FIPS PUB 88

FEDERAL INFORMATION
PROCESSING STANDARDS PUBLICATION

1981 AUGUST 14

U.S. DEPARTMENT OF COMMERCE / National Bureau of Standards

GUIDELINE ON INTEGRITY ASSURANCE AND CONTROL IN DATABASE ADMINISTRATION

CATEGORY: SOFTWARE
SUBCATEGORY: DATA MANAGEMENT APPLICATIONS

U.S. DEPARTMENT OF COMMERCE, Malcolm Baldrige, *Secretary*
NATIONAL BUREAU OF STANDARDS, Ernest Ambler, *Director*

Foreword

The Federal Information Processing Standards Publication Series of the National Bureau of Standards is the official publication relating to standards adopted and promulgated under the provisions of Public Law 89-306 (Brooks Act) and under Part 6 of Title 15, Code of Federal Regulations. These legislative and executive mandates have given the Secretary of Commerce important responsibilities for improving the utilization and management of computers and automatic data processing in the Federal Government. To carry out the Secretary's responsibilities, the NBS, through its Institute for Computer Sciences and Technology, provides leadership, technical guidance, and coordination of Government efforts in the development of guidelines and standards in these areas.

The need for policies and procedures to help assure the integrity and security of Federal databases has been recognized for some time. Office of Management and Budget Circular A-71, Transmittal Memorandum No. 1, requires that each Federal agency establish a management control process to assure that appropriate safeguards are built into all new computer applications. The June 1979 report from the Comptroller General of the United States to the Congress entitled "Data Base Management Systems—Without Careful Planning There Can Be Problems" pointed out that the determination of whether or not adequate controls exist over data input and processing is very complex in a modern database environment. Therefore, NBS makes available this Guideline to provide Federal agencies with explicit advice on database integrity and security control.

James H. Burrows, *Director*
Institute for Computer Sciences and Technology

Abstract

This Guideline provides explicit direction to Federal database administration and database security personnel on how to improve database control. The document identifies integrity and security problems in the administration of database technology, and discusses those procedures and methods which have proven effective in addressing these problems. The document also provides an explicit, step-by-step procedure for examining and verifying the accuracy and completeness of a database.

Key words: computer program; data administration; data dictionary system; database auditing; database controls; database integrity; database management; Federal Information Processing Standards Publication.

Nat. Bur. Stand. (U.S.) Fed. Info. Process. Stand. Publ. (FIPS PUB) 88, 71 pages
(1981)
CODEN: FIPPAT

For sale by the National Technical Information Service, U.S. Department of Commerce, Springfield, VA 22161

Federal Information Processing Standards Publication 88

1981 August 14

ANNOUNCING THE

GUIDELINE ON INTEGRITY ASSURANCE AND CONTROL IN DATABASE ADMINISTRATION

Federal Information Processing Standards Publications are issued by the National Bureau of Standards pursuant to the Federal Property and Administrative Services Act of 1949, as amended, Public Law 89-306 (79 Stat. 1127), and as implemented by Executive Order 11717 (38 FR 12315, dated May 11, 1973), and Part 6 of Title 15 Code of Federal Regulations (CFR).

Name of Guideline: Guideline on Integrity Assurance and Control in Database Administration.

Category of Guideline: Software, Data Management Applications.

Explanation: This Guideline provides explicit advice on achieving database integrity and security control, and documents a step-by-step procedure for examining and verifying the accuracy and completeness of a database.

Approving Authority: U.S. Department of Commerce, National Bureau of Standards (Institute for Computer Sciences and Technology).

Maintenance Authority: U.S. Department of Commerce, National Bureau of Standards (Institute for Computer Sciences and Technology).

Cross Index:

a. Federal Information Processing Standards Publication (FIPS PUB) 31, Guidelines for ADP Physical Security and Risk Management.

b. Federal Information Processing Standards Publication (FIPS PUB) 38, Guidelines for Documentation of Computer Programs and Automated Data Systems.

c. Federal Information Processing Standards Publicaton (FIPS PUB) 39, Glossary for Computer Systems Security.

d. Federal Information Processing Standards Publication (FIPS PUB) 41, Computer Security Guidelines for Implementing the Privacy Act of 1974.

e. Federal Information Processing Standards Publication (FIPS PUB) 64, Guidelines for Documentation of Computer Programs and Automated Data Systems for the Initiation Phase.

f. Federal Information Processing Standards Publication (FIPS PUB) 65, Guidelines for Automatic Data Processing Risk Analysis.

g. Federal Information Processing Standards Publication (FIPS PUB) 76, Guideline for Planning and Using a Data Dictionary System.

h. Federal Information Processing Standards Publication (FIPS PUB) 77, Guideline for Planning and Management of Database Applications.

i. Federal Information Processing Standards Publication (FIPS PUB) 87, Guidelines for ADP Contingency Planning.

Applicability: This Guideline is intended as a basic reference for Federal database administration and database security personnel who are responsible for the integrity and security of agency databases.

Implementation: This Guideline should be consulted when Federal agencies are: designing or reorganizing their basic database structures and procedures; evaluating the security and integrity safeguards in current database environments; or preparing to conduct or assist in a formal database integrity examination.

Specifications: Federal Information Processing Standards Publication 88 (FIPS-PUB-88), Guideline on Integrity Assurance and Control in Database Administration (affixed).

Qualifications: This Guideline is planned for use by data administration and database security personnel in those agencies that use generalized database management systems. Because of the nonstandard nature of DBMS software, and the range in size, complexity, usage, and integrity requirements of Federal data, not every issue discussed in this document will be critical to every agency. However, the fundamental approach to integrity verification addresses universal problems, and is applicable to all Federal database environments.

Where to Obtain Copies of the Guideline: Copies of this publication are for sale by the National Technical Information Service, U.S. Department of Commerce, Springfield, VA 22161. When ordering, refer to Federal Information Processing Standards Publication 88 (FIPS-PUB-88), and title. When microfiche is desired, this should be specified. Payment may be made by check, money order, or NTIS deposit account.

Federal Information Processing Standards Publication 88

1981 August 14

Specifications for

GUIDELINE ON INTEGRITY ASSURANCE AND CONTROL IN DATABASE ADMINISTRATION

CONTENTS

APPENDIX A—DATABASE CONTROLS

CONTENTS

APPENDIX B—CHECKLIST FOR VERIFYING DATABASE INTEGRITY

CONTENTS

1. INTRODUCTION

1.1 Objectives

Database administration covers a broad span of activities. The activities range from working with management in order to accomplish the agency's mission to assessing the adequacy of controls on highly sophisticated database technology.

This Guideline is designed for those people responsible for examining and verifying the accuracy and completeness of the database, as well as for those responsible for the establishment of controls. The intended audience includes database administrators, data administrators, database security officers, and others concerned about control. The Guideline is designed to provide these individuals with an overview of the integrity issues that need to be addressed by the database administration function, together with immediately implementable solutions for the design of database technology controls. The Guideline also provides a methodology for verifying database integrity—a suggested process designed to assess whether or not controls are operational, and the extent to which they are effective in achieving control objectives.

1.2 Defining Database Integrity Assurance and Control

Database and related terminology are used in different ways by different people. The following definitions are provided to avoid ambiguity in using this Guideline:

Database integrity [NBS 76b]—The state that exists when the computerized data in the database is the same as that entered into the database management system (DBMS) and has not been exposed to accidental or malicious alteration or destruction.

Database management system (DBMS) [NBS 80a]—A DBMS is a software package designed to meet common application goals by:

a) Providing features and preprogrammed functions to organize and process many different types of data in an integrated structure called the database.

b) Providing for database definition in generic or logical terms, independent of physical storage and machine-dependent factors.

c) Facilitating the rapid and economical development of many applications.

d) Providing a rather complete operational facility, with features for security, error recovery, monitoring, etc.

Database [NBS 80a]—A data collection so organized for computer processing as to reduce duplicate storage and improve the independence of the stored data structure from the using program(s).

Database administration (DBA)—A function concerned with the technical design and maintenance of databases used in information systems. Database administration is a highly technical activity which requires significant technical training.

Data administrator—The manager of an organization's data, responsible for the specification, acquisition, and maintenance of the database software, and for the design, validation, and security of the files or databases.

Distributed database—A logical integration of enterprise-related databases, which are physically stored in a network of geographically dispersed computers.

Database issue—A problem or concern which is either unique to or increased in a database environment. Any database issue requires identification, analysis, and control, as it can result in an unacceptable exposure to the enterprise.

Exposure—An exposure is the probable result of the occurrence of an adverse event, such as the destruction that could be caused by a fire.

Control—A control is anything that tends to prevent, detect, correct, or reduce an exposure.

Evidence—The information produced by or about the operation of database technology, such as the DBMS log of processing events.

1.3 Need for the Guideline

Database management systems can be an effective and efficient tool to improve the management and control of data maintained in a computer-based system. However, the effectiveness of the database system depends on proper planning and control. An extensive study by the General Accounting Office [GAO 79] concluded that Federal agencies need to receive technical assistance on the proper use of database technology. The GAO concluded in 1979 that most agencies did not adequately plan before acquiring database management systems; consequently, they may have spent substantial amounts for automatic data processing resources that they did not need.

