responsibilities, documentation of procedures, policy.

5. Strengths: Explicit accountability ensures correct processing. Failures can be identified more easily.

6. Weaknesses: Users may not be knowledgeable enough to determine that data are inaccurate or improperly handled. This control requires that users have at least a fundamental understanding of computer security and privacy issues and controls. This may run contrary to many current organizational structures where data processing in some sense controls the users.

7. How to Audit: Review organizational assignment of responsibilities for computer security and privacy matters. Discuss with both user and data processing management their mutual responsibilities regarding computer security and privacy. Review procedures in which users correct records, control the dissemination of records, and otherwise actively participate in the enforcement and design of computer security controls.

8. Purpose: Prevention

9. Control Area: Management

10. Mode: Manual procedures

11. Area of Responsibility: User

12. Cost: Low

13. Principles of Note: Simplicity, independence of control and subject, accountability.

1. Control Title: Suppression of Incomplete and Obsolete Data

2. Objective: Prevent modification, disclosure, or unauthorized use of obsolete or incomplete input/output data.

3. Description: Dissemination and use of incomplete and obsolete data are prevented or restricted by directive of the organization. This directive must be implemented by receivers of data that are to be processed, converted, or stored by reasonableness checks within application systems and by output control and dissemination activities. For example, in criminal justice information systems, access to nonconviction and arrest data that are one year old or more and do not contain a disposition is restricted to certain types of requestors. The same concept (i.e., if a record is incomplete or outdated it should not be disseminated) can be applied to other applications besides criminal histories. Such data may also be selectively restricted by requestor type.

4. Variables: Means of invoking directions, identification of relevant types of data, violation or exception actions, sanctions, recovery from disclosure.

5. Strengths: Prevents decisions from being based on outdated and/or incomplete information. Prevents the privacy of a data subject from being violated (in the above example if the individual were to be acquitted, the arrest information would not be disseminated). Allows data bases to be updated (old and irrelevant information may be deleted), thus reducing operating costs and potentially increasing performance.

6. Weaknesses: Prevents decisions from being made on the best information available (a worse decision might be made based on no information than on partial or outdated information). Lack of automatic means of detecting incomplete or obsolete data makes directives difficult to enforce.

7. How to Audit: Review dissemination policies and procedures for reasonableness and compliance with regulatory, statutory, and civil requirements. Review procedures to block dissemination of certain types of information. Review procedures to expunge records from certain data bases.

8. Purpose: Prevention

9. Control Area: Management

10. Mode: Manual procedures

11. Area of Responsibility: Input/output control, users, management, development.

12. Cost: Low

13. Principles of Note: Completeness and consistency.

1. Control Title: Discarded Document Destruction

2. Objective: Prevent disclosure, taking, or unauthorized use of documents.

3. Description: Input/output documents, including any human readable documents or nonerasable computer media (carbon paper, punch cards and tape, one-time-use printer ribbons), should be reviewed for potential loss sensitivity and appropriately destroyed when no longer needed. Appropriate protection of materials awaiting final disposition should be used. Logging of all actions to ensure an audit trail and adherence to rules is essential. Strict assignments of tasks and accountability are essential. Documents such as obsolete system development materials, test data and manuals, and obsolete criminal histories should be considered.

4. Variables: Secure storage facilities; method of destruction, e.g., mechanical (shredding), chemical, or burning; logging method; marking documents for disposition.

5. Strengths: Provides complete accounting for all documents. Reduces exposure to loss in facilities and trash. Makes facilities less cluttered and reduces fire hazards. Reduces cost of storage.

6. Weaknesses: Expensive errors could result from discarding valuable documents. Sensitive documents are concentrated in one area and in one activity.

7. How to Audit: Examine trash for sensitive documents. Examine sensitivity criteria for appropriateness. Observe storage and destruction areas. Do sample confirmations of destruction based on destruction log.

8. Purpose: Prevention

9. Control Area: Computer center

10. Mode: Manual procedures, hardware (shredder)

11. Area of Responsibility: Input/output

12. Cost: Low

13. Principles of Note: Least privilege, completeness, and consistency.

Selective
Personal Data Input from
or Output to External Organizations

1. Control Title: Personal Data Input/Output Inspection

2. Objective: Prevent disclosure or unauthorized use of personal information.

3. Description: An organization that receives or disseminates data bases from or to outside sources should have an input/output control group. This group checks the data bases when they are received and disseminated. It checks for the inclusion of improper data fields, such as individual names and social security numbers. Also, more sophisticated checking of the relational aspects of the data field is done to determine whether individuals can be identified by combining information from multiple fields. The group screens all files to be received and investigates anomalies. A log is kept of all activity.

4. Variables: Organization, specific rules, approval and logging forms.

5. Strengths: Potential privacy and confidentiality problems are caught early before data are made available to outsiders. This group also examines data to see that they meet the organization's standards with respect to items such as format, content, and value.

6. Weaknesses: High-level people are required to review the data bases.

7. How to Audit: Compliance review of existing data bases and review of criteria used by the group to evaluate the data bases.

8. Purpose: Prevention

9. Control Area: Computer center

10. Mode: Manual procedures

11. Area of Responsibility: User

12. Cost: Medium

13. Principles of Note: Independence of control/subject, compartmentalization, accountability.

Selective
Human Subjects of Research
or Processing

1. Control Title: Human Subjects Review

2. Objective: Prevent disclosure and unauthorized use of personal information.

3. Description: An independent review board (Human Subjects Review Board) reviews all proposals in an organization concerning treatment of subjects in studies. The board is made up of members of the parent organizations, some from the department in question, and some from outside the department. The charter of the board is to determine whether the subjects of a study will be put "at risk" or "at a disadvantage" because of participation in the study. The manner in which individual privacy (data confidentiality) is handled is a key issue. The board reviews the original plans of the project, the mode of operation, and justification of any risks to ensure that the potential benefits of the activity outweigh the potential costs. The board also has the responsibility to evaluate the staff decisions. The reason for this evaluation is that not all problems can be anticipated by the board. Three areas of qualifications are examined: (1) sensitivity to issues of privacy; (2) personal values; and (3) general competence and ability to cope with unforeseen problems. All decisions are documented.

4. Variables: Organization, criteria for acceptable activities, powers.

5. Strengths: An independent review is made at the beginning of the project. The review is made by peers and includes intangible factors.

6. Weaknesses: Control depends on the quality of board members, and sometimes not all problems are found.

7. How to Audit: Review minutes of the board meeting and any privacy problems that do occur.

8. Purpose: Prevention

9. Control Area: Management

10. Mode: Manual procedures

11. Area of Responsibility: Users

12. Cost: Medium

13. Principles of Note: Independence of control/subject, accountability.

1. Control Title: Proprietary Notice Printed on Documents

2. Objective: Prevent disclosure or unauthorized use of documents.

3. Description: Sensitive and valuable documents have a classification (e.g., "sensitive," "private," "proprietary," "confidential," "for authorized parties only") or an explicit warning indicating that the information is the property of a certain organization, that it should be handled according to special criteria, that it is not to be used for certain purposes, etc. One site chose to print confidential in the middle of the page; although this made reading a bit more difficult, it prevented people from cropping the record and photocopying it to remove any indication that it was confidential. Another approach is to have the computer print appropriate words on only sensitive output. (This has the advantage of warning display terminal users that the information should be specially treated.) Policies and procedures must also be written.

4. Variables: Selecting documents, wording, how printed, rules of use, owner's interest.

5. Strengths: This control reduces ambiguity associated with the use and dissemination of sensitive information, provides concrete evidence that steps were taken to control information (this may be of use in court), and can be used to control use of proprietary software. Likelihood of privacy violation can to some extent be avoided or lessened. Use of copyright or trademark laws may reduce unauthorized distribution and usage of sensitive information.

6. Weaknesses: Errors of omission become more severe.

7. How to Audit: Examine samples of output to see that they contain an appropriate notice. Discuss the wording of such notices with legal counsel. Determine that the notice cannot easily be stripped from the output.

8. Purpose: Deterrence

9. Control Area: Computer center, application system

10. Mode: Manual procedures, application system, computer system

11. Area of Responsibility: User, legal, computer security, operations, input/output.

12. Cost: Low

13. Principles of Note: Minimization of exceptions, compartmentalization, acceptance, sustainability, auditability.

1. Control Title: Completion of External Input Data

2. Objective: Prevent modification, disclosure, or unauthorized use of obsolete or incomplete input/output data.

3. Description: If missing essential data are still missing beyond a time limit, take steps to obtain the appropriate data. Within the criminal justice environment, a request for disposition information is issued when a particular record has remained incomplete beyond a time limit.

4. Variables: Types of external data, time periods, method of completion, forms design.

5. Strengths: Acts as an error correction/detection control identifying records for which important information is still missing after a certain period of time (the update could have been misplaced, processed incorrectly, inadvertently omitted, etc.). Preserves personal privacy, ensuring that incomplete records, which may have misleading decisions based upon them, are reduced. The control also helps keeps records up to date.

6. Weaknesses: Administrative overhead associated with requests for information, when the information may not yet be available, may be a burden to the data supplier who may not be able to easily provide the information requested or who may not provide it because it is too costly. Unless data suppliers have a good reason for providing additional information, they may ignore requests for additional information. Information providers may no longer be able to provide information (due to funding and other reasons). Resolution may involve significant liaison efforts and problems in different levels and branches of government.

7. How to Audit: Review policies and procedures for requesting additional data. Identify certain records (preferably based on a random sample) that are in need of followup and determine that the proper requests have been made.

8. Purpose: Prevention, detection

9. Control Area: Computer center, application systems

10. Mode: Manual procedures, application system

11. Area of Responsibility: Users, computer operations, development

12. Cost: Low

13. Principles of Note: Independence of control and subject; completeness and consistency; instrumentation.

1. Control Title: Low Building Profile

2. Objective: Avoid destruction of assets and business interruption.

3. Description: Buildings housing computer systems and the computer facilities should be unobtrusive and give minimum indication of their purpose. There should be no obvious signs identifying computing activities outside or inside buildings. Buildings should look unimpressive and ordinary relative to nearby buildings. Building lobby directories and company telephone books should not identify locations of computer activities except for offices and reception areas that serve outsiders (users, vendors, etc.) and are located separately from operational areas. Physical access barriers, including access control signs, should be reasonably visible, however.

4. Variables: Building materials, windows, location relative to other functionally related areas, prestige and image value, safety.

5. Strengths: A low profile reduces the likelihood of attention by destruction-minded outsiders. Such attention tends to be directed away to other more visible targets.

6. Weaknesses: A low profile may reduce business promotion values and inconvenience visitors, vendors, delivery people, and others who have a legitimate need to find computing facilities.

7. How to Audit: Observation by those familiar with computing locations. Tests by persons unfamiliar with computer locations.

8. Purpose: Deterrence

9. Control Area: Computer center

10. Mode: Manual procedure

11. Area of Responsibility: Management, security

12. Cost: Low

13. Principles of Note: Avoidance of need for design secrecy, completeness and consistency, least privilege.

1. Control Title: Physical Security Perimeter

2. Objective: To avoid destruction of assets and business interruption.

3. Description: The physical perimeter within which security is to be maintained and outside of which little or no control is maintained should be clearly established. All vital functions should be identified and included within the security perimeter. Physical access control and prevention of damage immediately outside security perimeters should be carefully considered. For example, physical barriers should extend to the base floor and to the base ceiling around sensitive areas. Areas beneath false floors and above false ceilings must be controlled consistent with the control of working areas between them. Important equipment, such as electrical power switching and communication equipment and circuits, must be made secure and included witin the security perimeter. Employees and on-site vendors should be made aware of perimeters on a least-privilege basis. The perimeter should be easily discernible, simple, uncluttered, and sufficiently secure relative to the value of assets inside the perimeter. Drawings and specifications of the perimeter should be available and used for planning any facilities changes. Additional barriers between areas with different security requirements within the exterior barrier also should be established.

4. Variables: Placement of perimeter, perimeter barriers

5. Strengths: Consistency and completeness in physical security will ensure maximum protection. Modification of facilities can be made without compromising security.

6. Weaknesses: Cooperation among all parties involved may break down and limit effectiveness. An obvious perimeter may atrract undesirable attention.

7. How to Audit: Physical inspection of security perimeters should be done periodically, and physical barriers should be tested.

8. Purpose: Prevention

9. Control Area: Computer center

10. Mode: Hardware

11. Area of Responsibility: Security

12. Cost: High

13. Principles of Note: Completeness and consistency, minimization of exceptions, isolation, compartmentalization.

1. Control Title: Placement of Equipment and Supplies

2. Objective: Avoid destruction of assets and business interruption.

3. Description: Equipment, such as telephone switching panels and cables, utilities, power and air conditioning plants, computer devices, and supplies, such as paper, cards, chemicals, water, tapes, and disks, should be placed or stored to ensure their protection from damage and minimize the adverse effects they may have on other items. Dust, vibration, chemical effects, fire hazards, and electrical interference are produced by some equipment and supplies, and they should be kept separate from equipment and supplies affected by these phenomena. Items requiring special safeguards should be isolated to reduce the extent of required safeguard coverage. In multifloor buildings, vertical as well as horizontal proximity should be considered.

4. Variables: Equipment and supplies, nature and extent of separation requirements and limitations, functional relationships.

5. Strengths: Cost of protection can be reduced. Damage can be reduced and isolated. Traffic can be reduced in some cases.

6. Weaknesses: Distances and barriers between functionally related items may reduce efficiency. For example, small supplies of paper may be needed close to printers because of the remoteness of the primary storage area. Traffic problems may arise, such as the need for access within the security perimeter by telephone repairmen.

7. How to Audit: Observe placement of equipment and supplies and conduct vulnerability analysis.

8. Purpose: Prevention

9. Control Area: Computer center

10. Mode: Hardware

11. Area of Responsibility: Computer security, operations

12. Cost: Medium

13. Principles of Note: Control and subject independence, limit of dependence on other mechanisms.

1. Control Title: Emergency Preparedness

2. Objective: Prevent human injuries and other damages from contingencies.

3. Description: Emergency procedures should be documented and periodically reviewed with occupants of areas requiring emergency action. Adequate automatic fire and water detection and suppression capabilities are assumed to be present. Reduction of human injury is the first priority, followed by saving other important assets. Emergency drills that enact the documented procedures should be periodically held. It should be assumed that occupants of an area in which an emergency occurs do not have time to read emergency procedures documents before action. Procedures should include activation of manual alarms and power shutoff switches, evacuation routes, reporting of conditions, safe areas for regrouping, accounting for all occupants, use of equipment such as fire extinguishers to aid safe evacuation, and actions following complete evacuation. A hierarchy of emergency commands should be established with backup assignments. Emergency drills should be organized to minimize loss of critical activities such as computer operation. Close supervision of drills by managers who are aware of practice or real emergencies is necessary. Large, clearly visible signs providing basic directions are required. For example, locations of fire extinguishers, portable lights, and emergency switches should clearly be identified with signs that can be read from likely positions of occupants. Firstaid kits should be available in regrouping areas. Emergency food, water, tools, waste disposal, waterproof equipment covers, communication and sleeping supplies should be available for prolonged emergencies. All civil ordinances and insurance policy requirements must be met.

4. Variables: Frequency and extent of drills and briefings, content and location of written procedures, manual alarms and switches, evacuation routes and regrouping areas, signs, command assignments, amount and locations of emergency equipment.

5. Strengths: The safety of occupants from injury is the primary purpose of this control. Employees will have more positive feelings about their employer's concern for their welfare, and alertness to potential emergencies is maintained.

6. Weaknesses: Drills can become too commonplace and not taken seriously. Emergency equipment and supplies can deteriorate. Written procedures become obsolete. Emergency switches can be accidentally or maliciously activated.

7. How to Audit: Observe drills, review written procedures, check signs and equipment.

8. Purpose: Prevention

9. Control Area: Computer center

10. Mode: Manual procedures, hardware

11. Area of Responsibility: Computer security, operations

12. Cost: Medium

13. Principles of Note: Override capability, completeness and consistency, acceptance by personnel, sustainability.

1. Control Title: Security for Sensitive Areas during Unattended Periods

2. Objective: To avoid destruction of assets and business interruption.

3. Description: Sensitive areas during unattended time should be made physically secure with locked doors, significant barriers, and automatic detection devices for movement or natural disaster losses. Periodic inspection by guards and closed-circuit TV monitoring are also important. In addition, sensitive areas not generally visible to others should never be occupied by a lone employee for safety and prevention of malicious acts. Some computer-related work areas such as the computer room are occupied by employees at all times. Other areas and some computer rooms are left unattended for varying periods of time from several hours per day to only 1 or 2 days, such as holidays, each year. Safeguarding when employees are present and not present represents significantly different security requirements.

4. Variables: Detection and suppression equipment (vendors of equipment can assist in selection), guard inspections, periods of unattended time.

5. Strengths: Adequate control of unattended areas will ensure consistency of security.

6. Weaknesses: Unattended sensitive areas are particularly vulnerable, and automatic monitoring may not be sufficiently comprehensive to cover all contingencies.