The GAO report stated that in February 1974, 925 data processing installations had acquired one of the six major DBMS software packages, but by October 1977 that number had increased to 3,720. There is no reason to believe that the growth trend has subsided since 1977.

The database approach emphasizes that data can be managed as an organizational resource separate from the operating uses for which it was acquired. Data is no longer dedicated to use by a single individual. function, or application program. As Federal agencies accept this approach, corresponding organizational and operational changes may occur in the agency to maximize the use of database technology. Closely related to these changes is the need for new methods of control and new methods for verifying data integrity.

1.4 Legislation and Database Technology

The Brooks Act (Public Law 89-306), which was passed in October 1965, provides for the economic and efficient purchase, lease, maintenance, operation, and use of ADP equipment. Database technology is but another advance in the use of ADP resources. Each Federal agency has responsibilities for the economic and efficient management of its own ADP resources.

Office of Management and Budget Circular A-71, Transmittal Memorandum No. 1, [OMB 78] requires each agency to establish a management control process to assure that appropriate safeguards are built into all new computer applications. Database technology introduces new risks to agencies. Each agency is required to protect database technology against unwarranted, unauthorized, and illegal uses of that technology.

A major impetus for the passage of the Privacy Act of 1974 was the ease of accessibility of data about people. Database technology facilitates this ease of accessibility. The Act states that the increasing use of computers and sophisticated information technology has greatly magnified the harm to individual privacy. The Act identifies when the information on an individual needs to be protected and states the type of disclosure required by the agency responsible for the application system.

2. OVERVIEW OF DATABASE TECHNOLOGY

Database administrators and database security officers need to understand how database technology affects the accuracy, completeness, and security of data. The overview of database technology presented in this section is designed to emphasize database integrity. Database technology will be divided into its functional components. References are provided explaining basic concepts for those needing to understand how a database system works technically. This section is designed to provide a technological framework for building and reviewing database controls.

2.1 Difference Between Database and Nondatabase Technology

Database technology provides for a concurrent sharing of data among multiple users. This is in contrast to nondatabase technology in which sharing, if it occurs, is sequential rather than concurrent. It is these differences between database and nondatabase technology that provide the systems opportunities as well as the integrity challenges. The following are the differences:

- **File maintenance is a centralized function**

A single software package administers the data used by application systems. This software package, the DBMS, is interposed between the set of application programs using the data and the operating system that reads and writes data to a physical storage area. It manages the data for each application program so that the program need only ask

for specific pieces of data and they are delivered. The DBMS maintains whatever indices are needed in order to translate application program data needs into the information needed by the operating system to read or write data to the physical database.

- **Data management is organizationally independent of applications development**

The DBMS is managed by data administration personnel who are, in general, organizationally independent of the application users. It is frequently unnecessary for the user of an application or the application system personnel to understand how data is retrieved for use by the application. Those functions of application programs that would have been designed by programmers in non-DBMS technology to structure the data are now provided by the data administration group.

- **Data is organized into complex data structures**

The technical complexities of databases should not be underestimated. Normally, sophisticated software packages are needed to aid in the design, maintenance, reorganization, and verification of the integrity of the database. It is not uncommon for the indices to consume one-fifth to one-third of the total database storage space.

A single write command may cause the execution of thousands of computer instructions needed to update the indices, pointers, and overflow areas. This is essential to ensure the continued integrity of the database.

- **Data can be shared concurrently**

A major advantage of database technology is the ability of multiple users to share the same piece of data concurrently. This ensures consistency and reliability of data throughout all the applications using any particular data element. However, this concurrent sharing poses both a technological and an integrity problem.

The technological problem of concurrent sharing is to protect against the loss of data updates. For example, if two users were permitted to update the same data element, one update would overlay the other. This would cause one of the updates to be lost randomly or to be garbled.

The integrity problem relates to the sequence in which those updates occur. In some processes, the order of update is important. For example, in an invoicing operation, all of the items ordered should be accumulated before sales tax is calculated. These are normally application system concerns, but ones which need to be considered during the database application design.

2.2 Understanding the Database Structure

The database structure must be viewed from three perspectives. These are the physical, logical, and individual user's view of the data. The database administrator is concerned with the physical and logical view of the database, while the user and application system personnel are interested in the user view of data. To design or verify database integrity requires an understanding of all three views.

The physical view of data shows where data is physically stored on a data storage device, while the logical view explains how the data elements interrelate. The structured architecture (e.g., hierarchical, network, or relational) is used to describe the logical view of data. That subset of the database used by any individual user is considered to be the user view of data.

All three views of data must be controlled. It is important to ensure the integrity of the physical, logical, and user's view of data. Later sections of this Guideline will describe the methods of ensuring the integrity of the different data views.

2.3 Components of a Database Environment

Control does not start or stop with the physical database and is not limited to the hardware and software of database technology. Control includes the database personnel, and the policies, procedures, and activities supporting the data managed by the database administration function. Only when viewed in its totality can the adequacy of control be determined. Understanding the special characteristics of a database environment explains what must be controlled.

- **A database uses a single software package called a database management system**

In a database environment, data is organized and maintained independently of the programs that use that data. Many of the file integrity functions previously performed by application programs are now performed by the DBMS. These functions include organizing the data, verifying the completeness of data, and providing for the backup and recovery of that data.

358-178 O - 82 - 2

- **The database architecture affects the user's approach to the database**

Databases are currently designed using hierarchical, network, or relational structures. The architecture of the structure determines how one item of data is related to other items of data. Hierarchical databases are composed of relationships that begin at the top and extend downward. Network structures are more flexible in that they enable downward relationships to cross hierarchical boundaries. Relational databases permit almost unlimited flexibility in that a direct relation or access between any two pieces of data is achievable.

There is the normal tradeoff between flexibility and efficiency. A hierarchical structure is the most efficient but the least flexible, while a relational one is the most flexible but the least efficient. Some of the inflexibility of hierarchical databases can be overcome through redundancy of data. When the same data item is needed in two parts of a hierarchical database, it may be duplicated in both segments. This common practice leads to a concern over consistency of redundant data.

- **Data dictionaries structure and formalize data documentation**

Since multiple users share common data, it is important that each user understand the content, reliability, timeliness, and consistency of the data. This type of information needs to be documented in a standardized format comprehensible to all users. A data dictionary system (DDS) can fulfill that need.

A data dictionary system is a software package used to record, store, and process information about all of an organization's significant data entities and associated data processing function [NBS 80b]. Many DDSs are specifically tailored to operate in conjunction with a DBMS, requiring the DBMS facilities to perform DDS functions. Others are self-contained software packages. Either type can be used to ensure consistent data definition and usage within an organization.

- **A special database administration function needs to be made responsible for the technical functioning of the database**

Databases are technically complex. The structuring and maintenance of the database requires a matching of the technological capabilities with the organization's needs. After design, the database must continually be fine tuned to ensure an acceptable level of performance and to meet the changing needs of users.

- **The data administration function establishes data policy**

Data policy describes the organizational philosophy of data. The data policy should be developed by management, possibly through a data administrator, to explain to users management's intent for the use of data. The data policy should cover such things as security, accessibility, retention, accountability, and documentation.

In smaller organizations, database administration and data administration may be combined. When combined, the emphasis of the function is normally dependent upon the background of the managing individual. When the manager is an administrator by training, the emphasis is normally on policy and data usage, while a software specialist in that job emphasizes the technical performance of database software.

2.4 Database Activities

Attempting to ensure the integrity of the large and technically complex database environment in its totality is analogous to attempting to computerize a large segment of an organization at one time. Experience has shown that it is better to divide complex tasks into a set of simpler activities.

The database environment should be divided into separate activities for the purposes of control design and verification. The activities discussed in this Guideline—planning, administration, operation, and use of database technology—have been selected because they emphasize the need and the location of the placement of controls.

- **Planning for database technology**

Implementation of database technology normally requires more planning than is required for nondatabase technology. This additional planning is needed to ensure that the user requirements can be accommodated by the available DBMSs, and that a database can be economically designed to meet the user requirements.

The objectives of planning for database technology include assuring that:

information is used as an organizational resource,
use of the database is optimized,

data definition structure satisfies the needs of users,
application design conforms to standards,
new applications utilize the database properly,
data definition and use is consistent among users, and
data redundancy is controlled.

- **Administration of database technology**

The data administration activity includes data definition, data security, and the design and maintenance of the data structure. With increasing frequency, data definition is performed using a data dictionary system. In some organizations, data security is defined through the DDS, while in other organizations it is accomplished using data security software. The security requirements should be incorporated into a profile of users and programs. This profile becomes the basis for implementing controls over access to resources.

The database structure selected should be designed to meet both current and future requirements. Once the data structures are selected, it is normally costly and time consuming to change from one to another.

- **Operation of database technology**

The operational activities of the database administrator include day-to-day processing, backup, restart, and recovery. Operations personnel must not only process work correctly, but also provide for sufficient backup and recovery procedures to ensure the continuity of processing in the event of database failures. Computer operations personnel make extensive use of utility programs in the fulfillment of their responsibilities.

The recovery of a damaged database is stated by many to be the most technically complex part of database technology. This is particularly true when the database is coupled with data communications. Recovery is a three-part process. First, the database must be duplicated at points of known integrity. Second, data that can be used to reconstruct the database must be continually collected. Third, when a malfunction has been identified, the process to recover the database from the point of last known integrity must be performed.

- **Use of database technology**

Activities of all users of an operational database system should be controlled. The three categories of database users are end users of application results, application systems and programming personnel, and database specialists. The end users use the data within the database, while the other two groups of users interface with the database structure. The needs and responsibilities at each type of user interface should be defined, and those users then restricted to those accesses needed to fulfill their responsibilities.

2.5 References for Understanding Database Technology

People with database technology control responsibilities need to understand how a database works. The following references may help to improve understanding (note that a more extensive bibliography is included at the end of this Guideline):

1. *An Introduction to Data Base Systems, 3d Edition* by C. J. Date
2. *Data Base Management Systems* by D. Tsichritzis and F. Lochovsky
3. FIPS Pub. 77, *Guideline for Planning and Management of Database Applications*, National Bureau of Standards, 1980
4. NBS Special Publication 451, *Database Directions—The Next Steps,* National Bureau of Standards, 1976
5. *Data Base Management*, AUERBACH Publishers, Inc., 1976
6. "Database Management Systems," March 1976 issue, *Computing Surveys* (ACM)
7. FIPS Pub. 76, *Guideline for Planning and Using a Data Dictionary System*, National Bureau of Standards, 1981

3. IMPLICATIONS OF DATABASE TECHNOLOGY FOR THE ORGANIZATION

The implementation of database technology can significantly alter the data processing function in an organization. It not only affects the way data processing applications are designed and operated, but affects the organizational structure itself. These implications of database technology for the organization need to be considered in the selection, implementation, and operation of database systems.

3.1 How Database Technology Can Be Used by an Organization

Database technology can be implemented in different ways in different organizations. In some organizations, conversion to database technology is almost as simple as unplugging an index sequential access method from an application system and plugging in database technology. At the other end of the implementation continuum, the entire method of conducting business in the organizational structure may be significantly changed as the use and control of data become more centralized.

- **Database technology as an access method**

A simple application, or related group of applications, uses database technology as an access method. As such, its use is similar to any other access method provided by a vendor. The processing capabilities correspond to those normally provided by a direct access method.

- **Database technology allows data to be shared among multiple users**

The same data is used concurrently by multiple users. Database technology controls the uses of data to ensure continued data integrity.

- **Database technology is used for multiple unrelated databases**

Two or more databases are established, each administered by its own DBMS. There is little or no sharing of data among the databases.

- **Database technology is used for multiple related databases**

There is redundant data in two or more physical databases, each administered by its own DBMS. The database administration function has the responsibility to ensure the consistency and reliability of the redundant data distributed among the multiple databases.

3.2 Planning for Database Usage Is a Time-Consuming Function

A report issued by the Comptroller General of the United States in June 1979 [GAO 79] concluded that "Most (of the) agencies GAO visited did not adequately plan before acquiring a database management system; consequently, they may have spent substantial amounts for automatic data processing resources that they did not need." The study went on to state that "If not properly planned and controlled, the systems can be complicated and costly, providing management with more problems than solutions or benefits."

When database technology is used for other than an access method, extensive planning is normally required. Some of the more common reasons for the extensive planning are:

- **Multiple uses of the same data**

With multiple users of the same data element, the agency must take special steps to ensure the accuracy and completeness of the database.

- **Restrictions inherent in each DBMS**

Each database system has a specific set of capabilities. For example, a DBMS may only provide for one database structure (e.g., hierarchical) and a limited number of subschemas. These types of restrictions limit both the current and future capabilities available to an organization in achieving its mission. Without sufficient planning, requirements may not be sufficiently defined to ensure the proper matching of needs with a DBMS' capabilities.

- **Coordination is needed among multiple users**

The sharing of data among multiple users normally requires some redefinition of data and extensive data documentation. Each user must understand the capabilities and limitations of database technology. Frequently there are diverse consistency and reliability requirements which must be resolved.

- **System design restrictions**

The design and extension of application systems interfacing with database technology are restricted by the capabilities incorporated into the data structure. Requirements not incorporated may be too costly to implement after the structure has been defined. Planning must ensure that both current and future information needs can be satisfied with the data structure design.

- **Greater need for data security**

The consolidation of data into a single location increases the need for security. The military early recognized this fact. When large amounts of unclassified data were stored in a single database, the classification of that database as a whole would increase over that of any single data item. The planning function must assess the security and privacy requirements when large amounts of data are combined and accessible to users [DENN 79].

- **Extensive training may be required**

Several weeks of training are necessary to introduce a programmer or systems analyst to database technology, and it may take him or her 6 to 12 months to become proficient. In addition, user, operations, and database administration personnel may also require extensive training. Planning should identify the amount and cost of training required to effectively use database technology.

3.3 The Organizational Responsibilities May Need To Be Changed

A number of changes in responsibilities may occur as a result of introducing database technology to an organization:

- **User responsibilities shift to a centralized function**

The implementation of database technology centralizes many of the responsibilities previously performed by users. For example, the function of formal data definition, data security, data integrity, and the backup and recovery of data may be assigned to a centralized database administration function. The functions of data administration and database administration generally emerge as a result of using database technology. However, the user is still accountable for data and its usage.

- **Senior management becomes involved with computerized data**

Database technology is shared by many users on the same organizational level. Without senior management involvement, these units of equal authority may disagree over data definition and usage, and thus impede the implementation of database technology. The type of data definition needed includes:

Consistency of data
Reliability of data
Timing of data
Responsibility for data
Definition of authorized users of data

- **Responsibility for data security becomes explicit**

The responsibility for data security should be assigned to a specific individual or group. The individual responsible for the security function is frequently called a security officer. This security officer function may or may not reside within the data processing area. Responsibilities normally include the definition and enforcement of access and data usage, which may be a full or part-time job. Specific requirements for this function are defined in Office of Management and Budget Circular A-71, Transmittal Memorandum No. 1, [OMB 78].

- **Independent quality assurance review of procedures are instituted**

An important aspect of database technology is the establishment of standardized procedures and methods for interfacing with and using the technology. Some organizations have established a quality assurance function, independent of the DBA, to oversee the use of database technology to ensure the reasonableness and consistent use of standards, the achievement of organizational objectives, and the effective use of the technology.

- **Database technology use becomes centrally coordinated**

Users of database technology need a central point to go to for information and coordination. This administrative function assists users in defining data, using data, and explaining the procedures to follow to interface application programs to the database through the DBMS.

3.4 Additional Operating Procedures Are Required

The operation of database technology is more complex than the operation of older technologies. This complexity is reflected in the functions needed to support day-to-day operation. Normally, this requires highly skilled operators,

especially those skilled in the use of recovery procedures which involve DBMS utilities. The specific areas requiring attention include:

- **Backup of data**

In the event of a failure involving a database, processing must be restarted from a point of known integrity. This requires backup databases and backup transaction data from the point in time at which the duplicate database was created, together with all of the utilities and procedures needed to perform the recovery process.

- **Recovery from DBMS failure**

The recovery operation involves notification of users, assembling of backup data, operation of recovery process, verification of integrity of the database after recovery, and restarting operations at the point where the last processing transaction occurred prior to the failure.

- **Reorganization of database**

Reorganization rearranges the data in the database both physically and logically. The procedure is necessary to reallocate storage to encompass current user data needs and to improve database performance. The reorganization process should not change data within the database if there is not a sufficient audit trail in the process. Utility programs are needed both to perform the reorganization and to verify the integrity of the database at the conclusion of the process.

- **Monitor DBMS performance levels**

One of the characteristics that determines when reorganization is needed is the level of performance of the DBMS software. As performance is downgraded due to inefficient space utilization, the monitoring process should signal the need for reorganization. Good monitoring techniques are also effective in identifying an inefficient mix of transactions and a data structure that is inappropriate to meet the organization's needs.

3.5 Database Technology Requires New Control Methods

The following outlines the changes caused by the introduction of database technology leading to new methods of control:

- **Database usage creates new activities**

In the establishment of the database, new activities are created, such as the database administration function and the interface procedures needed to use the DBMS. These are activities that did not exist prior to the use of database technology, and which can cause shifts in responsibility.

- **New activities cause new concerns**

Associated with the implementation of new activities and changes in responsibility is the challenge of mastering new technology and using it effectively in the organization. Organizations normally have no previous experience with new technology, and thus in many instances may not be fully aware of the exposures to their organization caused by those new activities. Part of the planning process is to identify those concerns and exposures.