7. How to Audit: Auditors should periodically inspect unattended areas during times in which they are unattended.

8. Purpose: Detection

9. Control Area: Computer center

10. Mode: Manual procedures, hardware

11. Area of Responsibility: Security

12. Cost: Medium

13. Principles of Note: Universal application, completeness and consistency, instrumentation.

1. Control Title: Areas Where Smoking and Eating Are Prohibited

2. Objective: Avoid destruction of assets and business interruption.

3. Description: Smoking and eating are not permitted in computer equipment areas. Prevention requires signs, written policy, enforcement, and penalties rigorously applied. In addition, personal grooming to eliminate long hair and loose clothing should be voluntarily practiced to avoid interference with moving parts of peripheral equipment and personal injury.

4. Variables: Designated areas, signs, policy.

5. Strengths: In addition to obvious benefits, prevents smoke detection and water detection alarms from being triggered unnecessarily; also increases worker productivity somewhat.

6. Weaknesses: Poses an inconvenience for employees; may require the establishment of a separate lounge area. If lounge area must be outside the security perimeter around the computer room, physical access to the computer room may be compromised. Heavy smokers may not be able to work in this environment. Disciplinary measures will need to be defined and enforced.

7. How to Audit: Observation that this policy is actually being followed.

8. Purpose: Prevention

9. Control Area: Computer center

10. Mode: Policy

11. Area of Responsibility: Operations

12. Cost: Low

13. Principles of Note: Acceptance by personnel.

1. Control Title: Minimize Traffic and Access to Work Areas

2. Objective: Prevent unauthorized access to sensitive areas.

3. Description: Employee and vendor work areas and visitor facilities should be located to minimize unnecessary access. Persons should not have to pass through sensitive areas to reach work stations. Sensitive functions should be placed in low traffic areas. Traffic points through security perimeters should be minimized. Employee convenience facilities such as lavatories, lounges, lockers, and food and drink dispensers should be located to minimize traffic through barriers and sensitive areas. Toilets outside of security perimeters, such as in lobby and receiving areas, are essential. Areas with many work stations should be separated from areas with few work stations. For example, computer peripheral equipment requiring human operation should be in rooms separate from computer equipment requiring little human attention.

   Access authorization should be granted on a privileged basis. Three access levels can be granted: general, limited, and by exception. General access is granted to those whose work stations are in a restricted area. In a computer room this includes computer operators, maintenance staff, and first-level supervisors. Limited access is granted for specified periods of time to those responsible for performing specified preplanned assignments, such as auditors, security personnel, and repair or construction crews. Finally, exceptions can be made in emergencies as long as those having access are escorted and after which extraordinary measures are taken to ensure integrity of the area. Application programmers no longer need access to computer rooms except on an emergency basis. Systems programmers need access on a limited basis. Visitors should be restricted entirely from computer rooms unless by exception and are accompanied by a high-level manager who explicitly accepts responsibility and is personally accountable. Other sensitive areas, such as programmers' offices, job set-up areas, and data entry work areas, should be similarly restricted to authorized access. Signs identifying limited access areas should be posted, and rules should be strictly enforced.

4. Variables: Functional relationships of computing activities, work assignments, logging accesses, building constraints, worker efficiency, space size requirements, security level differentials, and assets values.

5. Strengths: Unauthorized physical access is one of the greatest security vulnerabilities and is effectively reduced by careful placement of computing activities. Potential for criminal collusion is reduced. In addition, worker efficiency and productivity can be increased when interaction and communication among employees engaged in different activities are not essential. The number of security officers can be decreased.

6. Weaknesses: Employees and managers may resent restricted movement. Reduced interaction and communication among creative people may reduce their performance.

7. How to Audit: Observe traffic and work areas, study functional relationships, and perform traffic analysis.

8. Purpose: Deterrence, prevention

9. Control Area: Computer center

10. Mode: Hardware

11. Area of Responsibility: Security, management

12. Cost: Low

13. Principles of Note: Least privilege, minimization of exceptions, accountability, sustainability.

1. Control Title: Physical Access Barriers

2. Objective: Prevent unauthorized physical access to sensitive areas.

3. Description: Physical access through a security perimeter from a less sensitive area to a more sensitive area or between areas where different privileges apply must be limited to as few openings as possible. The remaining barrier between openings should be made of sufficiently sturdy materials to resist entry. Openings should have entrance controls consisting of one or more of the following methods.

   - o Sign in/out log
   - o Challenge of unauthorized entry by authorized persons
   - o Challenge access by posted signs
   - o Mechanically or electrically locked doors
   - o Guards (local or remote using CCTV)
   - o Mantrap (double) or turnstile doors.

   In computer centers, limited access should be maintained for all areas except public entry lobbies, lavatories, lounges, food areas, and all areas outside of the outermost security perimeter. There should be a central administration of access throughout a computer center. Procedures must be documented and include exception condition procedures. Emergency exit doors must be provided for safety and to comply with ordinances and insurance requirements.

4. Variables: Location of access, type of access constraints, authorization procedures, logging accesses, strength of barrier materials.

5. Strengths: Access control prevents unnecessary movements of people as well as unauthorized accesses for security purposes. The practice of a secure procedure for gaining access maintains a vigilance and security awareness among authorized persons. It also discourages malicious persons.

6. Weaknesses: Controls reduce efficiency. There is a danger of mismatching stringency of controls and actual needs. Sustaining adequate levels of effectiveness is difficult unless automatic barriers are used.

7. How to Audit: Frequent testing by making unauthorized access attempts (without force) and challenging a sample of persons in limited access areas should be done.

8. Purpose: Prevention

9. Control Area: Computer center

10. Mode: Manual procedures, hardware

11. Area of Responsibility: Security

12. Cost: Medium

13. Principles of Note: Least privilege, override capability, completeness and consistency.

1. Control Title: Remote Terminal Physical Security

2. Objective: Prevent unauthorized access to sensitive areas.

3. Description: Physical access barriers, accountability for use, and resistance to visual and electromagnetic monitoring of terminals and local communication loops are maintained and periodically reviewed consistent with security of the computer system being used from the terminal. Terminals are frequently owned or are under the control of computer users and often do not come under the jurisdiction of computer centers supplying services. Therefore, this control is directed to users or indirectly to computer center employee functions as liaison to terminal users and has the authority to disallow system access from any terminal where acceptable controls are not in place. Signed agreements are used to enforce the requirements. Resistance to visual or electromagnetic monitoring can include line-of-sight barriers to prevent reading of displays from a distance and placing terminals sufficiently removed from a security perimeter so that electromagnetic emanations would be costly to monitor. Securing of work papers and terminal media should also be ensured. Locks on terminals, clearing of work areas after use, and bolting of terminals to fixed objects might be considered.

4. Variables: Barriers, usage logging, distance to security perimeter, control of visual media, terminal locking mechanisms, mechanisms to prevent removal of equipment.

5. Strengths: Security consistency can be maintained over all system use. Losses are probably more likely to occur around terminals and during usage because people in positions of trust concentrate at terminals. Security reviews by computer center security staff facilitate independence and objectivity.

6. Weaknesses: Cost of security, remoteness, and informal environments make controls difficult to maintain. Portable terminals increase difficulty of security.

7. How to Audit: Review remote terminal inspection reports. Examine usage logs at terminals and compare with system-produced logs. Conduct surprise audits at selected sites where problems are reported.

8. Purpose: Detection, prevention

9. Control Area: Computer center (and its extensions)

10. Mode: Manual procedures

11. Area of Responsibility: Computer users

12. Cost: Medium

13. Principles of Note: Least privilege, completeness and consistency.

1. Control Title: Universal Use of Badges

2. Objective: Prevent unauthorized access to sensitive areas.

3. Description: To control access to sensitive data processing facilities, all persons are required to wear badges. Different color badges including photos in some cases are used for employees, visitors, vendor representatives, and those employees requiring temporary badges (used when employees have forgotten or lost their badge). All persons are required to wear their badges in conspicuous places on their person; visitors and in some cases everybody could be required to leave an item of identification such as a driver's license at the front desk when they are issued a badge. The decision to require badges depends on business practices, numbers of people, amount of traffic, and other access controls in use. For two or three people in an area with little traffic, the need for badges in that area may be precluded. However, minimization of exceptions may warrant their use. Positive badge administration is essential. Disciplinary action should result from infractions of the rules.

4. Variables: Type of badges, administration, use of card keys, areas and people affected.

5. Strengths: Quick visual inspection should allow management, auditors, and others to determine whether someone is authorized to be in sensitive areas and if so, what their status is. Badge color codes can also designate work areas. Unauthorized parties are prevented from gaining access and causing harm (violating someone's privacy, causing damage to expensive equipment, harming employees, etc.). Separation of duties and unnecessary visiting restrictions are strengthened when badges restrict the movement of employees within data processing facilities.

6. Weaknesses: Unless universally and continuously enforced, this procedure may provide little security.

7. How to Audit: Visually check the use of badges and the extent to which they control access to restricted areas. Examine logs of visitors to make sure that proper badges were issued, that proper records (time in, time out, name, badge number issued, etc.) are kept.

8. Purpose: Prevention, detection

9. Control Area: Computer center (and its extensions)

10. Mode: Manual procedures

11. Area of Responsibility: Security

12. Cost: Medium

13. Principles of Note: Override, overt design and operation, least privilege, universal application, instrumentation, minimization of interruptions.

1. Control Title: Alternative Power Supply

2. Objective: Avoid destruction of assets and business interruption.

3. Description: A power supply independent of the public utility source for uninterrupted service is provided by batteries charged from public utility power providing a few minutes of independent power or by an independent power source such as a diesel generator for longer durations. An alternative source of energy, such as a diesel generator without batteries but with adequate power quality regulators, can be used when uninterrupted service is not important, but long durations of outage are harmful. This control is needed only where power is sufficiently unreliable relative to the seriousness of computer failure or unavailability. The location, environment control, and access security are important to ensure integrity of the alternative power equipment and fuel. Periodic full tests are important for maintenance. Some organizations use the independent source as the primary supply and the public utility as a backup. One organization has located a new computer center at a site between two public electric power grids and obtains power alternatively from both to reduce the likelihood of public power failure.

4. Variables: Type and size of alternative supply, switching equipment, location of equipment and fuel, computing equipment and facilities to be supported, testing frequency.

5. Strengths: Electrical damage to computer equipment and loss of data can be prevented with uninterruptable power supplies.

6. Weaknesses: The cost may be prohibitive for large systems.

7. How to Audit: Auditors should require a demonstration of alternative supply use. An independent power engineer should be called in for periodic inspections. Fuel supplies should be checked periodically for supply levels, quality, and safety.

8. Purpose: Recovery

9. Control Area: Computer system

10. Mode: Hardware

11. Area of Responsibility: Computer security

12. Cost: High

13. Principles of Note: Limit of dependence on other mechanisms, sustainability.

1. Control Title: Delivery Loading Dock Access

2. Objective: Avoid destruction of assets and business interruption.

3. Description: The loading dock area is made secure with the use of a window and an intermediate holding room. The window is used by truck drivers when they wish to speak to someone from the facility, have receiving papers signed, and gain authorization for access to the intermediate holding room. An employee from the inside can release the lock on a door opening on the loading dock from the holding room. The truck driver can then unload supplies or other items onto the dock and into the holding room without having access to any other areas of the building. When the delivered material is entirely within the holding room, and when the delivery man has gone, the outside door can again be locked by the employee at the receiving window. Then an inside door leading to the holding room can be unlocked and opened for the movement of the material to its proper storage/use location.

4. Variables: Facility layout, staffing in area, volume of materials.

5. Strengths: Prevents unauthorized persons from gaining access to facilities through the loading area. Allows receiving clerk to stay physically separated from the driver/delivery men (employee safety is the concern here). Permits received materials to be inspected in a locked room prior to movement to operational and storage areas of a data processing center. A bell at the receiving window can be used to summon a clerk, thus eliminating the need for the window to be manned on a full-time basis.

6. Weaknesses: Holding room may take up a large amount of floor space, which could be used for other purposes. Receiving window, related doors and locks, plus additional walls incur additional costs. Only large data processing centers may have the volume of deliveries to justify such an expenditure.

7. How to Audit: Examine facilities to make sure that the appropriate loading dock access controls are in place. On a surprise basis, watch a delivery to make sure that specified procedures are being followed.

8. Purpose: Prevention

9. Control Area: Computer center

10. Mode: Manual procedures, hardware

11. Area of Responsibility: Security, operations

12. Cost: High

13. Principles of Note: Simplicity, least privilege, independence of control and subject, universal application, sustainability.

1. Control Title: Separation of Equipment

2. Objective: Prevent damage to equipment.

3. Description: Different types of computer equipment (central processors, disk drives, tape drives, communications equipment, printers, power supplies, tape libraries, terminals, consoles) each require different environments for optimum operation and different numbers and types of people in attendance. Therefore, they should be placed in different rooms with appropriate separation walls, distances, and accesses. For example, printers create dust and vibration from paper movement and should be separate from disk and tape drives that are sensitive to air quality and vibration. Central processors are normally unattended and should be in a low traffic environment.

4. Variables: Equipment configurations, size of spaces available, traffic patterns.

5. Strengths: Reduces repairs, avoids excessive environment and traffic controls.

6. Weaknesses: Increases expenses of facilities changes when new equipment is acquired.

7. How to Audit: Participate in facilities design. Review usable space.

8. Purpose: Prevention

9. Control Area: Computer center

10. Mode: Hardware

11. Area of Responsibility: Computer security, operations

12. Cost: High

13. Principles of Note: Simplicity, sustainability.

Selective
Fore of Law, High Traffic

1. Control Title: Inspection of Incoming/Outgoing Materials

2. Objective: Prevent unauthorized taking and facility damage.

3. Description: Certain materials and containers are inspected, and entry or departure is restricted. Within constraints of all applicable laws and personal privacy, guards would prevent movement of materials and inspect contents of closed containers into and out of sensitive areas. Materials may include tapes, disks, listings, equipment, recorders, food and beverages, chemicals, and such containers as lunch boxes and briefcases. Some unneeded materials could be kept stored outside for later retrieval by owners. Authorization forms may be used to control movement. Spot checks and posted signs rather than continuous inspection may be sufficient.

4. Variables: Materials, authorization, degree of inspection.

5. Strengths: Prevents unnecessary or dangerous materials from entering areas. Reduces suspicion of otherwise trusted persons. Reinforces restrictions or unauthorized persons.

6. Weaknesses: May reduce employee efficiency and freedom.

7. How to Audit: Observe inspection post activity. Attempt violation of rules (with great care).

8. Purpose: Prevention

9. Control Area: Computer center

10. Mode: Manual procedures

11. Area of Responsibility: Security

12. Cost: High

13. Principles of Note: Consistency and completeness, sustainability, acceptance by personnel.

1. Control Title: Isolation of Sensitive Computer Production Jobs

2. Objective: Prevent compromise of data.

3. Description: Some production systems, such as those producing negotiable instruments or processing personal information (as in organized crime intelligence files) are sufficiently sensitive to potential loss to require special handling. Such systems should be run on dedicated computers or only share computer systems with harmless or other trusted applications. For example, data communications access might be shut down during such a job. Some sensitive systems may be run at times when general activity is minimal, such as on Sundays, and run by an operations team especially held accountable for the operation. Extraordinary physical and computer security measures may be taken during the job run. Special marking may be done of all materials used.

4. Variables: Selection of sensitive applications, operational circumstances during job runs, operations staff selection, identification of materials used.

5. Strengths: Concentration of security resources is possible. Minimizes exposures to sources of loss. May increase operational efficiency.

6. Weaknesses: May introduce inefficiencies in scheduling production. Targets for compromise become obvious.

7. How to Audit: Rank and compare sensitivities of all production jobs. Observe special production runs and check on compliance with documented procedures.

8. Purpose: Deterrence, prevention

9. Control Area: Computer center

10. Mode: Manual procedures

11. Area of Responsibility: Operations

12. Cost: High

13. Principles of Note: Least privilege.

1. Control Title: Protection of Data Used in System Testing

2. Objective: Prevent compromise of data.

3. Description: Application and test programmers usually need test data to develop, debug, and test programs under development. In some cases, small amounts of fictitious test data can be generated independent of users and production data. However, many application programs require significant amounts of test data that are exact copies of a full range of production data. Test data are frequently obtained as samples or entire files of production input data currently being used or recently used for the application being replaced or as output from other preprocessing computer programs. There is sometimes significant exposure by providing real, current production data to programmers. Often data can be obtained from obsolete production input data files, but in some cases even these data may be confidential. Customers for whom production programs are being developed should be made aware of the exposure problem, and advice and assistance should be obtained in producing test data in the least confidential but expedient manner. Sensitive test data should be treated with the same care as equivalent production data. In any case, development and test programmers should not be given access to real production files in a production computer system except in the case of emergency and then under highly controlled conditions.

4. Variables: Selection of test data procedure, physical and logical handling of test data.

5. Strengths: This control can greatly reduce the exposure of an organization to a wide range of errors, omissions, and intentional acts. It also imposes a beneficial discipline on development and test computer programmers.