- **New concerns need new methods of control**

Controls used before the introduction of database technology may not be effective in a database environment. For example, controls designed for systems analysts who manage their own data files are not necessarily applicable to a centralized function which administers data for multiple users. The new technological processes may raise concerns within management about the ability of the technical personnel to successfully control and monitor that technology. The database planning process should outline the methods of control deemed effective for reducing the identified database technology concerns.

3.6 Database Verification Requires New Methods and Tools

Verification of the integrity of a database involves the assessment of controls and the examination of evidence. New methods of control may produce new forms of evidence. For example, evidence from an automated database

verification process or a DBMS log of transactions may be needed to verify the integrity of the database. Those individuals responsible for verifying database integrity may need new tools for the following reasons:

- **Application data is stored in the database**

A verification process for an application file in a nondatabase environment encompasses a single application and a single file. In a database environment, multiple applications may use a single data item. Thus, database integrity may need to be verified prior to verifying the applications's use of that data.

- **Database technology changes evidence**

The verification of the integrity of a database normally involves the examination of evidence. Examples of evidence include documented recovery procedures, DBMS logs, database verifier reports, etc. This evidence may be significantly different than nondatabase evidence.

- **Existing verification tools may not be effective**

The software tools used to verify the integrity of a file may not be effective when database technology is used. Unless those tools have the capability to access and analyze information contained in the database, new tools will be needed.

- **Applications are dependent upon DBMS controls**

Many application responsibilities may shift from the application area to the centralized data administration area. The implementation of those responsibilities is frequently automated through database technology. Thus, the application becomes dependent upon the adequacy of the DBMS controls to ensure the continued integrity of data. The verification of the adequacy of application processing should begin with verification of the adequacy of the controls over database technology.

4. DATABASE TECHNOLOGY ISSUES

4.1 Overview of Database Technology Issues

A database issue is loosely defined as a cause of potential database technology problems. Database technology issues included in this section are designed to illustrate the concerns that must be addressed by database administration personnel. The applicability of any issue to an agency will vary with the extent of use of database technology by that agency and the amount of attention paid to control. These issues are listed and briefly described in figure 4-1. The remainder of section 4 provides a more detailed explanation of each issue, together with some self-analysis questions about that issue. The objective of including the self-analysis questions is to aid personnel in assessing the applicability of that issue to the agency. "No" answers to these questions are designed to indicate that if the issue is not addressed it may cause problems for that agency.

Section 5 describes the types of controls available to database administration personnel to cope with these issues. The specific controls that are used to control database technology are described in detail in appendix A. The purpose of the appendix is to explain the control, describe how to use the control, and discuss the type and collection of the evidence that should be produced. Section 6 explains, in step-by-step format, how to assess the adequacy of database controls.

4.2 Explanation of Database Technology Issues

The database technology issues discussed in this section are:

#1 Inadequate assignment of responsibilities

Database technology creates new activities, such as administering and coordinating the use of common data. These activities may cause a shifting of responsibilities. Responsibilities residing in user areas when users process dedicated data shift to a centralized area when data is centrally administered.

Two "assignment of responsibility" concerns surface when responsibilities are shifted. The first concern is the concentration of responsibilities in a central location, which may reduce or eliminate some of the checks and balances

#	Database Technology Issue	Description of Issue
1.	Inadequate assignment of responsibilities	Inappropriate segregation of duties
2.	Inaccurate or incomplete data in a database	The integrity of data entered in the database is lost due to inadvertent or intentional acts
3.	Losing an update to a single data item	One or more updates to a single data item can be lost due to inadequate concurrent update procedures
4.	Inadequate audit trail	The use of data by multiple applications may split the audit trail among those applications and the DBMS audit trail
5.	Unauthorized access to data in a database	The concentration of data may make sensitive data available to anyone gaining access to a database
6.	Inadequate service level	Multiple users contesting for the same resources may degrade the service to all
7.	Placing data in the wrong calendar period	Identifying transactions with the proper calendar period is more difficult in some on-line database environments than others
8.	Failure of DBMS to function as specified	Most DBMSs are provided by vendors, making the data administrator dependent upon the vendor to assure the proper functioning of the software
9.	Fraud/embezzlement	Systems that control resources are always subject to fraud and embezzlement
10.	Lack of independent database audits	Most auditors are not skilled in database technology and thus have not audited database installations; in addition, many auditor software packages cannot access a DBMS
11.	Inadequate documentation	Documentation of database technology is needed to ensure consistency of understanding and use by multiple users
12.	Continuity of processing	Many agencies rely heavily upon database technology for the performance of their day-to-day processing
13.	Lack of cost/benefit analysis	Without established performance criteria, an agency cannot be assured that it is achieving database goals
14.	Lack of management support	Without adequate resources and "clout," the advantages of database technology may not be achieved

FIGURE 4-1. *Description of database technology issues*

that were present prior to centralization. Second, when responsibilities move, some tasks may not be performed. This occurs when responsibilities are not clearly defined and documented because each of the parties involved may assume the other party is still fulfilling the task.

The insertion of a database administration function into the design and operation of application systems creates a need for additional communication. Nondatabase systems normally involve only ADP systems programming personnel and users. With the advent of database technology, the database administration function frequently encompasses the system development and operation process. This new arrangement requires increased, and more formal, communication.

Self-assessment questions ("No" answers may indicate potential problems):

1) Has the reassignment of responsibilities associated with a database environment been formalized (i.e., revised job descriptions, department charters, etc.)?
2) Has a formal method of resolving data definition disputes been established?
3) Have the database administration activities been restricted to those required by that function?

#2 Inaccurate or incomplete data in a database

The need for accurate and complete data increases as more uses are made of that data. An inaccurate data element in a dedicated system only affects that system, but in an environment where multiple users use the same data the severity of the problem can be magnified manyfold. The advantages of the database can only be achieved when the integrity of the database can be ensured.

The database administrator should take the steps necessary to ensure accuracy and completeness of data entered into the database. Because of the multiple uses of data, additional resources should be allocated to the validation of input. The validation rules should be specified along with the definition of data in the data dictionary.

A difficult problem for many database organizations has been assuring the consistency of data that is deliberately redundant in the database. Many database administrators feel they do not have adequate tools and techniques in this area.

Self-assessment questions:

1) Have the validation rules for each data element been documented in the data dictionary?
2) Do you have procedures established to ensure the consistency of redundant data elements?

#3 Losing an update to a single data item

Database technology permits multiple users to concurrently access, and perhaps update, the same data element. Most database management systems have lockout procedures to prevent the second individual wishing to update a data element from doing so until the first is finished with his or her update procedure.

Equally important is the correct sequencing of events. For example, if a sequence of events is to modify pay rates and add and delete employees, the action should occur prior to the payroll calculation step. Database applications need to determine that appropriate controls are established to ensure the proper sequencing of events.

Self-assessment questions:

1) Does your DBMS have a lockout feature to prevent concurrent updates to a single data item?
2) Does your agency have a procedure to ensure the proper sequencing of events in database applications?

#4 Inadequate audit trail

Database technology has two audit trails; one for the applications using the database and one for operations to reconstruct processing. The audit trail is needed both to substantiate prior processing should the integrity of processing be questioned and to reconstruct processing should problems occur. The audit trail includes source documents, and computer logs and files, as well as the procedures and documentation needed to understand and utilize the audit trail. The database administration function should assist in the design of both audit trails because in some instances the data from both will be needed to prove or restore processing integrity.

The application audit trail should provide the capability to trace source documents to control totals, and to identify all the source documents supporting the control totals. The database audit trail should contain sufficient information to enable transaction processing to be reconstructed. The audit trail needed to accomplish all these objectives may be quite extensive.

In dedicated applications, the audit trail is normally easy to follow, provided sufficient data has been retained. However, in a database environment, following the audit trail is much more complex. First, the trail is split among multiple applications and the database itself. This makes identifying and obtaining the needed evidence more difficult technically. Second, the database audit trail is frequently enormous in scope. It is not uncommon to produce several hundred thousand audit trail records in one day. This is particularly true when the DBMS is accessed using sophisticated data communication technology.

The database administrator needs to determine that the audit trail has been clearly established, identified, and documented. In addition, it is important to determine the retention time for all parts of the audit trail. The voluminous DBMS log records may have a much shorter audit trail life than the application audit trail.

358-178 O - 82 - 3

Self-assessment questions:

1) Has the audit trail for database application processing been identified and documented?
2) Has the retention period for each part of the database audit trail been determined?
3) Can the audit trail trace source transactions to control totals and trace control totals back to the initiating transactions?
4) Can the audit trail provide the evidence needed to reconstruct transaction processing?

#5 Unauthorized access to data in a physical database

The accessibility control issue in a centralized database environment is increased when the DBMS is accessed on-line. Agency management must be concerned with both unintentional and intentional unauthorized access.

The database administration function should match user needs with database resources. Users should then be restricted to accessing only those elements of data for which they have a need. "Users" should be defined in the broad sense here, to include database administration, operations, and data processing systems personnel.

Current DBMSs offer many opportunities to achieve sufficient access control. Specific users can usually be restricted to specific subsets of the database. In more sophisticated systems, access can be restricted according to the type of data usage. Some data might be read only, other data might be accessible or not based upon the value of the data. For example, access to pay rates in a payroll application could be restricted, for clerical personnel, to those not exceeding $10 per hour.

Many organizations have established a database security officer function to enforce access rules. The security officer normally develops a profile of user, which becomes the specification for designing access authorization systems.

Self-assessment questions:

1) Have you established a user profile for your users which defines data access rules?
2) Have you automated the enforcement of your user profile?
3) Have you established the function of database security officer?

#6 Inadequate service level

Providing multiple users concurrent access to data may create a service level problem. One user can downgrade the service level for other users by consuming too large a portion of the database resources. In addition, if the database structure gets out of synchronization with user requirements the time required to satisfy requests may become excessive.

The database administration function should continually monitor the service level to users. As the service level begins to deteriorate, the DBA should fine tune the database to improve service.

Three options are available for improving service. First, the database structure can be reorganized to make it more responsive to user needs. Second, it is sometimes possible to encourage users to spread out their service requests in order to avoid peak service periods. Third, additional hardware and software can be added to improve performance.

Self-assessment questions:

1) Do you have procedures established to monitor the service level to users?
2) Do you encourage users, by the use of such techniques as varying charge-out rates, to spread out their nonurgent processing?
3) Have you explicitly identified the options available to improve service when it degrades, such as database reorganization?

#7 Placing data in the wrong calendar period

The placement of events into the proper calendar period is very complex in a database environment, and becomes even more so with continuous on-line processing. In some systems, events are entered and stored awaiting the appropriate processing date to occur.

Some database organizations time stamp transactions so that they can be recorded in the appropriate accounting period regardless of when they are entered into the database. This accounting period identification avoids any ambiguity caused by the time of entry, but requires additional processing time and storage space.

Self-assessment questions:

1) Is your agency devoid of time dependent data which is aggregated into accounting periods?
2) If such data is processed, has a procedure been established, such as time stamping transactions, so that each transaction can be readily identified with the appropriate accounting period?

#8 Failure of the DBMS to function as specified

Database management systems are complex software packages. Most DBMSs are obtained from independent vendors. In addition, the vendors continually release updated versions of their DBMS.

It is the job of the database administrator to verify the proper functioning of the database software. Each new DBMS release should be thoroughly tested by the DBA before it is put into operation. Agencies, of course, frequently contract for the actual maintenance of the DBMS software.

Should the DBMS not function properly, it could result in substantial erroneous processing due to the heavy use of the database. Database administrators should be alert to DBMS problems, and establish procedures for contractor call-in should problems occur.

Self-assessment questions:

1) Do you thoroughly test each new release of DBMS software?
2) Have you arranged for a maintenance contract for your DBMS?
3) Have you established procedures, and trained your staff, to identify DBMS problems?
4) Have you developed backup procedures to be used in the event of a DBMS failure?

#9 Fraud and embezzlement

The state-of-the-art in integrity management of advanced database technology may be encouraging fraud and embezzlement. No database organization visited in the course of preparation of the guideline had developed procedures for designing either controls of the DBMS or controls of applications using the DBMS. In addition, the GAO survey [GAO 79] of agencies using database technology failed to disclose a single organization which had been audited by its agency's auditors. Integrity management of database technology is just commencing.

Self-assessment questions:

1) Have you been audited recently by your agency's auditors?
2) Have you established a methodology for designing database controls (note that section 5 describes such a methodology)?
3) Do you have procedures to identify and report errors, omissions, and frauds to your management?

#10 No independent database audits

All activities need to be periodically assessed by an independent group. In most organizations, this independent review is performed by internal auditors. Their function is to verify compliance to the organization's policies and procedures, to determine that the operation is adequately controlled, that it is performed in an efficient, effective, and economical manner, and that it meets the intent of legislation.

The initiation of an audit normally occurs outside the database administration function. However, database administrators can request an audit. The objective of making such a request would be to have the adequacy of the database controls reviewed.

Self-assessment questions:

1) Do you have an independent audit agency that is capable of auditing database technology? If so, is it done?
2) Have you had an independent audit of your database technology within the past 12 months?
3) Are you satisfied that controls over your agency's database technology are adequate?

#11 Inadequate documentation

Documentation of a database environment includes documentation of both the individual data items and of the database structure. Many organizations use documentation aids such as a data dictionary system. Many DDSs can document the database structure as well as the data items in the database.

The types of documentation on the database structure that should be kept include [NBS 76a, NBS 79a]:

Principles of the schema
Principles of the subschemas

How security is achieved
Recovery actions
Reorganization changes required

The types of documentation that should be kept on each data element include:

A precise and unambiguous definition
Source of data
Frequency of change
The individual accountable for correctness
Relationship to other data items
Location
Program/individuals authorized access (and the type of access)
Reports in which the data item appears

Self-assessment questions:

1) Does your agency use a data dictionary system?
2) If yes, do you ensure that the information contained in the DDS is the same as that used in practice?
3) Have you developed data documentation standards?

#12 Continuity of processing

The development of database technology has accelerated the incorporation of automated systems into day-to-day processing. A result of this trend is the elimination of hard copy documentation. Individuals use computer terminals to enter information directly into processing, and receive many of the results directly from processing.

As organizations rely more heavily on their automated systems, their ability to continue processing without those systems is diminished. This poses two challenges to the database administration function. First is the development and implementation of those steps necessary to assure the continuity of processing of the automated systems. Second is the development of procedures to aid individuals in the conduct of their business during those periods in which the automated systems are not operational. The completeness of the performance of these two tasks may determine the success of the database installation [NBS 81].

Self-assessment questions:

1) Have you assessed the impact on your agency of a failure of the database?
2) Have you developed procedures to continue doing business during a database failure?
3) Have you taken sufficient steps to ensure that the integrity of the database can be restored after a database failure?
4) Have you documented the sequence of actions necessary to restore applications after a database failure?

#13 No cost/benefit analysis

Many database installations undertake either a cursory cost/benefit calculation or none at all before implementing database technology. The implementation is made solely upon technical recommendations and arguments by data processing personnel. In those instances where there is a cost/benefit calculation, there is often no follow-up made to verify that the costs predicted were accurate and that the anticipated benefits were achieved.

The implementation of the database management system can be costly. Only a small part of the cost is the procurement and installation of a DBMS. Organizations indicate that training and systems redesign costs exceed by many times the cost of DBMS acquisition and installation. The Brooks Act requires Federal agencies to provide for the economic and efficient purchase, lease, maintenance, operation, and use of ADP equipment. This is made significantly more likely by the performance of cost/benefit analyses.

Self-assessment questions:

1) Can you identify the costs associated with database technology?
2) Can you identify the benefits associated with database technology?
3) Have you performed a cost/benefit analysis for the installation and operation of database technology?
4) If so, have you monitored the installation to measure whether or not those cost/benefit projections have been achieved?

#14 Lack of management support

The costs of acquiring database management systems are generally small compared with the costs of using them in a "true database environment." This requires a long-term management commitment to application software, computer hardware, communications, procedures, training, and support which will cost far more than the DBMS itself.

Senior management support for a true database environment is essential if that environment is to be successful. Not only does database technology centralize many of the application functions, but for most organizations it changes their information processing procedures. Without management oversight and direction, some users may dominate requirements, causing the system to be more responsive to the needs of a few rather than to the total organization.

To guarantee adequate management support, some agencies have established a data administration function. This is a senior management position responsible for data policy, direction, coordination, and arbitration of disputes. Other organizations have established a sufficiently powerful central review board which establishes implementation priorities and oversees the use and extensions of database technology [PAPE 80].

Self-assessment questions:

1) Is the senior management of your agency involved in the selection, implementation, and use of database technology?

2) Have you established a data administrator position in your agency?

3) Have you established, and given sufficient power to, a review board comprised of users, ADP personnel, and senior managers to oversee the use of database technology?

5. ESTABLISHING CONTROL REQUIREMENTS FOR DATABASE TECHNOLOGY

5.1 Need to Control Database Technology

The primary objective of data control is to assure accurate, complete, authorized, and supportable data. This objective remains the same whether the system is manual, computerized using traditional files, or processed using database technology.

In on-line database environments, processing occurs instantaneously, with no time for human oversight. For example, in electronic funds transfer systems, the funds transfer is made within a fraction of a second of the request. The system must rely on the adequacy of the automated controls. If the controls are good, transactions will be processed in accordance with the intent of the agency. If the controls are inadequate, erroneous processing may occur.

This Guideline deals exclusively with database technology. However, applications are comprised of manual processing, automated application processing, and database processing. Control must exist over all three segments of processing, and it is the totality of control that determines the overall adequacy.

The American Institute of Certified Public Accountants Special Advisory Committee on Internal Accounting Control [AICP 78a] stated that without adequate environmental controls (e.g., database controls), it may not be possible to have adequate application controls. Thus, in an agency's control assessment process, it is important to assess the adequacy of database controls prior to evaluating application and manual controls.