6. Weaknesses: Providing separate test data may be particularly expensive and not necessary in every case. Good decisions require the knowledgeable participation of customers for whom computer programs are being developed. This is sometimes difficult to obtain. Test data may also not be sufficiently representative. Production runs masquerading as test runs to expedite work is a possible problem.

7. How to Audit: Auditing requires a detailed knowledge of programming and testing practices and detailed observation of the software development life cycle.

8. Purpose: Prevention

9. Control Area: Operations

10. Mode: Manual procedures

11. Area of Responsibility: Development

12. Cost: Medium

13. Principles of Note: Least privilege.

1. Control Title: Correction and Maintenance of Production System

2. Objective: Protect against unauthorized program or data modifications.

3. Description: In spite of implementation and strict enforcement of security controls and good maintenance of application and systems programs, emergencies arise that require violation or overriding of many of these controls and practices. Occasionally, production programs will fail during production runs on the computer. This may happen on second and third shift during periods of heavy production computer activity. If a failure occurs in a critical application production run, it is frequently necessary to call upon knowledgeable programmers to discover the problem, make a change in the production computer program, make changes in input data, or make decisions about alternative solutions (e.g., reruns using previous versions of the production program). When such emergency events occur, all necessary and expedient measures must be taken, including physical access of programmers to computer and production areas, access by such programmers to data files and production programs, correction of production programs, and ad hoc instructions to operations staff. During any of these activities, it is necessary for a trusted individual in computer application production work to record all of the events as they occur or shortly thereafter. Following the termination of the emergency, programmers should be required to make the necessary and ordinary permanent changes that may have been made on a temporary basis during the emergency and document the emergency actions. This usually requires updating and testing production programs and the normal process of introducing tested updated programs for production use. After an emergency and before permanent corrections have been made, the production application program should be treated in a suspicious mode of operation requiring increased levels of observance by users, production staff, managers, and possibly EDP auditors. These extra efforts should continue until confidence has been built up in the production activities through acceptable experience.

4. Variables: Emergency maintenance procedures, documentation of actions, past recovery procedures.

5. Strengths: Flexibility in handling emergency production situations and having security-related procedures and continuing levels of security at highly vulnerable times is important.

6. Weaknesses: Providing a formal method of handling emergency repair may encourage the excessive use of emergency repair procedures.

7. How to Audit: This control should be audited during emergency work periods by assigning EDP auditors to oversee emergency procedures and production work using patched computer programs. The basis of decisions to make emergency repairs should be examined for correctness and consistency.

8. Purpose: Recovery

9. Control Area: Computer center

10. Mode: Manual procedures

11. Area of Responsibility: Operations

12. Cost: Medium

13. Principles of Note: Override, least privilege, accountability.

1. Control Title: Computer User Trouble Calls Logging

2. Objective: Prevent overlooked security problems and detect potential adverse side effects of changes to computer systems and other elements of the operating environment.

3. Description: All calls from users and staff regarding problems with a computer and communications system are logged detailing the caller's name, the time and date, and the nature of the problem. A brief disposition report is then prepared for each problem report. A manager reviews each of the problem disposition reports to determine that the problem has been satisfactorily resolved and also to determine that there are not any adverse impacts of the solutions provided (e.g., a correction of the operating system may have some side effect with a security or privacy implication). The reviewing manager also determines whether or not the responding operating person taking care of the problem was within bounds of authority. Simple requests for information are not considered problems within this procedure.

4. Variables: Logging assignments, forms design, review process.

5. Strengths: This practice forces user and staff liaison people to justify their actions and to document each correctional action that they have taken. The log can be analyzed by performance monitoring and by system development people for possible improvements of the current operating environment.

6. Weaknesses: Preparation of logs and brief reports is time consuming and takes talented and knowledgeable people away from their other duties. Users may abuse the problem reporting system whenever they wish to get operation management's attention.

7. How to Audit: Review a sample of logs detailing all problem reports received. Examine problem disposition reports. Interview managers who review the disposition reports.

8. Purpose: Prevention, detection

9. Control Area: Data center

10. Mode: Manual procedures

11. Area of Responsibility: User (responsibility to report problems); operations.

12. Cost: Medium

13. Principles of Note: Instrumentation, accountability, auditability.

1. Control Title: Independent Control of Audit Tools

2. Objective: Prevent interference with auditing.

3. Description: Audit programs, documentation, and test materials are kept in secure areas by the internal auditors. Audit programs do not remain in the data center tape library. The audit programs are not kept on disk or in any other way kept on the system where they might be subject to tampering.

4. Variables: Storage area, materials stored, auditors accountable.

5. Strengths: Preserves independence of auditors.

6. Weaknesses: It may be inconvenient for auditors to keep their materials in a secure place. An installation may have a policy that no tapes are to leave the tape library unless they are to be transferred to another computer center; this practice would then require exceptions to such rules.

7. How to Audit: Ascertain that all audit materials are maintained under the direct control of auditors, not the persons being audited.

8. Purpose: Prevention

9. Control Area: Computer center

10. Mode: Manual procedures

11. Area of Responsibility: Audit

12. Cost: Low

13. Principles of Note: Independence of control and subject, least privilege.

1. Control Title: Limited Use of System Utility Programs

2. Objective: Prevent unauthorized program or data.

3. Description: Most computer installations have one or more system utility programs capable of overriding all or most computer system and application controls. In some computer installations, one such computer program is called Superzap. In one large computer installation, five such utility programs were found. These programs should be controlled by password or kept physically removed from the computer system and the program library and physically controlled so that they are available only to a limited number of trusted, authorized users. Occasionally, if the programs are made available on-line, they can be protected by special passwords required for their use. Changing the name or password frequently is another way to better safeguard these on-line programs.

4. Variables: Utility programs in use, residence of utility programs, operating system features.

5. Strengths: Limitation of availability of system utility programs forces programmers to use more accepted means of accomplishing their purposes that can be more safely done under the controls of the system.

6. Weaknesses: Limitations in the use of existing utility programs may encourage programmers to develop their own programs that are not under the same controls as the utility programs.

7. How to Audit: Operational audits should include the examination of physical and internal computer control of utility programs.

8. Purpose: Prevention

9. Control Area: Programming and maintenance

10. Mode: Manual procedures, computer operating system

11. Area of Responsibility: Operations

12. Cost: Low

13. Principles of Note: Override, least privilege.

Selective
High Tape Usage

1. Control Title: Tape Management Avoiding External Labels

2. Objective: Prevent loss, modification, or destruction of data assets.

3. Description: A tape management system can be used to keep track of all tapes using a serial number appearing on the tape reel. Serial numbers may contain storage rack location information as well as a serial number. Operators handling the tapes do not know the contents of the tapes because the identity of the data set owner, creation and update dates, data set names, and like information are recorded only on internal (machine readable) labels. The software package for managing tapes contains an index of serial numbers and the corresponding label information. An up-to-date copy of the index relating serial numbers and tape information is maintained at off-site storage location(s).

4. Variables: Tape management system, volume of routinely processed tapes, special handling.

5. Strengths: Provides operators with no more information than is necessary to do their jobs, thus preventing potential abusive acts that were made possible because these data were available to the operators. Operators are presented only with a request to mount, dismount, etc. certain tapes with provided serial numbers. Reduces operator errors associated with mounting the wrong version of a data set, the wrong user, etc. A tape management system can be used to monitor operator performance as well as control the tape library. Persons in the tape library or machine room cannot learn the nature of the data on a tape simply by examining the reel.

6. Weaknesses: Lack of functional labels may increase errors.

7. How to Audit: Trace the steps taken to mount and dismount a tape reel from the initiation of a request to the actual performance by the operator. Examine data available to the operator to determine that confidentiality is not lessened by unwarranted exposures.

8. Purpose: Prevention

9. Control Area: Computer center

10. Mode: Computer operating system

11. Area of Responsibility: Operations

12. Cost: Medium

13. Principles of Note: Cost effectiveness, simplicity, least privilege, independence of control and subject, instrumentation, sustainability, auditability.

1. Control Title: Separation of Test and Production Systems

2. Objective: Prevent loss, modification, disclosure, or destruction of data assets.

3. Description: When an organization is large enough to have need for more than one computer, there is a distinct advantage to limiting the development and test to one computer system and production work to another computer system. Further separation of activities can also be achieved by using multiple production systems and even multiple test systems where each application is run on a separate computer system. Likewise, each group of programmers could do testing on separate computer systems. The cost benefits of large size and high memory capacity would be lost, but applications could be more nearly matched to the appropriate size of computer and memory. Compilers may be moved to the test system.

4. Variables: Size of test and production workloads, available computers, location of development staff.

5. Strengths: Separation of systems reduces the possibility of accidental or intentional programmed access to production files and programs. It separates the duties of operations staff from development staff and reduces the likelihood of system crashes on the production system. The data processing organization can orient the systems configurations and mode of operation to that of the specific purpose of the system. This also forces a more formal approach to the movement of test systems to the status of production systems. The test computer can also provide backup for production computers.

6. Weaknesses: The increased complexity of operating more than one computer for different purposes increases other loss exposures. Operating systems and configurations will require compatibility.

7. How to Audit: This control can be audited to ensure that the production system is not being used for test or programming development purposes and that the test system is not being used for production purposes by examining usage logs and sampling output reports and the use of output.

8. Purpose: Prevention

9. Control Area: Computer center

10. Mode: Policy

11. Area of Responsibility: Operations, development

12. Cost: High

13. Principles of Note: Control and subject independence.

1. Control Title: Contingency Recovery Equipment Replacement

2. Objective: Recover from business interruption.

3. Description: Commitments should be obtained in writing from computer equipment and supplies vendors to replace critical equipment and supplies within a specified period of time following a contingency loss. Some vendors will commit to replacement of their products within a reasonable period of time and will specify that period of time as a commitment. For example, in one computer installation a vendor agreed to replace a central processor within 5 days and a second processor, if necessary, within 10 days. The paper forms supplier agreed to deliver a two-week supply of all special forms in the same time frame. In contrast, other vendors wuld not guarantee replacement times but would only indicate that best efforts would be provided. This usually means that the next available equipment within the vendor company inventory would be provided with a priority over other normal product deliveries. Emergency ordering procedures should be established as part of a contingency recovery plan.

4. Variables: Willing vendors, delivery time constraints, content of binding letters of agreement.

5. Strengths: Vendor commitments provide a means of planning alternative data processing until equipment and new computing capabilities have been restored.

6. Weaknesses: The legal value of vendor commitments is not known. A payment in return for commitments may be required. A false sense of security may be produced because other contingencies may interfere with vendor commitments.

7. How to Audit: Auditors should periodically confirm the validity of agreements to be sure that they are still in effect. Agreements should be reviewed with legal counsel. Commitment periods should be checked relative to other contingency recovery plans.

8. Purpose: Recovery

9. Control Area: Computer center

10. Mode: Policy

11. Area of Responsibility: Management

12. Cost: Low

13. Principles of Note: Sustainability, accountability.

1. Control Title: Computer Systems Activity Records

2. Objective: Detect unauthorized system use.

3. Description: Most computer systems produce a number of system activity logs, journals, and exception reports. Such recordings should be periodically and selectively examined both manually and through automated means looking for key indications of possible unauthorized activities. Such recordings on tape, disk, and sometimes paper listings should be archived for a reasonable period of time, and records should be kept to ensure that no reports are missing. For example, printed console logs should be on continuous forms. Any breaks in the forms should require signatures indicating integrity of operation and no missing pages. In one computer installation the console logs are examined on a sample basis monthly. All logs should be dated and timed with an indication of operational personnel on duty at the time the logs were produced. It may be necessary to keep manually written logs of some computer operation activities to compare with or complete the automatic logging of system activity.

4. Variables: Types and contents of activity recordings, mode of recording and archiving of records, archive cycling periods, analysis methods and frequency.

5. Strengths: Activity records may be important for evidence in litigation and insurance claims. Accountability of employees can be better assured. Recovery from contingencies can be facilitated.

6. Weaknesses: Large amounts of systems resources may be consumed in the recording and analysis. Large volumes of data may discourage manual inspection.

7. How to Audit: Periodic sampling and evaluation of recordings should be performed. Recordings represent an important audit trail for auditing various applications and computer usage.

8. Purpose: Detection

9. Control Area: Computer system

10. Mode: Computer operating system, computer application systems, manual procedures.

11. Area of Responsibility: Computer security, operations

12. Cost: Medium

13. Principles of Note: Control and subject independence, completeness and consistency, instrumentation, accountability.

Baseline

1. Control Title: Minimizing Numbers of Copies of Sensitive Data Files and Reports

2. Objective: Prevent loss, modification, disclosure, or destruction of data assets.

3. Description: The number of copies of sensitive tape, disk, or paper files should be minimized. Destruction dates should be specified and destruction instructions followed. It may be advisable to destroy most paper copies of files on the basis that the information can be retrieved and reprinted from computer media when necessary. This is based on the concept that files stored in computer systems and computer media are generally often more secure than on paper. Normal backup procedures often require that several copies of computer media files be made and stored at different sites. However, some files may be so sensitive that numerous copies in different locations may contribute seriously to their exposure. As many as 20 to 30 copies of computer-stored files may be produced in a single year in a large computer installation. The organization primarily accountable for highly sensitive information should have control and logs of all copies and their locations. Adequate backup must be balanced with the exposure danger of multiple copies and backup procedures.

4. Variables: Selection of data for special copy control, copy logging procedures, dating for destruction, assignment of responsibilities and accountability.

5. Strengths: Reduction in storage space and orderliness of facilities may be enhanced.

6. Weaknesses: Retention of minimum numbers of copies of records may weaken the backup capability.

7. How to Audit: Selective examination of storage areas looking for sensitive records and comparing to logging forms should be done periodically.

8. Purpose: Prevention

9. Control Area: Computer center

10. Mode: Manual procedures

11. Area of Responsibility: Operations, input/output, computer users

12. Cost: Low

13. Principles of Note: Simplicity, least privilege, completeness and consistency, accountability.

1. Control Title: Data File and Program Backup

2. Objective: Prevent loss, modification, disclosure, or destruction of data assets.

3. Description: The current form of every data file that may be needed in the future should be copied at the time of its creation, and the copy should be stored at a remote, safe location for operational recovery purposes. It may be advisable to store several copies, one immediately available in the computer center, another available some short distance away, and a third archived at some remote distance for longer term storage. Periodically updated data files should be cycled from the immediate site to the local site to the remote site by data file generations (father, grandfather, etc.). In addition, copies of the computer programs necessary to process the backed-up data files, documentation of the programs, computer operation instructions, and a supply of special printed forms necessary for production running of the programs should also be stored at a remote, safe location. This hierarchical arrangement of backup data files provides for convenient restarting of production runs in case of damaged or missing files. More serious problems that could result in loss of local backup data files can be resolved by using copies of remote backup data files. When a backup file is returned to the computer center for use, there must be assurance that it also is backed up safely with another copy.

4. Variables: Data files to be backed up, higher hierarchical arrangement in locations of backup files, cycling frequency and methods, archivable recordkeeping, security of backup facilities.

5. Strengths: Defensive depth of backup provides significant increase in assurance of recovery that addresses small as well as large contingencies. Recovery from backup files is commonly done under abnormal conditions that usually accompany recovery efforts. These conditions increase the likelihood of loss of the backup files. Therefore, it is important to have at least secondary backup in addition to primary backup files.

6. Weaknesses: Operational complexity in moving backup files from one stage to the next at a multiplicity of backup sites may increase the opportunity for human errors or intentional acts of sabotage or theft. Multiple backups may produce complacency and cause degeneration of computer center procedures. There is an increased exposure to loss in transporting files to the remote sites.

7. How to Audit: An audit should periodically include the actual demonstration of recovery from each level of backup. Inspection of backup sites should be conducted to ensure their secure states.

8. Purpose: Recovery

9. Control Area: Computer center

10. Mode: Manual procedures

11. Area of Responsibility: Operations

12. Cost: Medium

13. Principles of Note: Defensive depth sustainability.

1. Control Title: Disaster Recovery

2. Objective: Recover from business interruption.

3. Description: Every computer center must have a written disaster recovery plan and a recovery management team. Primary and backup managers must be assigned specific responsibilities for each aspect of recovery from all types of partial or complete disasters. Each aspect of the disaster recovery plan should have assigned a specific individual responsible for its execution. Separate individuals should be assigned to coordination, systems support, hardware recovery, facilities, administration, scheduling, communications, documentation and supplies, backup data files and security recovery funding, insurance, personnel, historical recording of events, and public affairs. Priority processing needs of all time-dependent applications to be recovered after a disaster must be identified. This requires that all computer users specify the importance of their computer applications, processing requirements and alternative means of processing, and consequences of failure to process. Data processing management is responsible for meeting the critical needs of computer users in the best interests of the organization. Priorities will assist in the scheduling of processing when it is restored. A designated person should provide liaison with users informing them of special needs and the status of processing of their work. A detailed history of the recovery process must be documented and recovery activity verbally reported during the recovery process. After recovery, the historical documentation should be analyzed to determine how future contingencies may be better handled and to handle insurance claims recovery and any litigation that may follow a disaster. Every job function should be analyzed relative to its performance during and prior to a disaster. Measures of criticality and priority of functions should be determined and documented in the plan.

4. Variables: Identification of anticipated disasters, applications and their priority for recovery, staff assignments, disaster and recovery plan, type of data processing backup site, documentation and distribution, identification or arrangement of alternatives, data processing capabilities during recovery, and arrangements for alternative services, such as communications, transportation, security guards, equipment, supplies, facilities, and personnel.

5. Strengths: Flexibility in plans facilitates meeting a wide range of contingencies. A documented recovery plan provides for a means of practicing and testing all recovery procedures. Potential threats that can provide a means of adding controls to reduce risk may be identified. Prioritizing applications provides users with perspective on the importance of better applications recovery needs. Application of limited data processing resources can be more effectively planned. Communication among recovery managers helps ensure smooth and minimum cost recovery. Documentation of recovery activities encourages responsibilities and accountability among managers and workers. Job function analysis facilitates management's quick mobilization of critical personnel and resources in the event of a disaster. Management can more easily and effectively assign work to employees during recovery. A disaster plan reduces the likelihood of confusion. Use of a disaster recovery contact list provides for speedy notification of vendors, suppliers, and customers who can take appropriate action to assist or reduce loss.

6. Weaknesses: Documentation of a backup plan may produce complacency unless the plan is frequently reviewed and tested. Documented backup plans may also become quickly outmoded. Ranking of priorities of applications may cause ill will and disputes among computer users. The preparation of historical documentation may be distorted or incorrect and result in reduced capability to file loss claims with insurance companies or provide defense in litigation or governmental hearings. Documented recovery plans that have not been tested may quickly become too detailed or inappropriate for recovery.

7. How to Audit: Disaster recovery plans should be studied to ensure that they are still current. Proof of testing plans should be documented and reported. Scenarios of possible disasters can be generated and theoretically played against the disaster recovery plans to ensure their adequacy. Application priorities can be verified through auditors responsible for the audit of specific functions of an organization dependent on computer services. Examination of historical documentation recovery experience should be performed to note any changes necessary in disaster recovery planning for the future.

8. Purpose: Recovery

9. Control Area: Management

10. Mode: Manual procedures

11. Area of Responsibility: Management

12. Cost: High

13. Principles of Note: Simplicity, override capabilities, limit of dependence on other mechanisms, completeness and consistency, instrumentation.

1. Control Title: Electrical Equipment Protection

2. Objective: Prevent damage to equipment.

3. Description: Every item of computing equipment that is separately powered should have a separate circuit breaker in the electrical supply for that equipment. Alternatively, equipment may be supplied with other protective mechanisms from power failures or other electrical anomalies. Circuit breakers should be clearly labelled for manual activation. The locations of all circuit breakers should be documented and available in disaster and recovery plans.

4. Variables: Identified equipment, types of protective devices, assignments of acountability for activation, location, redundant transformers, documentation.

5. Strengths: Individual devices can fail and be switched off without having to cut power to other devices. Failures can be localized as well as more readily detected. Device configurations can be changed more readily, avoiding excessive time in diagnosing electrical problems and reconfiguring electrical systems to suit new equipment setups.

6. Weaknesses: Additional opportunity to tamper with equipment is possible.

7. How to Audit: Electrical switch boxes and circuit breakers should be periodically examined.

8. Purpose: Prevention

9. Control Area: Data center

10. Mode: Hardware

11. Area of Responsibility: Operations

12. Cost: Medium

13. Principles of Note: Override capability, limit of dependence on other mechanisms.

1. Control Title: Electrical Power Shutdown and Recovery

2. Objective: Prevent damage to equipment.

3. Description: Emergency master power-off switches should be located next to each emergency exit door. The switches should be clearly identified, and easily read signs should be posted giving instructions for use of the switches. Activation of any of these switches should be followed with reports documenting the circumstances and persons responsible for their use. Alternative power supplies should be available when data processing needs justify continuous operation, and they should be tested on a periodic basis. The power supply should be used during the test for a sufficiently long period of time to ensure sustained operation under emergency conditions. Fuel supplies for alternative power should be periodically measured, and the quality of the fuel tested. Pumps, switches, and valves for switching from alternative fuel tanks should also be periodically tested. In one computer installation having an uninterruptible power supply, two independent, separately located oil tanks are used. Either tank can independently supply the entire uninterruptible power supply. Each tank is filled by a different oil company. Two diesel generators and engines are also installed for backup purposes.

4. Variables: Number and location of master power-off switches, power-down and power-up operation instructions, frequency and extent of alternative power system testing, redundancy of power generators and fuel supplies.

5. Strengths: Easily identified power-off switches are valuable for firemen, rescue workers, and others in the event of emergencies. Testing facilitates preventive maintenance work and familiarizes staff with emergency procedures. Redundancies in alternative power supplies increase assurance of emergency recoveries.

6. Weaknesses: Unauthorized or accidental use of power-off switches can cause extensive damage to computer equipment and loss of data. Intentional use of power-off switches could assist in gaining unauthorized entry to computer facilities. Cutover to alternative power supplies may result in interruption of service and inconvenience to users. Redundancy increases the complexity of alternative power systems. This increases maintenance problems and likelihood of failures.

7. How to Audit: Periodically examine logs and question all switch activations. Ensure proper posting of identification and warning signs at switches. Observe testing of alternative power supplies and review testing logs. Review maintenance logs for excessive maintenance as an indication of possible problems.

8. Purpose: Prevention and recovery

9. Control Area: Data center

10. Mode: Hardware

11. Area of Responsibility: Operations

12. Cost: Medium

13. Principles of Note: Override capability, limit of dependence on other mechanisms, instrumentation, sustainability.

1. Control Title: Employees Identification on Work Products

2. Objective: Detect unauthorized activities of employees.

3. Description: All computer operators and other employees should have standard identification in the form of official names, numbers, or passwords. This identification is to be entered into all records, data input, and activity logs and journals to identify workers associated with all work products. Identification can be accomplished by manual signatures or keying of identification into equipment keyboards. Data entry clerks should be required to initial all forms or batch control forms used for data entry and enter identification into computer input data. Computer operators should sign computer console printer listings or enter their codes through console keyboards indicating the starting and ending of work periods.

4. Variables: Form of employee identification, entry of identification, manual verification of correct identification activity.

5. Strengths: Manual identification on forms can be compared with identification entered into computer systems to match times and work products. Incentives for higher quality and quantity of work are possible when work products are identified by individual worker. Tracking of errors and unauthorized activities is facilitated.

6. Weaknesses: Possible forgery can result in errors in accountability for unauthorized activity.

7. How to Audit: Spotchecking of employee codes with immediate supervisors. Sampling of computer output by audit trail back to source data handling.

8. Purpose: Detection, deterrence

9. Control Area: Computer center, applications systems

10. Mode: Manual procedures, computer application system

11. Area of Responsibility: Operations

12. Cost: Low

13. Principles of Note: Control and subject independence, least privilege, instrumentation, acceptance by personnel, accountability.

1. Control Title: Magnetic Tape Erasure

2. Objective: Prevent compromise of data.

3. Description: Computer centers should have magnetic tape erasure devices, commonly referred to as "degaussers," for the erasure of the contents of magnetic tapes. Such devices should be kept under strict control of the computer centers. Preferably, the device should be kept in a locked cabinet and authorized for use by selected individuals. The device should also be kept a significant distance away from magnetic tape storage areas. An erasure service should be offered to computer users, and an option for tape erasure should be made available on magnetic tape disposition forms providing a date upon which erasure should be performed. All magnetic tapes used for temporary storage (scratch tapes) should also be routinely erased before reuse. Dual control or separation of functions should be established to ensure that tapes containing valuable information are not mistakenly erased without authorization.

4. Variables: Location of equipment, procedure for use, erase disposition service.

5. Strengths: Routine erasure of tapes may prevent obsolete data from being used. Erasure of tapes can also be done at the time they are cleaned. High-speed degaussing devices, even when placed near magnetic tapes in storage, do not threaten magnetic media. A log can be used to record all degaussing.

6. Weaknesses: The ease with which large amounts of data can be lost requires great caution.

7. How to Audit: Examine documentation of procedures to erase sensitive information. Observe the handling of erasure activities.

8. Purpose: Prevention

9. Control Area: Computer center

10. Mode: Manual procedures, hardware

11. Area of Responsibility: Operations

12. Cost: Low

13. Principles of Note: Override capability.

Selective
Use of Couriers for Output Delivery

1. Control Title: Courier Trustworthiness and Identification

2. Objective: Prevent disclosure, taking, or unauthorized use of documents.

3. Description: Couriers are frequently used to distribute computer output reports to computer users. Couriers must be especially trustworthy, have a background investigation similar to that for computer operators, and be bonded. A new courier should be personally introduced to all those persons to whom he will be delivering computer output and to all persons from whom he will be receiving materials for delivery. Couriers should be required to use signed receipts for all transported reports. Couriers should be required to keep all reports in their personal possession in properly locked or controlled containers. All users should be informed immediately upon the termination of any couriers delivering or picking up reports. Couriers should carry special identification to show that they are authorized to function in claimed capacities. Telephone calls in advance of delivery of highly sensitive reports should be made to recipients of those reports.

4. Variables: Courier background investigations, identification procedures, design of receipt forms, delivery procedures, logging procedures.

5. Strengths: Procedures ensure positive accountability by receivers and senders of reports as well as couriers.

6. Weaknesses: Because couriers are generally low-paid employees, their potential for trustworthiness is reduced. Bonding of such employees is imperative.

7. How to Audit: Couriers should periodically be followed in their delivery work and be observed. Their activities should then be compared to receipt documents.

8. Purpose: Prevention

9. Control Area: Computer center

10. Mode: Manual procedures

11. Area of Responsibility: Input and output, computer users

12. Cost: Low

13. Principles of Note: Control and subject independence, limit of dependence on other mechanisms, instrumentation, accountability.

1. Control Title: Production Program Authorized Version Validation

2. Objective: Prevent unauthorized program or data modification.

3. Description: The authorized versions or copies of production programs, according to identifiers, are checked with a list of authorized copies and changes made to the production programs to determine that the version of a production program to be run is authorized. Update of the list is part of the ordinary maintenance process of production programs. Separate test and production program libraries are maintained.

4. Variables: Identifiers, procedures, exception handling.

5. Strengths: Prevents unauthorized versions of the production programs from being executed when used in conjunction with other related controls. Accidentally running a test version or an old version of a production program can be prevented and detected using this technique. Unauthorized versions of production programs can be similarly detected and prevented from being run.

6. Weaknesses: Requires that the list of authorized change dates and identifiers be protected from unauthorized changes. Adds additional complexity to the maintenance and production running procedures. The process may have to be disabled for recovery or emergency purposes.

7. How to Audit: Logs showing all exceptions (compile dates that do not match) should be examined regularly; additionally, it should be determined whether action has been taken to follow up on all instances where a match between the list of authorized versions does not match identifiers.

8. Purpose: Prevention, detection

9. Control Area: Computer center

10. Mode: Manual procedures

11. Area of Responsibility: Operations

12. Cost: Low

13. Principles of Note: Minimization of exceptions, instrumentation; auditability.

1. Control Title: Independent Computer Use by Auditors

2. Objective: Prevent interference with auditing.

3. Description: Audit independence can be considerably enhanced by using a computer not associated with the data processing activities being audited. Otherwise, if the same computer is being used, then the computer should be used in isolation from all other activities. Where data tapes are being audited, they may be taken to a service bureau to perform audit activities.

4. Variables: Computer availability, computer system compatibilities, computer audit activity.

5. Strengths: Use of an independent computer may provide the EDP auditors with more direct computer operation experience, adding to their capabilities. Audit computer use may avoid conflicts or overloading of the computer system being audited. The transportability of data from one computer to another can be validated.

6. Weaknesses: Unless a separate computer is readily available, the cost of audit may be prohibitive. Movement of sensitive data from the computer center may expose them to new vulnerabilities.

7. How to Audit: Investigate possible systems interconnections and ensure their independence.

8. Purpose: Prevention

9. Control Area: Computer system

10. Mode: Computer applications system, manual procedures

11. Area of Responsibility: Audit

12. Cost: Medium

13. Principles of Note: Cost effectiveness, least privilege, control and subject independence, limit of dependence on other mechanisms, auditability.

1. Control Title: Automation of Computer Operations

2. Objective: Prevent unauthorized computer activities.

3. Description: Computer operations should be made as automatic as possible, using such capabilities as production, program and test program libraries, automatic tape library management, reduction of job control by punch cards, and computer operator activity logging.

4. Variables: Availability of computer operations software package, high volume of activity justifying use of automated methods, amount of routine production activity.

5. Strengths: Reduction of manual procedures generally results in improved control of computer operations activities. Reduction of staff reduces exposure to accidental or intentionally caused loss, provides motivation to use automated operations packages beyond other considerations of cost-effectiveness.

6. Weaknesses: Concentration of trust among fewer people may result in less exposure to loss but potential for larger losses if they occur. It becomes more difficult to separate job duties among fewer operations personnel.

7. How to Audit: Observe erasure activity and location of degaussing.

8. Purpose: Prevention

9. Control Area: Computer center

10. Mode: Manual procedures

11. Area of Responsibility: Operations

12. Cost: Low

13. Principles of Note: Accountability, instrumentation.

MANAGEMENT-INITIATED CONTROLS

1. Control Title: Separation and Accountability of EDP Functions

2. Objective: Prevent loss of security support.

3. Description: Holding managers accountable for the security in the areas they manage requires that these areas be clearly and explicitly defined so that there is no overlap or gaps in managerial control of EDP functions. EDP functions should be broken down into as many discrete self-contained activities as is practical and cost-effective under the circumstances. Besides being a good general management principle to maintain high performance, it also provides the necessary explicit structure for assignment of controls, responsibility for them, accountability and a means of measuring the completeness and consistency of meeting all vulnerabilities adequately. Separate, well-defined EDP functions also facilitate the separation of duties among managers, as is required in separation of duties of employees. This reduces the level of trust needed for each manager. The functions of authorization, custody of assets, and accountability should be separated to the extent possible.

4. Variables: EDP functions, accountability policy.

5. Strengths: This separation reduces the possiblity of accidental or intentional acts resulting in losses. It forces the need for collusion among individuals who may attempt unauthorized activities. More efficient EDP functions are possible. The possible loss of control is inhibited from migrating from one function to another.

6. Weaknesses: Increased complexity of EDP functions could result from excessive separation of functions, making the application of individual controls more difficult. Small shops may not have adequate numbers of employees to support extensive separation of duties.

7. How to Audit: Managers of EDP functions should be interviewed and their charters examined to ensure adequate separation and effectiveness of functional interfaces. Interfaces should be reviewed for consistency and completeness.

8. Purpose: Prevention

9. Control Area: Management

10. Mode: Policy

11. Area of Responsibility: Management

12. Cost: Low

13. Principles of Note: Limit of dependence on other mechanisms, completeness and consistency, accountability.

1. Control Title: Computer Security Management Committee

2. Objective: Prevent loss of security support.

3. Description: A high-level management committee is organized to develop security policy and oversee all security of information handling activities. The committee is made up of management representatives from each of the parts of the organization concerned with information processing. The committee is responsible for coordinating computer security, reviewing the state of security, ensuring the visibility of management's support of computer security throughout the organization, approving computer security reviews, receiving and accepting computer security review reports, and ensuring proper control interfaces among organization functions. It should act in some respects similar to a Board of Director's Audit Committee. Computer security reviews and recommendations for major controls should be made to, and approved by, this committee. The committee ensures that privacy and security are part of the overall information handling plan. The Steering Committee may be part of a larger activity within an organization to carry out the function of information resource management. For example, in one research and development organization an oversight council made up of representatives from organizations that send and receive data bases from the R&D organization was established. They are charged with oversight responsibilities for the conduct and control of the R&D organization relative to the exchange of data bases. Especially important are questions of individual privacy concerning the content of the data bases.

4. Variables: Level and participation of Steering Committee members, objectives and charter of the Steering Committee, powers and advisory capacity of the committee.

5. Strengths: A Steering Committee visibly shows the dedication and support of security by top management to the entire organization. Security activity is organized on a top-down basis. A committee that crosses organizational lines can better ensure the consistency of security across the interfaces and the consistency of attention to security in all information-processing-related functions. The Steering Committee can consider security and privacy within the context of other issues confronting the organization. Policies and procedures can be more effectively enforced. The committee approach can avoid the control of computer security by technologists who tend to be limited to technical solutions to security problems.

6. Weaknesses: A computer security management Steering Committee could add a level of undesirable bureaucracy. Control procurements and decisions may become time-consuming and expensive because of approvals necessary from a high-level committee. Individual managers may attempt to avoid the responsibility for security by assuming that the Steering Committee absolves them of such responsibility.