5.2 New Database Activities

Problems, concerns, and database issues cannot be controlled. Only activities can be controlled. An activity is defined as a segment of the database operation. The activities used in this Guideline were selected to emphasize control.

For example, one cannot just initiate a control to prevent fraud; the control must be implemented within activities. An agency can restrict data access to authorized users which, in turn, should reduce the probability of fraud. In other words, the agency should install specific controls in the security activity, not simply decree a general control policy stating that fraud is not permitted.

Database activities requiring new methods of control are listed and briefly described in figure 5-1. These activities will not necessarily be independent, since the list was constructed to emphasize those activities which are, in fact, controllable.

5.3 Database Technology Controls

The controls listed in this Guideline were drawn from discussions with database administrators, examinations of organizational standards and procedures, and a search of database technology literature. The listing is not exhaustive but, rather, represents the type of controls that are actually implemented in database organizations.

The list of controls is organized by activity, with many of the controls occurring in more than one activity. The classification selected is typical of the activity in which the control will be found. The control/activity matrix at the end of this chapter shows some of the other activities in which the control can be effective.

Each of the database activities enumerated in figure 5-1 is listed below, together with controls used in that activity. Each control is briefly described in the listing, with a more detailed description provided in appendix A.

#	Controllable Activity	Description
1.	End user interface to the DBMS	Those individuals/programs who need to access data or the attributes of the database structure
2.	Operation of the DBMS	The procedures necessary to use the DBMS in an operational environment
3.	Database administration	Those activities necessary to design, implement, and monitor the DBMS and to coordinate its use with users
4.	Data definition	The documentation of the data elements and database structure
5.	Security/access	Those functions which must be performed to protect the integrity of the database from inadvertent or intentional unauthorized access
6.	Systems development	Those tasks involved in developing applications to use database technology
7.	Backup/recovery/reorganization	Those functions necessary to modify the database structure and to restore the integrity of the database after a database failure

FIGURE 5-1. *Controllable database activities*

- **End user interface to DBMS**
  1) *Program modification and maintenance control*—Ensures that the proper change is installed in the proper version.
  2) *Adequacy of programmed input validation check*—Programmed routines to verify the accuracy, completeness, and authorization of input.
- **Operation of the DBMS**
  3) *Access authorization control*—Ensures that only authorized individuals gain access to database resources.
  4) *Data error handling*—The procedures and timeliness used in examining and correcting detected errors.
  5) *Remote data transmission control*—The terminal controls needed to assure that data is not lost at the terminal site.
  6) *Central data transmission control*—Ensures the accuracy and completeness of the communication system for the entire network.
  7) *Processing intent*—Explains the objective of management in processing a specific transaction.
  8) *Concurrent data control*—Ensures that data elements will not be misprocessed due to two or more users processing the same data element concurrently.
  9) *Deadlock detection and resolution*—Breaks a stalemate in processing between two users.

- **Data administration controls**

  10) *Assignment of responsibilities*—Making individuals accountable for their functions.
  11) *Segregation of duties*—Splitting functions so that no one individual has the responsibility for performing a function and at the same time has responsibility for using the results of that function.
  12) *Operation documentation*—Details operating procedures.
  13) *Output control*—Details the procedures for preparing and disseminating output results.
  14) *Rotation of duties*—Limiting the amount of time any one individual has day-to-day responsibility for an operating task.
  15) *Processing performance standards*—The establishment of criteria to measure economy, effectiveness, and efficiency of database technology.
  16) *Risk management team*—A task force comprised of multiple backgrounds identifying the concerns and problems faced when using database technology.

- **Data definition controls**

  17) *Centralized coordination of external schema*—Placing the responsibility for coordinating external schema definition in a centralized group.
  18) *Data element responsibility*—Making individuals accountable for each data element in a database.
  19) *Conceptual data independence*—The organization establishes the data definition as opposed to individual user groups.
  20) *Data dictionary system*—An automated documentation tool for data.
  21) *Active data dictionary system*—The documentation in the data dictionary is fed automatically into the operating environment.

- **Security/access controls**

  22) *Physical barrier*—A physical restraint preventing individuals from accessing database technology.
  23) *Surveillance*—The use of guards or electronic equipment to detect penetration.
  24) *Database malfunction reporting*—Reports to management identifying the type and severity of problems occurring with database technology.
  25) *Natural disaster and environmental protection*—Taking the measures necessary to protect database technology from acts of God and man, such as fire, earthquake, etc.
  26) *Maintenance plan*—A predetermined schedule for performing maintenance to correct problems before they occur.
  27) *Security officer function*—Appointing one individual accountable for security of database technology.
  28) *Security profile*—A matching of user needs to database technology capabilities.
  29) *Passwords*—A secret code or word that individuals or programs must know in order to gain access to database technology.

- **Systems development controls**

  30) *Database administration function*—A function that establishes interface standards for systems under development and advises systems analysts and programmers on database technology capabilities and interface procedures.
  31) *Application system testing*—Methods of assuring that operational systems cannot adversely affect the database.
  32) *Formal design process*—The use of structured methods or automated tools and techniques to aid in the design process.
  33) *Top management checkpoints*—A series of steps throughout the developmental process at which top management will make a decision regarding performance and continuance of the project.
  34) *System implementation standards*—Methods and procedures that must be followed when implementing systems using database technology.
  35) *Database standards*—Methods and procedures that must be followed when establishing and operating a database.
  36) *Training of personnel*—Providing those courses and materials needed to provide appropriate skills for people using database technology.
  37) *System documentation*—Sufficient formal written explanation of the database environment so that its continuity and maintenance can be assured.

38) *Review board*—A group of managers, users, and database personnel who oversee priorities and projects using database technology.
39) *Government reporting requirements*—A formal method of assuring that the use of database technology is in compliance with Federal regulations.
40) *Personal privacy requirements*—Methods and procedures of assuring that an individual's privacy has not been compromised through database technology.

- **Backup/recovery/reorganization controls**

41) *Audit trail*—The ability to trace transactions from source document to control totals and back to source documents; and to reconstruct processing should problems occur.
42) *Recovery procedures*—Automated tools and techniques for recovering integrity of database.
43) *Reorganization utilities*—Automated tools and techniques for restructuring and expanding the database.
44) *Database verifier*—An automated tool to assure that all of the data in the database is properly structured and can be located.
45) *Application system failure*—Procedures for users to continue operations in the event their applications are not operational.
46) *Backup databases*—Copies of databases made at specific points in time to use for recovery purposes.

5.4 Integrity Issue/Activity Matrix

Controls are installed within activities for the purpose of addressing specific integrity issues. If an organization deems that a specific integrity issue needs to be addressed because the potential problem or loss due to that issue is greater than the organization wishes to accept, it needs to determine appropriate controls. The integrity issue/activity matrix is designed to aid in that process.

The matrix lists the integrity issues from section 4 in the left-hand column, and the database activities from this section across the top. The controls used over database technology have been briefly described in this section and further explained in appendix A. The matrix shows which of the controls (by control number) are effective in reducing which integrity issue.

The matrix can be used both to design and to verify the adequacy of control. For example, if the integrity issue of inaccurate or incomplete data was a concern in the recovery process, then the individual responsible for recovery would need to select a control. The matrix shows that a control effective over this integrity issue is the use of a database verifier. The same process can be used by an individual charged with verifying the adequacy of control. If that individual wanted to know how the recovery process reduced the probability of inaccurate or incomplete data, the matrix would lead that individual to inquire as to whether or not a database verifier was used at the completion of the recovery process.

This matrix is not meant to be comprehensive in documenting all of the controls used over database technology. It is recognized that the evolution of database controls is an ongoing process so the designer and verifier should not be restricted to the population of controls included in this Guideline. They are meant to aid in understanding the types of controls that are available to control database technology. Individuals responsible for database technology control may wish to use or find different controls which are equally effective. This effectiveness is a judgmental decision by the designer or verifier.

Database Integrity Issues \ Activity	End User Interface to the DBMS	Operation of the DBMS	Database Administration	Data Definition	Security/ Access	Systems Development	Backup/ Recovery/ Reorganization
1. Inadequate assignment of responsibilities			10, 11 14, 16		27	30	
2. Inaccurate or incomplete data in a database	1, 2	4				31, 32	44
3. Losing an update to a single data item		8, 9				31, 34	
4. Inadequate audit trail				21, 22		34, 35 36, 37	41
5. Unauthorized access to data in a database		3			22, 23, 24 25, 26, 27 28, 29		
6. Inadequate service level		4, 5, 6			24, 26	34, 35	42, 45 46
7. Placing data in the wrong calendar period	2			20		36	
8. Failure of DBMS to function as specified		4, 7	13	19, 20		31, 34 35, 36	42
9. Fraud/embezzlement	2	7	16			36	42
10. No independent database audits			16			38, 39	
11. Inadequate documentation	1		12	20, 21		32, 34 35, 36 37	42
12. Continuity of processing	1, 2	4, 5, 6			22, 23 24, 25 26		41, 42, 43, 44, 45, 46
13. No cost/benefit analysis		7	15			38	
14. Lack of management support	1	7	10, 11, 15		27	30, 33	42

FIGURE 5-2. *Integrity issue/activity matrix*

6. VERIFYING DATABASE INTEGRITY

The objective of this section is to provide a methodology for verifying the integrity of the database. The recommended procedure is pieced together from techniques used by many database administrators, together with good business practices. The entire recommended process is probably not practiced in any one organization, but the use of these procedures should assist those responsible for performing the difficult task of verifying database integrity.