7. How to Audit: Review decisions of the committee and its work products. The head of EDP Audit should be a member of the Steering Committee.

8. Purpose: Prevention, deterrence

9. Control Area: Management

10. Mode: Policy

11. Area of Responsibility: Management

12. Cost: Low

13. Principles of Note: Completeness and consistency, accountability.

1. Control Title: Financial Loss Contingency and Recovery Funding

2. Objective: Recover from business interruption.

3. Description: Self-insured organizations, such as government agencies, should be assured of readily available emergency funds for contingencies and recovery. Specialized EDP insurance is available and should be considered when insurance covering other types of losses in a business may not apply. Financial risk protection should cover asset losses, business interruption, and extra expenses resulting from contingency recovery. Organizations not self-insured should bond all employees against fraud in high-risk areas of data processing activities. Blanket bonds will normally cover this activity.

4. Variables: Organization insurance practices, lines of credit and availability of emergency funds, size of potential losses, and deductible amounts.

5. Strengths: Protection against financial loss by sharing risks is an important business protection.

6. Weaknesses: Insurance must not be used as an alternative to good security.

7. How to Audit: The insurance or self-insurance program should be periodically reviewed. Assistance of experienced risk and insurance experts should be used.

8. Purpose: Recovery

9. Control Area: Management

10. Mode: Policy

11. Area of Responsibility: Insurance

12. Cost: High

13. Principles of Note: Cost-effectiveness, minimization of exceptions, limit of dependence on other mechanisms.

1. Control Title: Data Classification

2. Objective: Prevent compromise of data.

3. Description: Data may be classified at different security levels to produce cost savings and effectiveness of applying controls consistent with various levels of sensitivity of data. Some organizations maintain the same level of security for all data, believing that making exceptions is too costly. Other organizations may have only small amounts of data of a highly sensitive nature and find that applying special controls to the small amount of data is cost-effective. When data are classified, they may be identified in two or more levels, often referred to as general information, confidential information, secret information and other higher levels of classification named according to the functional use of the data, such as trade secret data, unreported financial performance, etc.

4. Variables: Amounts of data at various levels of sensitivity, potential controls, cost savings for no classification or several levels of classification, policies concerning security for each level of classification.

5. Strengths: Separate security treatment of data at different levels of security can result in control cost savings when the volume and concentration of sensitive data warrant special treatment. Otherwise, savings can be made by reducing control exceptions.

6. Weaknesses: Classification of data can easily result in excessive complexities in data handling and processing.

7. How to Audit: Review classification policy and sample data for audit trail testing of controls.

8. Purpose: Prevention

9. Control Area: Management

10. Mode: Policy

11. Area of Responsibility: Management

12. Cost: Low

13. Principles of Note: Cost-effectiveness, simplicity, least privilege, minimization of exceptions, accountability.

1. Control Title: EDP Auditor

2. Objective: Prevent inadequacy of system controls.

3. Description: Organizations with internal audit resources should establish EDP audit expertise within the internal audit function. In small organizations, general auditors can acquire EDP knowledge and skills. In larger organizations, full-time EDP audit specialists should be established to carry out EDP audits and assist general auditors in financial audits.

4. Variables: Amount of audit resources, regulatory or legal requirements for internal audit.

5. Strengths: Management can be assured about adequacy of computer security and auditability of systems and be notified on a timely basis of vulnerabilities.

6. Weaknesses: EDP auditors may not be given sufficient responsibilities and resources to perform an adequate job. EDP auditors may fall behind in state-of-the-art EDP audit practices and tools.

7. How to Audit: Periodic external audits should report to management on the adequacy of internal EDP audit capabilities and practices.

8. Purpose: Detection

9. Control Area: Computer center, computer system

10. Mode: Manual procedures, computer application system policy

11. Area of Responsibility: Management

12. Cost: High

13. Principles of Note: Auditability, instrumentation, sustainability.

1. Control Title: Computer Security Officer

2. Objective: Prevent inadequacy of system controls.

3. Description: An organization with sufficient computer security resources should have an individual identified as a computer security officer. In small organizations, the individual appointed may share this responsibility with other duties. In large organizations, one or more full-time employees should be assigned computer security administration responsibilities. The computer security officer should ideally report to the protection or security department covering the entire organization. This provides proper scope of responsibility for information and its movement throughout the organization. For practical purposes the computer security officer often functions within the computer department. Job descriptions are highly variable; examples may be obtained from many organizations with established computer security officers.

4. Variables: Computer security resources, functional and administrative position and reporting, job description.

5. Strengths: A computer security officer provides a focus for the formal development of a computer security program.

6. Weaknesses: Line management may attempt to transfer their responsibility for security to the computer security officer.

7. How to Audit: The computer security officer's activities should be audited according to his job description.

8. Purpose: Prevention

9. Control Area: Computer center, applications systems, computer system, programming and maintenance, management

10. Mode: Manual procedures

11. Area of Responsibility: Computer security, management

12. Cost: High

13. Principles of Note: Control and subject independence, acceptance by personnel, sustainability, accountability.

1. Control Title: Keeping Security Reports Confidential

2. Objective: Prevent disclosure, taking, or unauthorized use of documents.

3. Description: Computer security requires the use and filing of numerous reports, including results of security reviews, audits, exception reports, documentation of loss incidence, documentation of controls, control installation and maintenance, and personnel information. These reports are extremely sensitive and should be protected to the same degree as the highest level of information classification within the organization. A clean desk policy should be maintained in the security and audit offices. All security documents should be physically locked in sturdy cabinets. Computer-readable files should be secured separately from other physically stored files and should have high-level access protection when stored in a computer.

4. Variables: Security documents, safe storage containers, access authorization.

5. Strengths: The security function in an organization sets an example for the rest of the organization by appropriately caring for confidential information.

6. Weaknesses: Keeping security information under a high degree of protection makes the information difficult and time-consuming to use.

7. How to Audit: The auditors should periodically make an operational audit of the computer security program, including the safe storage of security documents.

8. Purpose: Prevention

9. Control Area: Management

10. Mode: Manual procedures

11. Area of Responsibility: Computer security

12. Cost: Low

13. Principles of Note: Completeness and consistency, accountability, least privilege.

1. Control Title: Cooperation of Computer Security Officers

2. Objective: Prevent inadequacy of system controls.

3. Description: Maintaining an effective computer security function can be enhanced by exchange of information with computer security functions in other outside organizations. Local computer security organizations can be developed within a city, a part of a city, or regionally. Monthly or other periodic meetings of computer security officers can be held to exchange useful information and experience. A hotline communication capability can be established for exchange of information on an emergency basis to provide warning of possible mishaps or losses. It is important to limit the details of information exchanged to ensure that confidential controls information is not disseminated to unauthorized parties.

4. Variables: Identification of cooperating organizations, types of information exchanged, procedures.

5. Strengths: This cooperation provides an opportunity to share important experiences and information and develop professional relationships that strengthen the career path of computer security officers.

6. Weaknesses: Too much information regarding an organization's security may become known to unauthorized persons.

7. How to Audit: EDP auditors should become involved in such outside organizational activities.

8. Purpose: Detection

9. Control Area: Management

10. Mode: Manual procedures

11. Area of Responsibility: Computer security

12. Cost: Low

13. Principles of Note: Overt design and operation, least privilege.

Control Section 5

COMPUTER PROGRAM DEVELOPMENT AND MAINTENANCE

1. Control Title: Responsibilities for Application Program Controls

2. Objective: Prevent inadequacy of controls.

3. Description: The inclusion of controls in application programs should be explicitly ensured and documented starting with design requirements and continuing through specifications development, production, and maintenance stages. The responsibility for adequacy and types of controls should be shared among EDP auditors, systems analysts, computer programmers, users, and data owners. Explicit documentation of controls is essential to ensure completion of their implementation, test, development of operational procedures, to carry out the intent of the controls, and to ensure their integrity during change and maintenance.

4. Variables: Documentation procedures and forms, policy.

5. Strengths: It is difficult to document explicitly all controls that must be in application programs. However, establishing the procedures to ensure that controls are adequate and included in applications provides assurance that applications will be adequately controlled.

6. Weaknesses: Controls that are not adequately supported by computer program application users will not be effective, and sufficient budgeting of money and resources will not be provided to adequately complete the specified controls.

7. How to Audit: Auditors' participation in design requirements and postimplementation testing for compliance with specifications.

8. Purpose: Prevention

9. Control Area: Programming and maintenance

10. Mode: Manual procedures

11. Area of Responsibility: Development, computer users

12. Cost: High

13. Principles of Note: Completeness and consistency, instrumentation.

1. Control Title: Compliance with Laws and Regulations

2. Objective: Avoid violations of laws and regulations.

3. Description: A statement regarding the new or modified system's compliance with relevant laws and regulations must be provided in requirements and specifications. Direct quotes from laws and regulations regarding EDP security and privacy applying within a legal jurisdiction, or those that may apply, should be included.

4. Variables: Legal and regulatory requirements for inclusion of statutes, laws, and regulations.

5. Strengths: Provides management with increased assurance that an application system is in compliance with relevant laws and regulations, thereby reducing the chances that management liability and other sanctions might be applied.

6. Weaknesses: Unless reviewed by a lawyer or some other knowledgeable person and compliance assured by audit, the control can become merely a perfunctory piece of paperwork where the blanks are filled in regardless of compliance with laws and regulations.

7. How to Audit: Examine documentation for statements regarding compliance, i.e., did the system designers actually have cause to represent that the new system was in compliance? Discuss the applicable laws and regulations with corporate legal counsel and system designers.

8. Purpose: Prevention

9. Control Area: Application system

10. Mode: Manual procedures

11. Area of Responsibility: Legal counsel, development

12. Cost: Medium

13. Principles of Note: Simplicity, universal application, accountability.

1. Control Title: Computer Program Quality Assurance

2. Objective: Detect computer, application, and communications systems and operations failures.

3. Description: A testing or quality control group should independently test and examine computer programs and related documentation to ensure integrity of program products before production use. This activity is best authorized by software development management or by the quality assurance or test department. Excessively formal program development standards should be avoided. Basic life-cycle procedures should be established before more elaborate practices are required. However, compliance with the established standards and procedures should be strongly enforced.

4. Variables: Quality assurance resources available, procedures, staff charter and size, sign-off forms design.

5. Strengths: A consistent compliance with good controls design offsets computer programmers' resistance to independent observation of their work.

6. Weaknesses: Imposing too much discipline too quickly on applications programming staff may cause negative reaction. Quality assurance programmers are difficult to motivate.

7. How to Audit: Operational audits should be performed by EDP auditors with extensive experience and reputation as competent computer programmers.

8. Purpose: Prevention

9. Control Area: Application system

10. Mode: Manual procedures

11. Area of Responsibility: Development

12. Cost: High

13. Principles of Note: Acceptance by personnel, least privilege, accountability.

1. Control Title: Computer Programs Change Logs

2. Objective: Detect computer, application, and communications systems and operations failures.

3. Description: All changes to computer programs are logged in a permanent written document. The log can be used as a means of ensuring formal approval of changes.

4. Variables: Log content, assignments, and accountability.

5. Strengths: Review of the purpose, time, type, and individuals who made changes is facilitated. This control aids in researching problems that occur. Utility programs that maintain program libraries in the computer are useful; they can automatically log change activity.

6. Weaknesses: Enforcement to ensure completeness is difficult.

7. How to Audit: Visual review of logs and random verification of changes.

8. Purpose: Detection, prevention

9. Control Area: Development

10. Mode: Manual procedures

11. Area of Responsibility: Development

12. Cost: Low

13. Principles of Note: Accountability.

1. Control Title: Secrecy of Data File and Program Name

2. Objective: Prevent loss, modification, disclosure, or destruction of data assets.

3. Description: Names for data files and computer programs are necessary for computer program development and documentation. They are also necessary for job setup and in some cases for computer operation. However, file and program names need not be known by those people who are in a transaction relationship with the computer system and not concerned with programming of computer applications. Therefore, a different set of terminology, and naming of entities should be developed for documentation of users manuals and for transaction activities.

4. Variables: Selection of systems, naming conventions.

5. Strengths: The least-privilege or need-to-know principle significantly reduces the exposure of sensitive assets. Separation of duties must also include the separation of information.

6. Weaknesses: Having two sets of names for computer program application entities complicates communications between programmers and users.

7. How to Audit: Examination of computer program documentation and user documentation can indicate that different naming conventions are being used.

8. Purpose: Prevention

9. Control Area: Application system

10. Mode: Manual procedures

11. Area of Responsibility: Development

12. Cost: Low

13. Principles of Note: Least privilege, control and subject independence.

1. Control Title: Participation of Computer Users at Critical Development Times

2. Objective: Prevent inadequacy of system controls.

3. Description: Computer users, including those providing input data and using computer output reports, should supply explicit control requirements to systems analysts and programmers who are designing and developing application systems. Users should also be required to explicitly agree that necessary controls have been implemented and continue to function during production use of the system and programming maintenance.

4. Variables: Policies and procedures, forms for control requirements statements, responsibilities and accountability for adequacy of controls.

5. Strengths: Users' understanding of their own applications is enhanced significantly when control specifications are required from them. Users are placed in a position where they can make better decisions regarding the appropriate controls in some aspects of applications and determine recovery time requirements. Users become knowledgeable of and sensitive to the needs for computer security and privacy. Sharing of responsibility and accountability for control is enhanced. Separation of duties is also enhanced. Completeness and consistency of controls are more ensured.

6. Weaknesses: Users may not have sufficient expertise to identify necessary controls. Systems development procedures become more complex.

7. How to Audit: Review systems design and development procedures at points where users are to be involved. Interview users with respect to their participation, understanding of their role, and awareness of the potential for controls in applications systems.

8. Purpose: Prevention

9. Control Area: Systems development

10. Mode: Manual procedures

11. Area of Responsibility: Users, development

12. Cost: Low

13. Principles of Note: Independence of control and subject, completeness and consistency, acceptance by personnel, accountability.

1. Control Title: Programming Library Access Control

2. Objective: Prevent unauthorized access to sensitive areas.

3. Description: Computer program libraries containing listings of programs under development and in production and associated documentation must be protected from unauthorized access. In larger organizations, a full-time or part-time librarian may be used to control access, logging in and logging out all documents. The program library should be physically separated by barriers from other activities. Documents should be distributed only to authorized users. It may be necessary to enforce strict access control to programmers' offices as a means of protecting programs and documentation. Programmers should have lockable file cabinets in which they can store materials currently in use. A clean desk policy at the end of each working day may be justified as an extreme measure. Program and documentation control is particularly important when using or developing licensed software packages because of the strict contractual limitations and liabilities.

4. Variables: Resources available for program library access control, barriers surrounding the program library and programmers' offices, policies and procedures regarding protection of documentation and program listings.

5. Strengths: Demonstrates the importance of computer program assets to the organization. Provides separation of duty among programmers to ensure that programmers have access only to the documentation and programs within their areas of responsbility.

6. Weaknesses: Restrictions on access may stifle communications and creativity of the programming staff.

7. How to Audit: Observe operation of the program library, make unexpected visits and observations of programmer offices, review procedures and policies for restricting access.

8. Purpose: Prevention

9. Control Area: Programming and maintenance

10. Mode: Manual procedures

11. Area of Responsibility: Development

12. Cost: Medium

13. Principles of Note: Least privilege, control and subject independence, acceptance by personnel, accountability.

1. Control Title: Requirements and Specification Participation by EDP Auditors

2. Objective: To prevent inadequacy of system controls.

3. Description: EDP auditors should participate in the development of requirements for important applications systems to ensure that the audit requirements in applications systems are adequate and that adequate controls have been specified. EDP auditors should be required to sign off on all formalized application system requirements and specifications.

4. Variables: EDP audit resources, procedures specifying EDP audit participation, forms for signoff.

5. Strengths: The auditability of application systems is strengthened and can reduce the cost of both internal and external audits.

6. Weaknesses: It may be claimed that excessive participation by EDP auditors could result in a loss of independence since the EDP auditors must also evaluate the adequacy of implemented controls.

7. How to Audit: Audit management should periodically review EDP auditor participation and ensure that all significant application systems receive audit attention.

8. Purpose: Prevention

9. Control Area: Programming and maintenance

10. Mode: Manual procedures

11. Area of Responsibility: Audit

12. Cost: Medium

13. Principles of Note: Auditability, accountability, control and subject independence, completeness and consistency.

1. Control Title: Vendor-Supplied Program Integrity

2. Objective: Avoid inadequacy of controls.

3. Description: To the greatest extent possible and practical, vendor-supplied computer programs should be used without modification. Many new vendor-supplied computer programs have been developed with controls and integrity built into them. Any modifications to these programs will possibly compromise the built-in capabilities. Desired changes to the programs should be obtained from the vendor as standard program updates.

4. Variables: Selection of programs, authorizations.

5. Strengths: This control is a means of preserving the security and integrity built into vendor-supplied computer programs. It is also a means of holding vendors responsible for any deficiencies in the programs.

6. Weaknesses: Failure to modify computer programs to make them more responsive to user needs may encourage users to subvert or neutralize existing controls.