The verification of the integrity of the database is based upon the following three factors:

1) Adequacy of database controls—The stronger the controls over database technology, the easier the verification process.

2) The skills of the individual verifying the integrity—The more skills the individual has in database technology control and evaluation the more effective the verification process is likely to be.

3) Verification methodology—Database technology is highly structured and complex. The verification process must complement the characteristics of the database if it is to be effective.

358-178 O - 82 - 4

Previous sections in this Guideline have explained the need for designing controls. Appendix A explains the more common database controls. This section provides a discussion of the skills needed to verify control and recommends an explicit set of steps to verify database integrity.

6.1 Skills Needed to Verify Database Integrity

The effective assessment of database integrity may require the reviewer to obtain new skills. General skills include a knowledge of: management concepts and practices; the theory of computer systems, operations, and software; data processing techniques; management of the data processing function; security of the data processing function; the theory of database technology; and risk analysis and threat assessment concepts. The specific areas of knowledge helpful in assessing computer technology are outlined in the National Bureau of Standards March 1977 workshop session on "Qualifications and Training" [NBS 77].

Testing of database technology involves four new considerations for the reviewer. These considerations pertain to the database integrity verification skills needed, and are:

1) The individual must have sufficient database technology skills to recognize integrity concerns in the environment and the types and sources of evidence needed to satisfy those concerns.
2) The individual must be familiar with the database verification methods and techniques that need to be utilized in reviewing database technology.
3) The individual must have the technical ability to obtain the needed database evidence.
4) The individual must have the technical ability to evaluate the results of the test.

In order to conduct the test, the individual must possess the following knowledge about the database:

1) The database standards, policies, and procedures (for which compliance is required).
2) The types and location of database controls used.
3) The types and purposes of transactions to be tested.
4) An understanding of the tools and techniques available to assess database integrity.

The individual conducting the review must eventually develop an opinion as to the adequacy of database control. In order to arrive at this opinion, the reviewer must have the following knowledge:

1) A knowledge of the criteria used in developing an opinion regarding the adequacy of controls over database technology.
2) Sufficient knowledge of the database integrity issues so that an assessment can be made regarding the impact of those issues on the agency.
3) Familiarity with management terminology and reporting practices so that the implications of control weaknesses can be appropriately communicated to management.

With regard to training, it is assumed that individuals conducting database integrity evaluations have had the basic education and experience in a discipline such as accounting, business administration, engineering, or computer science that enables them to perform methodical processes. Experience has dictated that efficient and effective reviews of computer integrity require this basic level of education as a foundation on which to build the additional education and experience needed for this work.

In addition to an individual's basic education experience, he/she will need approximately one academic year or equivalent of education in the subjects considered to be components of the common body of database technology knowledge needed for this work. To be efficient and effective in conducting these reviews, it may take an individual an additional 1 to 5 years of on-the-job training or practical experience in performing this work.

6.2 Evidence in a Database Environment

The database integrity methodology presented in this section is designed around the examination of evidence, and the major difference between the verification of database technology and nondatabase technology is the type of evidence produced and evaluated.

The primary reason for the presence of new types of evidence in database technology is the DBMS software package. The file maintenance evidence in a nondatabase environment is incorporated into the application system logic. In a database environment, not only is much evidence transferred to the centralized administration function, but normally it exists in new forms.

The second major reason for the presence of new evidence is the use of a data dictionary system. Many of the attributes of data and file maintenance that were manually maintained are transferred to the DDS. This automatic documentation tool can be integrated with the DBMS so that the rules and specifications included in the data dictionary are enforced in the operating environment. In addition, some data dictionary systems can generate data validation programs, assuming that complete validation rules have been documented in the data dictionary.

Each database environment may have slightly different forms of evidence. Appendix A lists the type of evidence produced by controls. The items listed below, together with a brief description, are the more typical forms of evidence that should be evaluated in verifying the integrity of database technology:

1) *Database management system*—The software package that manages the database.
2) *Data dictionary system*—An automated documentation tool for data.
3) *DBMS logs*—A history of all the transactions occurring during database operations.
4) *Security log*—A listing of accesses and potential security violations.
5) *Database utilities*—A variety of utilities, normally included with the DBMS, that perform much of the day-to-day maintenance on the DBMS.
6) *Database structure map*—A pictorial representation of the database structure. This can be produced by a utility program.
7) *Database verifier reports*—A listing of integrity problems in the database structure. Produced each time the database verifier utility is executed.
8) *DBMS reports*—Periodic status reports produced by the DBMS providing statistics about the content and operation of the DBMS.
9) *Security profiles*—A listing of the resources accessible to individual users.
10) *Database standards*—The required procedures and methods for operating and interfacing with the database.
11) *Organizational charts/job descriptions*—The assignment of responsibility, segregation of duties, and creating accountability for actions.
12) *User complaints/requests*—Documentation of the problems and needs of users.
13) *Master terminal operation procedures*—The process for performing privileged maintenance on the DBMS.
14) *Database operating procedures*—The instructions provided operators for the day-to-day operation.
15) *Database recovery procedures*—The instructions provided operators on how to prepare for and conduct recovery after a database failure.
16) *Database reorganization procedures*—The instructions provided on when and how to reorganize the database.
17) *Database integrity procedures*—The manual methods used by database administration, operations, and user personnel to verify the proper functioning and content of the database.
18) *Database controls*—The guidelines provided users of database to help ensure the integrity of the application data.

6.3 Steps in Verifying Database Integrity

This section covers the recommended approach for verifying database integrity, and is directed primarily to reviewers from outside the DBA function. Reference is made to material, in checklist format, in appendix B. These checklists are designed both to assess the adequacy of control over the database environment and to provide direction to the reviewer on what to do should the integrity be in doubt. Figure 6-1 illustrates the steps in verifying database integrity.

Step 1—Understand the System

Before developing a database integrity strategy, the individual assigned verification responsibility must perform a preliminary review in order to understand the system. The objective of the preliminary review is to gain sufficient insight into the problems, capabilities, and uses of database technology in the organization so that a realistic verification strategy can be developed.

The type of information the verifier should obtain about the system includes:

Type of database technology used. This would identify the DBMS that is used, the utilities available, the computer hardware, other supporting software, and the hours and size of operation.

The application/department/users of database technology.

The types of evidence available for examination by the reviewer (see sec. 6.2 for a listing of database evidence).

Responsibilities of the data administration/database administration functions.

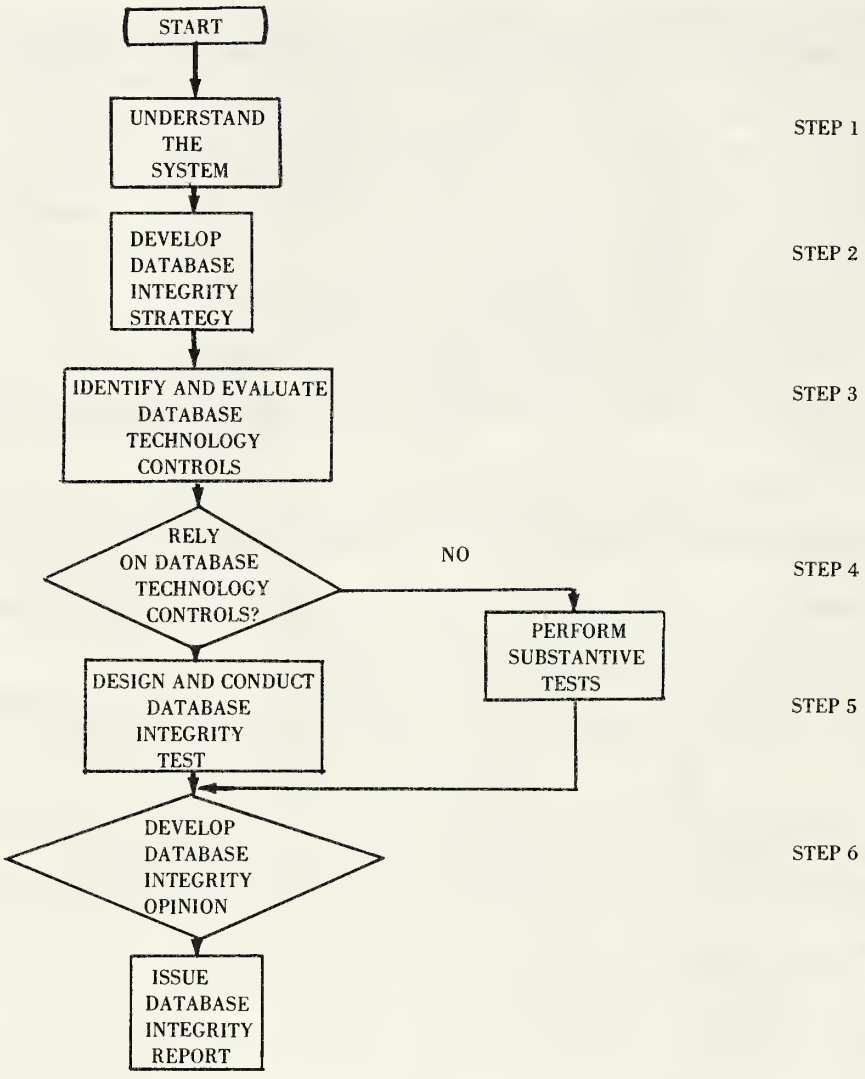

FIGURE 6-1. *Verification of database integrity*

Extent and type of management direction provided over the implementation, use, and expansion of database technology.