7. How to Audit: This control could reduce the frequency of changes to computer programs, thus facilitating direct code comparison of production programs with master backup copies of programs. This should be done periodically to ensure that management policy is followed in restricting modification of vendor-supplied computer programs.

8. Purpose: Prevention

9. Control Area: Computer center

10. Mode: Policy

11. Area of Responsibility: Management

12. Cost: Low

13. Principles of Note: Accountability.

Baseline

1. Control Title: Technical Review of Operating System Changes

2. Objective: Avoid inadequacy of controls.

3. Description: Whenever any change is to be made to the computer operating system programs, a review of the change is made. The intent is to make sure that the new changes are valuable and will not compromise controls and integrity, have an unanticipated impact on some other part of the system, or interfere excessively with vendor updates.

4. Variables: Review procedures, authorization assignment.

5. Strengths: Review helps prevent unnecessary changes and simplifies testing and understanding of the system.

6. Weaknesses: Slowdown of changes may occur. Loss of compatability with vendor's version may require costly, independent maintenance.

7. How to Audit: Review the logs of systems changes and compare with actual changes.

8. Purpose: Prevention

9. Control Area: Computer system

10. Mode: Manual procedures

11. Area of Responsibility: Operations

12. Cost: Medium

13. Principles of Note: Override capability, accountability.

Selective
Processing of Personal Information

1. Control Title: Separation of Personal Identification Data

2. Objective: Prevent disclosure or unauthorized use of personal information.

3. Description: For data bases that identify individuals as well as contain sensitive information about individuals, the data base is separated into a file of personal identifiers and a file of data with an index linking the identifiers with the data.

4. Variables: Justification for separation, method of separation.

5. Strengths: Physical separation of data fields ensures that privacy of individuals will not be compromised, even if other controls are compromised. It is required by law (Title 28) in criminal justice agencies and possibly in other situations.

6. Weaknesses: The process is complex and requires significant administrative procedures. Special systems procedures may be needed.

7. How to Audit: Review how files are set up and check records that log destruction of link files.

8. Purpose: Prevention

9. Control Area: Application system

10. Mode: Manual procedures

11. Area of Responsibility: User

12. Cost: Medium

13. Principles of Note: Independence of control and subject.

1. Control Title: Sufficient Personal Identifiers for Data Base Search

2. Objective: Prevent disclosure or unauthorized use of personal information.

3. Description: To reduce the probability that an erroneous match between personal data and identification will occur, a sufficient set of personal identifiers is required before searches are permitted. Using techniques for the location of a personal record involves the ranking of several matches or near matches on several fields, such as name, date of birth, race, and sex. Because the erroneous identification, such as a criminal history or other record for an individual, may involve potential harm to the individual, the probability of a correct match should be very high. One installation identifies a sufficient set as complete name including known aliases (or maiden name if applicable), race, sex, and date of birth.

4. Variables: Data files to be protected, identifier sufficiency.

5. Strengths: Increases the chances that records will be updated with valid information.

6. Weaknesses: Valuable processing may be precluded because the requisite search information was not obtainable. Special circumstances, such as a variable number of personal identifiers, increases complexity. Administrative costs may be increased if such strict rules are implemented and followed.

7. How to Audit: Examine data base search procedures looking for situations in which an individual could erroneously be associated with a record.

8. Purpose: Prevention

9. Control Area: Application system

10. Mode: Computer application system

11. Area of Responsibility: Computer users

12. Cost: Medium

13. Principles of Note: Simplicity, override capability, least privilege.

1. Control Title: Cryptographic Protection

2. Objective: To prevent compromise of data.

3. Description: A high level of data communications and storage protection can be obtained by using the Data Encryption Standard (DES). However, effective encryption key management is essential. Frequently, applications do not require this level of encryption, and much simpler forms of encryption may be used. Data compression is a particularly simple form of encryption that also increases the efficiency of data storage. Data compression can be achieved by eliminating redundant information (spacing, etc.) and by encoding data fields. The cryptanalysis work factor should be determined and compared to the value of compromising the data being protected.

4. Variables: Selection of data for encryption, selection of encryption methods and products, key management.

5. Strengths: Encryption provides varying amounts of protection to data in communication circuits and when stored in computer-readable form. Its strength depends on the work factor of cryptanalysis and the effectiveness of key confidentiality and administration.

6. Weaknesses: Weak encryption or powerful encryption but weak key confidentiality and administration may provide a false sense of security.

7. How to Audit: Periodic audits should be performed to determine the proper application of cryptographic protection, the effectiveness of the key confidentiality and administration, and independent verification of unauthorized decryption work factor.

8. Purpose: Prevention

9. Control Area: Computer center

10. Mode: Hardware

11. Area of Responsibility: Computer security

12. Cost: High

13. Principles of Note: Least privilege.

1. Control Title: Exception Reporting

2. Objective: Detect computer, application and communications systems, and operations failures.

3. Description: Exception reporting on a timely basis should be built into the computer operating system, utility programs, and application systems to report on any deviation from normal activity that may indicate errors or unauthorized acts. For example, if a user defines a data file that allows public access, a message will be printed out warning the user, and possibly the operations staff, that the file is not protected. Exception reporting should occur when a specific control is violated, or the exception report may constitute a warning of a possible undesirable event. Exception reports should be recorded in a recoverable form within the system and when necessary for timely action, displayed to the computer operator, or, in case of on-line terminal use, displayed to the terminal user.

4. Variables: Actions requiring exception reporting, method of reporting exceptions, procedures for taking action on exceptions reported.

5. Strengths: This control is automatic and reduces the likelihood of human error in handling exceptions.

6. Weaknesses: Frequent or voluminous exception reports may result in lack of sufficient attention.

7. How to Audit: Tests that force exception reporting should be run, and actions taken should be reviewed.

8. Purpose: Detection

9. Control Area: Computer system

10. Mode: Computer operating system, computer application system, manual procedures

11. Area of Responsibility: Computer users, operations

12. Cost: Medium

13. Principles of Note: Override capability, minimization of exceptions, instrumentation.

1. Control Title: Input Data Validation

2. Objectives: Prevent loss, modification, disclosure, or destruction of data assets.

3. Description: Validation of all input to a computer system should be performed in both applications and computer operating systems to assist in the assurance of correct and appropriate data. Validation should include examination for out-of-range values of data, invalid characters in data fields, exceeding upper and lower limits of data volume, and unauthorized or inconsistent control data. Program errors dependent on the content or meaning of the data can also be checked. For example, inconsistent criminal justice disposition data relative to previously entered dispositions can be flagged for manual checking and correction.

4. Variables: Validation checks, error actions to be taken, locations in processing sequences for validation activity.

5. Strengths: Early validation of input data can result in prevention of error propagation.

6. Weaknesses: Excessive computer resources may be used for infrequently occurring errors.

7. How to Audit: Review systems design documentation to determine that input data controls are appropriately designed into the system. Run tests using erroneous data to check on the functioning of validation controls.

8. Purpose: Prevention

9. Control Area: Application system, computer operating system

10. Mode: Computer operating system, computer application system

11. Area of Responsibility: Computer users, operations, input and output

12. Cost: High

13. Principles of Note: Simplicity, override capability, minimization of exceptions, completeness and consistency, instrumentation, auditability.

Control Section 7

COMPUTER SYSTEM TERMINAL ACCESS CONTROLS

1. Control Title: Telephone Access Universal Selection

2. Objective: Avoid computer access exposure.

3. Description: Limiting access to a computer and data files can be an important means of security. Several means of accomplishing this are possible. It may be possible and important to eliminate dial-up access to a computer. A computer interfaced to the dial-up public telephone network is exposed to access from any telephone in the world. There may be a trade-off in computer security by giving up or limiting the benefits of dial-up access. This can be accomplished by using only point-to-point wire or leased-line telephone access to the computer. An alternative is to provide dial-up access to a small computer for development or other timesharing purposes while reserving another computer for more sensitive production activity that is not interfaced to dial-up telephones. A control computer providing access to two or more other computers can also be used as a means of protecting them from dial-up access. An alternative method of restricting access is to provide for dial-up access at limited periods of time of day. During periods of dial-up access, particularly sensitive files or applications would not be resident in the computer system or secondary storage. A variation is to remove all sensitive files from secondary storage except at the explicit times of use of these files. A partial degree of protection for dial-up access systems is to maintain strict need-to-know availability of the telephone numbers and log-in protocol for accessing the computer system. Most dial-up timesharing computer services have similar access protocols; therefore, a unique, very different initial access exchange of identifying information may be useful to limit access. The telephone numbers should be unlisted, different in pattern of digits, and have different prefixes from voice telephone numbers for the organizations that are publicly listed. Call back to verifying the source of telephone access is also popular.

4. Variables: Type of communication service, selection of telephone numbers, log-in protocol, time limits, call back.

5. Strengths: Avoidance of exposure is a particularly strong means of simplifying and reducing the problems of securing computer systems. Limiting or eliminating dial-up access significantly reduces exposure.

6. Weaknesses: An important objective for computers is to make them easily and widely accessible. Eliminating or limiting dial-up significantly reduces this capability.

7. How to Audit: Access capabilities, review access logs.

8. Purpose: Prevention

9. Control Area: Computer systems

10. Mode: Hardware

11. Area of Responsibility: Operations

12. Cost: High

13. Principles of Note: Least privilege, limit dependence on other mechanisms.

1. Control Title: Limit Transaction Privileges from Terminals

2. Objective: Prevent loss or destruction of assets, prevent unauthorized browsing of systems files, prevent "hacking" (trying commands just to see what will happen), prevent system crashes caused by unauthorized use of certain systems commands.

3. Description: In addition to controlling resources (files, off-line data storage volumes, etc.), the transactions that a particular user is permitted to initiate are limited. What the system commands that a user can use or is informed of is controlled by the user's job duties. Thus, the systems level and application commands, such as reporting who is currently logged into the system, are restricted on a need-to-know basis. Logs may be kept for all attempts to use an authorized system command; this can be used to determine who needs training or perhaps disciplinary action.

4. Variables: Transactions to be limited, assignment of privileges to users.

5. Strengths: Prevents users from performing unauthorized acts, including examination of file names of other users and other system-related commands. Without these systems transactions, compromise of the operating system and other such abuses are made significantly harder to accomplish. Because the system commands are monitored and controlled by the computer, they can be sustained and enforced.

6. Weaknesses: May unduly restrict users' ability to perform their jobs, especially if the users are programmers. Undue restriction may result in reduced productivity and increased levels of frustration. Determination of what commands should be restricted may be involved and time consuming.

7. How to Audit: Examine system commands permitted for certain groups of users for reasonableness. Review requests for changes in systems command privileges for authorization and need. If available, examine logs for unauthorized attempts to use systems commands that certain users are not permitted to use.

8. Purpose: Prevention

9. Control Area: Computer systems

CONTINUED

2 OF 3

10. Mode: Computer operating system, computer application system

11. Area of Responsibility: Operations management

12. Cost: Medium

13. Principles of Note: Simplicity, least privilege, independence of control and subject, sustainability.

1. Control Title: Privileged Information Display Restrictions

2. Objective: Prevent unauthorized data disclosure.

3. Description: Programmers, users, and others who have access to computer data bases are allowed to view only the data that pertain to their own job functions. Other data that may be resident on computers, outside the purview of an individual's job duties, are not available, nor is the knowledge of such data available. For example, data base data item descriptions have only subsets of the data supplied to particular individuals. Assistance programs, system documentation, and the like are specially tailored to the needs of different groups of individuals with different duties.

4. Variables: Design of data base index and tables of contents displays, access administration.

5. Strengths: If users, programmers, and others with access to the data do not know that certain data types are available, then they are prevented from perpetrating abuses associated with these data. Similarly, if these individuals do not have documentation or other information regarding these data, although they know these data exist, they are prevented from perpetrating unauthorized acts.

6. Weaknesses: Time-consuming and expensive to maintain separation of reference information of the data resident on computerized systems. May not facilitate certain efficiencies to be discovered and implemented.

7. How to Audit: Review systems design documentation to determine that individuals are not provided with more than the requisite information. Review systems development guidelines. Test access controls.

8. Purpose: Prevention

9. Control Area: Application system, computer system

10. Mode: Computer operating system, computer application systems

11. Area of Responsibility: Computer security, development

12. Cost: High

13. Principles of Note: Simplicity, avoidance of need for design secrecy, least privilege, acceptance by personnel, minimization of exceptions.

1. Control Title: Data File Access Subcontrols by Job Function

2. Objective: Prevent unauthorized access to data.

3. Description: Different types of data base read and update privileges are given to employees with different job functions. Data field read privileges can be granted or not depending on user job function. Likewise, update privileges may not be granted, or may be granted only for certain data fields within certain types of records of a data base. For instance, clerks handling mailing-related matters would be permitted to update only the address field. This control results in division of labor and separation of duties.

4. Variables: Data file access control capability, identification and authorization of users, data files and fields within data files, administration.

5. Strengths: Collusion is made necessary and more difficult when privileges for file and field access are directly related to an employee's job duties. Employees are prevented from altering fields in records that do not come within the domain of their jobs. Privacy and confidentiality are preserved when persons who do not need to be able to access certain fields are prevented from doing so; browsing is prevented.

6. Weaknesses: Users must be uniquely identified with passwords and identification user words in order for this control to be applied. Significant system overhead may be associated with the authorization. If someone is unavailable, then another person who may not have the same privileges may need to perform the other's duties; this could lead to sharing of passwords and other circumventing of controls activities.

7. How to Audit: Ask employees to demonstrate certain system capabilities, if possible asking them to do things that they properly should be prevented from doing. Care should be taken that internal system alarms triggered by such testing do not cause problems. Discuss with applications management and systems designers the segmentation of personnel duties within certain applications areas and the separation of duties enforced by the procedures.

8. Purpose: Prevention

9. Control Area: Application systems, computer systems

10. Mode: Manual procedures

11. Area of Responsibility: Computer users, management, development operations

12. Cost: Medium

13. Principles of Note: Least privilege, independence of control and subject, accountability.

1. Control Title: Monitoring Computer Use

2. Objective: Detect unauthorized activities.

3. Description: On a random or periodic selective basis, communications between the host computer and remote terminals are monitored. File names and contents are examined. Such monitoring must be limited to computer activity that is established for business purposes only to avoid privacy invasion. The usage is logged and analyzed to determine that the user is only doing actions that have been explicitly authorized.

4. Variables: Selection basis, monitoring and examination methods and assignments, exception reporting.

5. Strengths: Allows management to determine that computer/communications resources are being used as authorized. Allows management to take evidence of activities of persons they suspect of some wrongdoing. Allows management to determine how certain users interact with the system toward improving services (response time, application, ease of use, etc.). Useful as an audit tool. If users are aware that the activity exists, then they may be deterred from engaging in certain types of acts.

6. Weaknesses: Could be used by unauthorized persons to spy on and/or harass users.

7. How to Audit: Use the same procedures for other auditing matters. Identify individuals who engage in this activity and review their work.

8. Purpose: Deterrence, detection

9. Control Area: Computer system

10. Mode: Manual procedures, computer operating system

11. Area of Responsibility: Computer security, operations

12. Cost: Low

13. Principles of Note: Simplicity, independence of control and subject, instrumentation, accountability.

1. Control Title: Terminal Identifiers

2. Objective: Prevent unauthorized computer access.

3. Description: Automatic terminal identification circuits can be installed in or associated with terminals for identification in host computers. Terminal identifiers are used to indicate whether a particular terminal is permitted to initiate or receive certain transactions. This access control requires that remote terminals be physically secured and that only certain known individuals be able to access remote terminals. Cryptographic devices can be used as terminal identifiers. Certain record change requests must be handled by means other than the use of these remote terminals, such as through the mail to a central facility; in this way records integrity can be preserved. Unauthorized intentional or accidental use of applications programs is prevented. A log records all unauthorized attempts to use applications programs.

4. Variables: Selection of devices, host system controls, exception reporting and journaling usage.

5. Strengths: Users may not have to be bothered with log-in/log-off procedures.

6. Weaknesses: Requires that remote terminals be attended or physically secure 24 hours a day. Does not have users individually identified, hence accountability is hindered. Does not permit different users to have different privileges if only one terminal is available.

7. How to Audit: Examine records of access privileges to determine that users are not given privileges that they do not need in order to do their job. Examine all user privilege change requests and actions to determine that all changes of user privileges are both justifiable and authorized. Use remote terminal to actually test the access control system and logging facilities. Examine exception report produced when unauthorized accesses occur to make sure that all unauthorized attempts were followed up.

8. Purpose: Prevention

9. Control Area: Computer system

10. Mode: Hardware, computer operating system

11. Area of Responsibility: Computer security, development

12. Cost: High

13. Principles of Note: Least privilege, instrumentation, auditability, accountability.

1. Control Title: Passwords for Computer Terminal Access

2. Objective: Prevent unauthorized computer system access.

3. Description: Secret passwords are commonly used for access to computer systems through terminals. However, there is wide variation in the procedures for password administration. Passwords are normally accompanied by a protocol of exchange of recognition between the user and the computer, including the input from the user of a project or account number and a password. Normally, one or more users are working with the computer under a single project or account number. Occasionally, only one password is used for a group of people as well. However, each user should have his own secret password. In some cases, each user may select his own password, and it is known only to him and stored in the computer system. Others select their passwords but must receive approval of them from the computer security coordinator to ensure that they are appropriate and not easily guessed. Some organizations use computer programs to produce appropriate, easily remembered, but somewhat random passwords. In other cases, passwords are chosen by a computer security administrator and assigned to users. And finally, passwords can be generated automatically by the computer system and assigned to users. Another variation is the assignment of a password to a user with instructions that he is to use his password for initial access, at which time he must then change his password in the computer system. He should be prevented from using the initial password again. Frequently, privileged passwords are identified in the computer system so that systems programmers and others requiring password access allowing a wider range of system usage and use of special commends may carry out their work. It is generally accepted that passwords should be changed among a group of computer users who might share their passwords every time an individual leaves the immediate group by terminating his employment or given new assignments. Privileged passwords should be changed more frequently than others. Passwords should also be changed whenever there is any indication of possible system abuse or compromise. If passwords are manually conveyed to users, it should be done in confidential, sealed envelopes personally delivered by a trusted employee or orally in face-to-face conversation in confidential surroundings. A receipt should be received from the user indicating that he has received and accepted a new password and agrees to keep it confidential. These receipts should be kept on file by the computer security administrator. It is best to keep no paper record of passwords, and the master password file in the computer system should be encrypted or otherwise protected. If a

password is forgotten by the user, then it should be removed from the computer system and a new password should be assigned. The user should destroy any written record of the password once memorized, and severe penalties should be enforced for writing or revealing the password. An alternative is to keep a record of passwords locked in a safe place such as a vault. This can be done by the project leader for each group of users and is more desirable than having a centralized record of project numbers.

4. Variables: Password selection, password length, change frequency, recordkeeping.

5. Strengths: Secret passwords provide the equivalent protection of combinations for vault access that has long been accepted as safe access to valuable assets. The strength of the password system is primarily dependent on the length of passwords and the password administration.

6. Weaknesses: The primary weaknesses of password systems concern the administration and discipline with which passwords are used and kept secret by users and administrators and the characteristics of the log-in procedure that limits the likelihood of password compromise.

7. How to Audit: Auditors should periodically examine the journaling of password activity looking for unusual patterns. They should observe the password administration to ensure compliance with procedural policy. They should also periodically observe terminal areas to ensure that controls are in place and working.

8. Purpose: Prevention

9. Control Area: Management

10. Mode: Manual procedures

11. Area of Responsibility: Computer security

12. Cost: Medium

13. Principles of Note: Least privilege, independence of control or subject, instrumentation, acceptance, accountability.

Selective
Many Remote Terminal Users

1. Control Title: Passwords Generated and Printed by Computer in Sealed Envelopes

2. Objective: Prevent disclosure of passwords.

3. Description: User passwords are provided by a computerized random number/letter generator and printed directly through sealed envelopes, using the same carbon paper in envelope techniques that are used for many direct deposit receipts. These sealed envelopes are delivered directly to the user without the password ever having been seen by humans. Because the user expects a new password at a certain time, a missing envelope will be noticed and the previously generated password will be cancelled and reissued. Similarly, if an envelope is opened or has evidence of tampering, then the password is cancelled and reissued. Receipts are returned to ensure delivery.

4. Variables: Frequency, computer security during password generation.

5. Strengths: Prevents persons involved in the password administration area from using passwords without the user's knowledge. Ensures that passwords are distributed on a regular basis without compromise.

6. Weaknesses: Known techniques can be used to read passwords within these envelopes without having to destroy the seal.

7. How to Audit: Witness the generation and distribution of sealed password envelopes. Examine the envelopes to determine the ease with which the passwords can be discovered without having to break the seal. Discuss with operations management the pros and cons of assigned versus user-chosen passwords.

8. Purpose: Prevention

9. Control Area: Computer system

10. Mode: Computer application system

11. Area of Responsibility: Operations, computer security

12. Cost: Medium

13. Principles of Note: Least privilege, independence of control and subject.

Selective
Frequent Terminal Usage Interruptions

1. Control Title: Dynamic Password Change Control by User

2. Objective: Prevent unauthorized use of passwords.

3. Description: Users are allowed to change their passwords any time once they have logged in to the system. A parameter can be set at log-in time or at any time during a logged-in session that prevents changing a password. This would be useful in the case where an individual logs in to the system, gets up and leaves the terminal for a short period of time, and does not want anyone to come along and change the password while he is away. The user must enter a new password twice to prevent an incorrect password entry caused by a typing error. If the second password is not the same, the user must begin again.

4. Variables: Password change protocol

5. Strengths: Provides flexibility for users.

6. Weaknesses: User motivation is difficult.

7. How to Audit: Conduct live test of the change procedure.

8. Purpose: Prevention

9. Control Area: Computer system

10. Mode: Computer operating system

11. Area of Responsibility: Computer security

12. Cost: Low

13. Principles of Note: Instrumentation, accountability.

Baseline

1. Control Title: Data Files Access

2. Objective: Prevention of unauthorized access to, modification, destruction, and disclosure of, and taking or using data stored in computer systems.

3. Description: Every data file stored in a computer system that could result in a significant loss if compromised through modification, destruction, disclosure, taking, or use should be protected by having access restricted based on a secret password known only to authorized persons and computer programs. File access should further be restricted by mode of access allowed: read only, append only, modify only, file name change, file access control change, or some combination of these modes. Commercial file access control computer program packages are available for some makes of computer systems to provide this protective feature. The operating systems of some makes of computers have this capability integrated into the system. Specific resources such as magnetic tapes and disks can also be controlled. Access controls should also include the journaling of accesses to provide audit trails and should produce a set of journal reports and exception reports, for example, of all unauthorized attempts to access specific files. The administration of assigning access rights and password assignments is important for the effectiveness of internal computer controls.

4. Variables: Selection of computer program package or implementation of operating system programs, administration of access control, forms design, identification of data files to be protected, identification of authorized file accessors.

5. Strengths: Employees, knowing that their activities are controlled and monitored, are deterred from engaging in unauthorized activity. Journals and exception reports can be used to investigate suspected unauthorized activities or to obtain evidence of known or suspected activities.

6. Weaknesses: Computer program commercial packages or other programs for file access control may degrade system performance.

7. How to Audit: Review system journals and exception reports to determine that proper actions have been taken. Test file access control for effects of unauthorized access. Review file access control administration.

8. Purpose: Prevention

9. Control Area: Computer system

10. Mode: Manual procedures, computer operating system

11. Area of Responsibility: Computer security, operations

12. Cost: Medium

13. Principles of Note: Least privilege, control and subject independence, completeness and consistency, instrumentation, acceptance by personnel, accountability.

1. Control Title: Computer Use Access Control Administration

2. Objective: Prevent unauthorized computer access.

3. Description: People wishing to have access to a computer system or to change their mode of access and authorized privileges must go through a formal procedure administered by a computer user coordinator. Usually one or more special forms must be completed indicating the type of request and providing for authorizing signatures of appropriate managers. A specific document stating the conditions of access and privileges should accompany the authorization form. The person gaining access should be required to sign his name indicating that he has read and understands the conditions of access and limitations. The computer user, administrator, or coordinator may be in the data processing department or in a department where computers are being accessed.

4. Variables: Assignment of user coordinator, forms and agreements designed, authorization procedures, administration and record-keeping of access authorizations, coordination with computer operations staff for assignment of access in the computer system.

5. Strengths: Separation of duties between computer users and computer service providers is enchanced. The use of signed forms and agreements documents provides accountability and deterrent values.

6. Weaknesses: Adds complexity and bureaucracy, especially in small informal organizations.

7. How to Audit: Examine the coordinator's administrative activities and records to ensure proper management authorization of forms for access. Trace changes made to access authorization by interviewing computer users and operations staff.

8. Purpose: Prevention, deterrence

9. Control Area: Computer center, management

10. Mode: Manual procedures, computer operating system

11. Area of Responsibility: Computer security management, operations, computer users

12. Cost: Medium

13. Principles of Note: Override capability, least privilege, control and subject independence, instrumentation, accountability

1. Control Title: Computer Terminals Access and Use Restrictions

2. Objective: Prevent unauthorized use of computer terminals.

3. Description: Access to the use of all terminals owned or under the control of the organization should be restricted to authorized users. This can be done by physically securing rooms in which terminals are located and, where justified, by using metal key or electronic key locks to activate terminals. Terminals within security perimeters that are used frequently may be turned on at the beginning of the work day and left unlocked throughout the business day, then locked again at the end of the business day. Those terminals that are used only occasionally may be left locked except during use at any time of day. It may also be advisable to use various commercial locking devices to prevent terminals from being removed from assigned areas.

4. Variables: Physical security barriers around terminals, terminal locking mechanisms, procedures for locking and unlocking terminals and physical access areas, manual or automatic logging of usage at or within the terminal.

5. Strengths: The need for security can be impressed upon terminal users through secure locking capabilities.

6. Weaknesses: Physical security may sometimes be difficult to enforce in the informal environments in which terminals are frequently used.

7. How to Audit: Periodically observe terminal areas to ensure that physical security procedures are being used. Review the administration of key access control devices.

8. Purpose: Prevention

9. Control Area: Computer center

10. Mode: Manual procedures, hardware

11. Area of Responsibility: Security, computer security

12. Cost: Low

13. Principles of Note: Least privilege, limit of dependence on other mechanisms, instrumentation, accountability.

1. Control Title: Terminal Log-in Protocol

2. Objective: Prevent unauthorized computer access.

3. Description: The protocol for logging into a computer system from a computer should be designed to reduce unauthorized access. The terminal response to a log-in should provide a minimum of information to avoid providing an unauthorized user with any assistance. No system identifying information should be provided until the full user identification process has been successfully completed. There should be no feedback aids to an unauthorized user at any time during the log-in process that would provide clues to correct or incorrect input. Incorrect input should result in no assistance, and the system should disconnect. When user identification and password are being typed in, there should be no intermediate feedback from the system during the typing of this information that indicates whether the system has accepted any partially completed identification input. This requires that a user enter the complete set of identification and password information before there is any indication of whether this information is correct or not. Identification information should consist of the user name or other non-secret identification such as account number, followed by input of the secret password. Display terminals should provide display suppression while the password is being typed in to avoid its observation by another person. Printer terminals should provide nonprinting character mode or provide underprinting and over-printing of the spaces where the password is printed on the page. Additional, personal questions may be posed by the computer system to be answered by the terminal user to further ensure correct identity. No more than three attempts at entry of an unacceptable identification or password should be allowed. Three unsuccessful attempts should cause a telephone line disconnect. Time delay after an incorrect identification or password input of several seconds should occur to increase the work factor of automated exhaustive search for passwords. Also, a limited amount of time should be allowed for entry of a password before a telephone disconnect is performed. A variation of a password should be provided as a duress alarm. For example, if an individual is being forced to enter his password at a terminal he might interchange the last two characters that result in an immediate alarm at the host computer system that an entry is being attempted under duress. Any log-in that deviates from normal or accepted ranges of activity should be noted in an exception report at the host computer console in a timely manner for immediate action by a computer operator. All log-ins, whether authorized or unauthorized, should be journaled for later audit trail analysis. A means of allowing an unauthorized terminal user to gain authorized access to the system under totally monitored conditions should be provided to assist in locating sources of unauthorized attempts. Unauthorized users can be provided enough benign services to keep them at the terminal long enough for other detection activity to take place. Each time authorized users log into the system successfully, they should be provided with information concerning the date and time of the last time they logged into the system. Other information about their last sessions may also be summarized. Users can be made aware of any possible unauthorized use of their password in this manner.

4. Variables: Protocol information exchanges, nature and length of identification and password information, limit parameter values, journaling and exception reports, controlled unauthorized access mechanisms, computer operator procedures in the event of exceptional activity.

5. Strengths: Log-in controls can provide a means of positive identification of terminal users and motivate them to use good security practices.

6. Weaknesses: Inconveniences during log-in may discourage terminal users or tempt them to violate or test the log-in requirements. Excessive log-in requirements may cause many more log-in mistakes by authorized users.

7. How to Audit: Periodically test log-in procedures using out of bound, unacceptable activities to ensure exception recording effectiveness.

8. Purpose: Prevention

9. Control Area: Computer system

10. Mode: Computer operating system

11. Area of Responsibility: Computer security

12. Cost: Low

13. Principles of Note: Simplicity, override capability, least privilege, minimization of exceptions, instrumentation, acceptance by personnel.

1. Control Title: Computer System Password File Encryption

2. Objective: Prevent unauthorized computer access.

3. Description: The password file in the computer system contains master copies of passwords to verify correct identification and password input from terminal log-ins. This data file is one of the most sensitive in the entire computer system and therefore must be properly protected. Passwords in the file should be individually encrypted using a one-way encryption algorithm, i.e., the password can be encrypted but there is no reasonable means of decryption that would be computationally feasible given the current state of the art in switching speeds and cryptanalysis. When a password is entered from a computer terminal, it is immediately encrypted using the same algorithm and compared with the encrypted form of the master password for matching. In this manner, clear text passwords reside within the computer system for the shortest possible amount of time.

4. Variables: One way encryption algorithm, change control of passwords in the encrypted password file.

5. Strengths: Unlimited levels of protection are possible, depending on the strength of the cryptographic algorithms.

6. Weaknesses: Modification of the encryption algorithm computer program could cause a total compromise of the system and would not be easily detected.

7. How to Audit: Analyze the cryptographic algorithm program to ensure its integrity.

8. Purpose: Prevention

9. Control Area: Computer system

10. Mode: Computer operating system

11. Area of Responsibility: Computer security

12. Cost: Medium

13. Principles of Note: Override capability, avoidance of need for design secrecy, least privilege

1. Control Title: Remote Terminal User's Agreement

2. Objective: Prevent assets responsibility loss.

3. Description: All remote users are required to sign a user's agreement before they are permitted to use system resources. The agreement covers who shall pay for systems-related expenses, identifies physical location and relocation of terminals, establishes maintenance and service of equipment, assigns training of users, states hours of usage, instructs on further dissemination of information obtained from the system, details proper usage of the system, assigns physical security of terminals and other equipment, states service provider rights to deny service and to inspect equipment, establishes insurance coverage and liability for losses and renegotiation of the agreement, and other related matters.

4. Variables: Form design and content, accountability for administration, period of agreement.

5. Strengths: Clearly delineates the rights and obligations of both the service user and provider. Serves as an authoritative source for resolution of disputes between users and service providers. Allows service providers to sensitize users to security and privacy concerns before users can do work on the system.

6. Weaknesses: Legality of certain provisions may be in doubt and may require attention of legal counsel. Certain users may believe that the agreement does not suit their circumstances and may wish to modify the agreement or eliminate it entirely. Agreements may need to be renegotiated in light of additional legislation, regulation, or management decisions.

7. How to Audit: Examine user agreements for reasonableness and to make sure that they are still current. Consult with legal counsel about the enforceability of various clauses in the contract. Visit user sites to determine that the terms of the contract are being met.

8. Purpose: Deterrence, recovery

9. Control Area: Computer center, management

10 Mode: Manual procedures

11. Area of Responsibility: Legal, user, computer security, operations

12. Cost: Low

13. Principles of Note: Simplicity, independence of control and subject, accountability.

Appendix A

CASE STUDIES IN SELECTION AND APPROVAL OF CONTROLS

Appendix A

CASE STUDIES IN SELECTION AND APPROVAL OF CONTROLS

This section presents three case studies of how organizations select and approve security controls at computer centers. At each site, the principal contact was asked to describe the computer security control decision process within his organization.

Government Agency

When legislation requires controls, they are proposed to the government ADP Policy Committee for review. If the Policy Committee concurs, then the controls are implemented.

If no legislative requirements exist, then procedures vary, depending on the expected costs to install a control. Control operating costs are not part of this decision process but are just absorbed in the operating budget. If control installation is expected to cost more than $25,000, and the control has not been previously implemented, then a proposal is prepared for the ADP Policy Committee. The committee is presented with cost-benefit analyses (to the extent that these can be prepared without excessive resources being consumed) and descriptions of prudence of a particular control. Seldom is any directly measurable financial benefit associated with a control. Occasionally it can be shown that the the government might be saved from a possible lawsuit if a control is installed. Instead of financial considerations, management may demonstrate to the Policy Committee that the control is widely used. Management also frequently explains to the Policy Committee that a control is recommended by either internal or external auditors.

Loss experience elsewhere is not relied on to demonstrate that a control should be installed. Similarly, the use of a control elsewhere is not relied on to indicate that the agency should also have this control at its installation. Figures for loss experience and usage at other sites are often provided by vendors of particular products, but these figures are suspect and generally not used. The Committee decides whether additional resources should be provided.

If the cost of the control installation is less than $25,000, then a proposal is taken to a steering committee of the ADP Policy Committee. Management may take such a proposal to the finance and tax, transportation, or criminal justice steering committees. Controls are ranked by importance in the proposal. Management attempts to show that there are valid reasons to use their budget money for the controls placed high on

the priority list. The steering subcommittees do not approve the issuance of additional budget dollars, only the rearrangement of the spending plans.

The data processing center of this government agency processes ballots in elections, increasing concern about the appearance of good security, as well as actual security. Every election is followed by at least one suit usually brought by a losing candidate that alleges that the computer center employees could unduly influence the counting of ballots.

The preparation of a control proposal for either the ADP Policy Committee or one of its subcommittees usually involves an examination of the products on the market and detailed evaluation.

Research and Computer Program Development Organization

No specific methodology is used for justifying the installation of a computer security control in this organization. Controls are justified based on common sense and an understanding of the problem and the alternatives to remedy the problem. Controls are installed to a large extent when the budget will permit. Major controls that the firm feels it needs, yet is not able to afford, have been listed. For instance, management has for some time wanted a shredder that could destroy a large volume of discarded but still confidential reports. Because the cost of the needed type of shredder was about $67,000, this control could not be justified given the type of business that they were normally doing. When the firm obtained a contract that required the purchase and use of a shredder, they took the opportunity to acquire one.

Another example of an item appearing on the list of needed controls is a fireproof and burglarproof vault for the storage of accounting records, magnetic tapes, and disks. Management has not yet approved it because of its high cost. Because the control is not part of an operating budget, the acquisition must be approved by the firm's president. The president's approval would still be required for a control where included for purchase in the budget, if it were not listed as a separate line item. There is no exact cut-off value above which certain approval procedures are required.

The organization has a security committee that discusses policies and procedures relevant to security. Several members of top management, including the corporate attorney, sit on the committee. The committee discusses needs and changing circumstances, but does not have an audit or control review function. The committee also discusses the requirements of laws and regulations, as well as requirements placed on the firm by clients or potential clients. Ordinarily, the security committee will urge the data processing manager to investigate a certain area of concern based on the personal interests of members. In general, a staff member who has technical expertise in the area of concern will conduct a

study of the options, costs and benefits and then make recommendations to middle management. Depending on the source of funding (e.g., overhead, funds, project fund, line item), the proposal will or will not be passed to higher management.

The approval process is informal and not well-documented for a control that is part of a research project or used for in-house operations. If a control is to be part of a computer program package that the firm provides to outsiders, however, very strict adherence to documentation and system development standards is required.

The differences between approval of the retrofit of a control and the inclusion of a control in a new system are not substantial. The organization has just planned a new computer facility that will be remote from the firm's offices; thus, additional physical security was felt to be needed. To ensure that the controls fit together properly, management paid special attention to the entire control environment when building the new computer center.

One problem associated with expenditure for a control is a continuing disagreement centering around whether it should be charged to a contract or to overhead. In one case a line printer located in an office area is available to any employee who can walk up and remove printed reports. If a print job involved the output of assigned sensitive data, an employee was to stand at the printer and remove the sensitive output, making sure that it did not fall into the wrong hands. The organization discussed locating another printer in a physically secure area. The proposed printer could be monitored by an operator and have all output logged, stamped "sensitive", placed in an envelope, and hand-delivered to the user initiating the print request. The current printer costs are charged to projects, whereas the proposed additional printer involves additional overhead expenditure.

Large Business Firm

This firm rarely performs a cost-benfit analysis for any decision on implementing computer security controls, even though cost is an important consideration. Otherwise, justification for a particular control is based on what is considered prudent. Prudence in this context includes: meeting requirements of laws or regulations, taking steps to support management policies with respect to privacy and security, making decisions in a good business sense (cost-benefits being considered), providing the best possible service to salesmen and customers, and avoiding undue exposure to liability.

Approval procedures are different for proposed controls that are to be retrofitted to existing systems and those part of a new computer center or application. The firm is currently constructing two new computer centers where the controls to be used are to be decided on simultaneously. Physical access controls and controls in computer programs involved different procedures.

When a control is to be retrofitted, it is considered in the context of the current system of controls. When deciding on the controls to be used in the new centers, the staff relied on brainstorming and reasoning that indicated that a particular course of action was prudent. The data processing vice president decided which controls were appropriate based on proposals that were prepared by people in the facilities management, computer security, physical security, data processing systems development, and data processing operations groups. The audit department was not involved to any great extent; audit participates in these decisions only sporadically because of its limited staff. The computer security officer acted as overseer and coordinator. Loss experience was not usually cited as a reason to use a particular control at a new installation because reliable data are not considered to be available, with the exception of risks associated with fire. A control used at other sites is an important factor in the determination that it is prudent.

If a control is to be retrofitted to an existing system, then a formal system improvement request is prepared. This document is prepared by the group that recognizes that additional control is needed, it describes the reasons why the control is needed. The approval process for a control varies depending on the nature of the proposed improvement (who it will affect) and total cost. If a proposed improvement will cost $100,000 or more, involve six or more staff years of effort, or be especially sensitive or critical, special approval and monitoring procedures are called for.

Retrofit, low cost controls in computer programs are approved by the data processing divisional managers. Corporate data processing management decides on operational controls and controls that affect several divisions. High-cost controls require senior divisional or corporate management approval. The Human Resources Department (to determine staffing needs arising from the proposed control) and users may participate in decisions when appropriate. The audit department sometimes reviews controls to ensure that they are cost-effective and are achieving the stated objectives.

It can been seen that the procedures used by businesses are significantly different from the procedures used by not-for-profit organizations. Competition and ownership issues associated with the business environment are the primary factors leading to use of different procedures, which in turn may lead to a different set of controls.

Appendix B

THE BASELINE REVIEW METHOD

Appendix B

THE BASELINE REVIEW METHOD

Baseline Specifications

Baseline control objectives, controls, and control variants can be described in specifications showing their relationships. For more limited purposes, selective baselines using selective baseline control objectives, controls, and variants can be separately represented. Beyond baseline and selective categories, special control objectives, controls, and variants can be documented. A tabular approach is suggested to specify a baseline of data security. Variants are not depicted to simplify the diagram.

Baseline			
Control Objective 1	Control Objective 2	Control Objective 3...	Control Objective N
Control 1,1	Control 2,1	Control 3,1	Control N,1
Control 1,2	Control 2,2	[Control 3,i]*	Control N,2
Control $1,n_1$	Control $2,n_2$	Control $3,n_3$	Control N,n_N

*Example of a control not used. Justification would be provided.

Note that no vulnerabilities, risks, or other justifications need be supplied to accompany this baseline specification since all control objectives and controls are chosen for only one reason, general use. However, if a generally used control objective or control is missing, then the array should be supplemented with a note of the lack of that control objective or control and the justification for not using it supplied.

Likewise, a more limited, selective baseline of control objectives and controls can be specified in a tabular array similar to the baseline array but with the circumstances of need for each objective prefixed at the top:

Selective Baseline		
Selective Need	Selective Need	Selective Need
Control Objective 1	Control Objective 2...	Control Objective M
Control 1,1	Control 2,1	Control M,1
Control 1,2	[Control 2,i]*	Control M,2
Control 1,m_1	Control 2,m_2	Control M, m_M

*Example of a control not used. Justification would be provided.

A selective need for each control objective is identified by stating a particular environmental factor such as type of industry, potential threat, type of equipment, mode of equipment use, or application. Often, no one-to-one correspondence exists between a selective need and a selective control objective. One or several needs may be met with one or more control objectives, and controls may serve more than one need and control objective. As with the baseline, objectives and controls for a particular need that are not used would be identified and justified. Similarly, as with a baseline, no other justifications other than identifying selective needs need be supplied in a selective baseline.

Finally, special control objectives and controls will probably be necessary for special needs not commonly found in other computer centers. These can be structured similarly to the baseline array or in more free-form fashion. There may be fixed numbers of control objectives and controls for a baseline of security. The numbers of special controls may vary over short periods of time.

Profound differences between baselines, selective baselines, and special controls in these specifications reiterate the baseline concept:

- The only justification needed in a baseline is when a generally used control is not included.
- The only justification needed in a selective baseline is to describe the need for a control objective and when a generally accepted control for a selective control objective is not included.
- The justification for special controls is a description of the need for each control when it is included.

Up to this point the models have been described only to the detail of specifying controls. Control variants have not been explicitly identified because they introduce a significant increase in model complexity. Every control has a set of variables for which values must be selected. Some variants in a control may fall within the baseline, others may fall within the selective baseline, and still others may subdivide part of a baseline or selective baseline control into a special control.

A model combining all three levels and explicitly including variants, but again in simplified form, could appear as Table B-1.

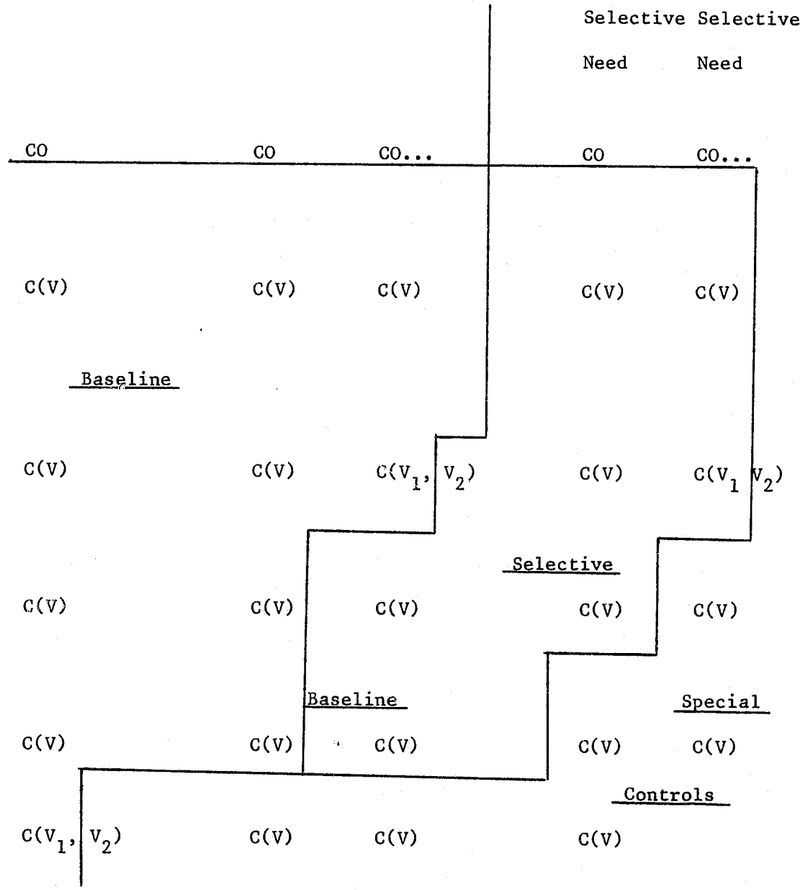
A Baseline Control Selection Example

A difficulty arises in specifications of generally used controls and their implementation variations. For example, prevention of unauthorized computer room access is a baseline objective, but the prudent controls to accomplish the objective and the values of the control implementation variables vary widely. Specific physical access controls found in many published security checklists can include the following:

(1) Sign-in/out log
(2) Procedure to challenge the presence of a person
(3) Mechanically locked doors
(4) Electronically locked doors
(5) Guards at doors
(6) Badge-access areas
(7) Closed-circuit television (CCTV) monitoring of doors and areas
(8) Man-trap or turnstile doors (a pass-through isolation booth)
(9) Microprocessors for access monitoring
(10) Automatic physiological identification verification for access (e.g., geometry, fingerprint scanning, voice pattern analysis, signature dynamics analysis)
(11) Frequent test and audit of access controls
(12) Contingency plan for failure of access controls
(13) Policy and procedure documents for access control
(14) Administration of access controls
(15) Physical barriers (sturdy walls, windows, and doors).

A control objective, "Prevent unauthorized physical access to computer room," in a security checklist is often claimed to be satisfied by marking "present." This checklist approach is clearly insufficient to assure prudent security. An array of electronic controls implemented in various compatible ways is needed to prevent unauthorized physical access. However, Items 1, 2, 6, 7, 9, and 13 are generally not acceptable by themselves. Control items 11-15 must be present to meet the control objective, but the use of other controls depends on traffic, different security levels on each side of the barrier, alternative forced access possibilities, and the degree of risk of unauthorized access.

Table B-1
BASELINE MODEL



Legend: CO = control objective
C = control
C(V) =control with an array V of variants
$C(V_1,V_2)$ = two subarrays of variants

The following generally used computer room access controls should be the baseline in any well run computer center:

(1) Physical barrier access control (strong walls, windows and doors, access mechanism)

(2) Administration of access control (responsibility assigned to somebody accountable, recordkeeping, authorization activity)

(3) Frequent testing and audit (frequency specified)

(4) Contingency plan for failure of access control

(5) Policy and procedure documentation

(6) Identification and authentication of authorized accessors

(7) Constraints on unauthorized accessors

This list expands the one control objective in a typical checklist to seven controls. Within each control, some specifications would be identified: strength of walls, person to administer access control, frequency of audit, content of a contingency plan, explicit policy content, method and records for identification of accessors and specific constraints. The baseline of seven controls has more detail than the typical checklist, but not so much as to include specific values of many of the variants.

The control implementation variations of whether windows are present, for example, would be beyond baseline specifications because the choice would depend on the nature of the potential threats, the type of area adjacent to the windows, and their purpose. However, another variant, the type of window material, may fall within the baseline because of general agreement that high-impact-resistant plastic or specially hardened glass is always necessary. An organization would consider the advice of the vendor's sales staff, its own experience, and the experience of other organizations with similar circumstances. This last consideration of what others are doing would be the key to assuring use of generally used controls and establishment of the baseline.

The Baseline Review and Selection Method

It is important that either periodic, comprehensive studies be conducted or that an ongoing documented security activity be maintained. Otherwise, serious vulnerabilities can arise that are not noticed or that are ignored because taking action against them may add unwanted cost or reduce performance. In addition, developing scenarios of potential threats can be used to discover many vulnerabilities.

The method of security review to evaluate the level of security, determine security needs, and recommend changes to achieve adequate protection derives from the foregoing concepts of generally used controls and baseline security. The active steps after a review of a computer center or system is authorized are as follows:

(1) Determine the scope of the review by identifying in gross form the facilities, people, equipment, supplies, computer programs, production processes, sources and destinations of data, and data files, and where stored and processed. Documentation must be collected, and supportive functions such as audit, safety, security, personnel, insurance and computer user departments must be identified. Potential threats need not be identified at this stage.

(2) Identify and document all existing controls and catalog them according to their purpose (control objectives). Include complete descriptions of all control variants.

(3) List additional control objectives, controls and control variants from current data security literature and from ideas collected from security review staff, managers, auditors, past audit reports and past security reviews. Catalog controls according to the control objectives and order the objectives from Step 2.

(4) Visit several other computer centers that are judged to have characteristics similar to yours and have effective data security. The number will depend on review resources available and opportunities. Visits should be arranged by an exchange of letter agreements assuring confidentiality and benefits for all parties from mutual exchange of information. In these visits identify the best controls, how they were justified, the cost-effectiveness, and the experience with them. Also identify controls that were rejected or that are not particularly effective and reasons for this.

(5) Synthesize information collected in Steps 1 through 4 into a baseline representation of control objectives, controls, and selected variants where no justification for their selection is to be developed other than citing general use. Also develop a selective baseline similarly where identification of purpose is needed to supplement information concerning limited use by other organizations. Categorize all controls and variants in both baselines according to whether they are currently installed, would cause a change to currently installed controls, are new controls, or are new controls that are not to be recommended (along with explanations).

(6) Perform potential threat, vulnerability, and risk analysis using current methods documented in the literature for those assets that would not be adequately (by consensus) protected by the baseline and selective baseline. There should be relatively few assets or issues remaining to be treated in this way. Reasons include new technology in use, unusual conditions, and possibly issues resulting from lack of concurrence on a baseline control or variant or where high cost of possible controls requires further justification.

(7) Make recommendations to management in three categories:

A. Baseline controls where no justification other than general use is provided.

B. Selective baseline controls where justification extends to a statement of purpose.

C. Special controls where full and detailed justification is provided.

In addition, recommendations can be organized according to priorities for implementation: immediate, soon, future, and when other conditions make them appropriate.

Steps 1 through 7 need not be accomplished in one study by one task group for all control needs on a comprehensive basis, even though that may be the most desirable way. Practically, the baseline, selective baseline, and special controls reviews could be done separately, by different people at different times, and can apply to specific control areas, control objectives, and vulnerabilities when they are noticed or opportunities arise to tackle them.

☆U.S. GOVERNMENT PRINTING OFFICE: 1982-361-233/1873

Related BJS Publications

Computer Crime: Criminal Justice Resource Manual
NCJ-10550

Computer Crime: Legislative Resource Manual
NCJ-78890

Computer Crime: Expert Witness Manual
NCJ-77927

Computer Crime: Computer Security Techniques

Computer Crime: Electronic Funds Transfer Systems and Crime

END