Detailed plan for installing, operating, and expanding the use of database technology.

It is a common practice among individuals verifying integrity of computerized applications to develop a checklist for use in understanding the system. The checklist serves the two purposes of reminding the reviewer of those areas where gaining an understanding is helpful to the review, and of documenting the information gathered during this preliminary review. In most agencies, the preliminary review can be accomplished within 1 or 2 days.

Step 2—Develop Database Integrity Strategy

The decision as to whether the database must be reviewed depends upon the reliance the application user(s) places upon the integrity of the database environment. In those instances where the DBMS is used as an access method for a single application, application controls may be sufficient to ensure the continued integrity of the database. This may also be true in very large applications where a single application consumes an entire computer (e.g., social security system). On the other hand, if multiple applications share data, it is normally necessary to verify the integrity of the database environment explicitly.

The tasks that need to be performed, together with a description of those tasks, to develop a database integrity verification plan are:

Task 1: *Identify database integrity issues to be addressed*—This establishes the scope of the review.

Task 2: *Establish review objectives*—This defines the specific tasks to be accomplished, for example, verifying that recovery of application "X" can be completed within 3 hours after a DBMS failure.

Task 3: *Identify database evidence to be reviewed*—This determines the type, amount and location of evidence to be collected during the review.

Task 4: *Determine review staffing requirements*—This process selects the individuals who will participate on the review. In larger organizations, the staff might be specified by type of skills required.

Task 5: *Establish review budget*—This determines the amount of resources to be allocated to the review.

Task 6: *Specify support*—If special assistance is needed in conducting the review, such as would be provided by a DBMS software expert, that expertise needs to be specified during the strategy setting process.

Task 7: *Identify database technology contacts*—This involves developing a list of all the people with whom the reviewer might interact during the review process. This should include the name, position, location, and telephone number.

Task 8: *Develop work program*—Design and document the steps and procedures to be undertaken while conducting the review.

Step 3—Identify and Evaluate Database Integrity Controls

Because of the technical complexities involved in evaluating controls over database technology, it is often necessary for a trained database analyst to conduct the review. The nonspecialist may not have sufficient technical knowledge to identify and evaluate the adequacy of database controls. When a technical expert is employed, the reviewer should work closely with him or her in evaluating controls.

It is important for the reviewer to understand the nature of the controls and the rationale behind any negative responses recorded in the internal control questionnaire. The reviewer should begin by identifying those conditions leading to the implementation of control. In this Guideline, those issues have been defined as data integrity control issues (see sec. 3 for a discussion of control issues).

A database integrity review program in the form of a checklist to be completed by the reviewer is provided for each of the database integrity issues described in this Guideline. This checklist can be found in appendix B, and includes a series of questions designed to probe the adequacy of controls over database integrity. A positive response indicates that the area being probed is adequately controlled. A negative answer implies that the reviewer should take additional action to verify whether or not there is a control problem, and if so, to determine the severity of that problem.

Step 4—Reliance Upon Database Technology Controls

Organizations approach control from many different perspectives. In some organizations, environmental controls are extremely strong, and in others the emphasis is placed on application control.

In database technology, the control philosophy is partially dependent upon how the database technology is used. When used as an access method, there appears to be more emphasis on control in the application area, but when data is shared among multiple users the control emphasis is shifted to the environment. In addition, some organizations put their emphasis on preventive controls, while others make heavy use of detective or corrective controls.

There are three aspects which the reviewer should consider in evaluating the adequacy of the system of controls over database technology:

1) Heavy reliance may need to be placed on controls over the central DBMS.
2) The documentation of controls using the matrix approach provides an overview of the total system of controls.
3) The documented control matrix also shows separation of functions.

Section 3 used the database integrity/activity matrix to explain how controls function. The documentation of existing controls using this same matrix approach should be used in the evaluation process.

Reviewers need an organized method for documenting controls so that they can systematically approach the control assessment process. Checklists have proved valuable in identifying controls, but they do not show

interrelationships. Therefore, it is normally better to reformat that information for the assessment process for the total system of controls.

Three relationships need to be shown in the control assessment process. These are:

1) *Compensating controls relationship*—Listing all of the controls addressing a given database integrity issue shows the totality of controls. If the controls over one activity appear weak, the assessor should look at the strength of controls in other activities and their ability to "compensate" for a weakness in control in another activity. For example, the controls may appear weak over access to data in the database. However, further examination may show that the assignment of responsibilities and segregation of duties is such that it compensates for apparent weaknesses in access controls.

2) *User/access relationship*—The ability to access resources is one of the more important controls. If the agency cannot control access through some mechanism, then the evidence produced by the database environment may not be reliable because the data could be changed by inadvertent or intentional unauthorized modification without detection.

3) *Separation of functions relationship*—The relationship between organizational functions must be such that there is a sufficient check and balance between the various duties. No one function should be able to perform an improper action and at the same time be able to conceal the action.

Using the database issue/activities matrix to document the controls shows these three relationships. Consider an example of assessing the adequacy of controls over the inaccurate and incomplete data integrity issue. This hypothetical example is used to explain the evaluation of the three relationships and show how a judgment might be made evaluating the controls.

Control Assessment Example

A problem faced by the database administrator is ensuring the accuracy and completeness of data within the database. The responsibility can be jointly shared by application systems as they are equally concerned about the accuracy and completeness of data used for their applications.

The case requiring accuracy and completeness controls is a database containing all of the information about the personnel in a designated agency. The database is used by the personnel department, payroll department, employee benefit department, and personnel administration department. Consider the three relationships:

1) *Compensating controls relationship*

The application systems using the database have established the policy of maintaining control totals over the key fields. A payroll application system using the personnel database might keep control totals over year-to-date earnings, year-to-date retirement contributions, year-to-date Federal withholding taxes, and other accumulations. If the database administrator failed to keep central control totals, those maintained by the applications should compensate for this lack. The controls used by the application in this case would be:

data element responsibility (18)
adequacy of programmed input validation checks (2)

2) *User/access relationship*

The agency can secure the data in its database by permitting access to only those needing the data. User profiles could be maintained on all users, and enforced through automated security procedures. For example, the payroll system may restrict access in one application to GS15 and lower, while another application can access the pay rates and pay information for members of the Senior Executive Service as well. The types of controls used for access control might be:

Security profile (28)
passwords (29)
database malfunction reporting (24)

3) *Separation of functions relationship*

Functions are divided to avoid both intentional and unintentional manipulation. By limiting the responsibility of any one party, the ability for someone to affect the accuracy and completeness of data without being detected by

another party is minimal. Some of the separation of function controls that could be used in controlling the personnel database include:

rotation of duties (14)
segregation of duties (11)
assignment of responsibilities (10)
risk management team (16)

4) *Control evaluation*

The reviewer looking at the types of controls would probably conclude that control over accuracy and completeness is adequate. The application systems maintain control totals, access of all parties to the database is restricted on a need-to-know basis, and functions are properly segregated to give an effective check and balance to detect problems as soon as they might occur.

Step 5—Design and Conduct Database Integrity Tests

Database integrity tests are designed based upon the assessment of database controls. If controls can be relied upon, then audit tests need only determine whether or not those controls perform as expected. This can be determined by testing. However, if controls cannot be relied upon, then more extensive testing may be necessary.

The database issue checklists have recommended the type of tests that should be performed if controls appear weak. Some of these tests require use of database review tools and techniques. These tools are needed because there are new sources of evidence to be reviewed. Many of these tools should be familiar to database software specialists. Most are the tools used by database administration personnel in the performance of their day-to-day functions.

Some of the more common validation tools and techniques are explained below:

- **Data Dictionary System (DDS)**

In addition to controlling the use of data (see 2.3), the DDS can help an agency review the completeness of documentation and identify data to be used for review purposes.

- **Query Language and Report Writers**

The term "query" usually refers to on-line access to the database. The supporting processing capabilities are often very powerful. Query languages and report writers are very flexible, and can be used in place of audit software.

- **Database Structure Mapping**

A pictorial chart or graph of the logical organization of the database needs to be produced. This helps the reviewer understand the database structure and focuses his or her attention on the *capability* of each program (processing, access, and operation).

- **DBMS Log**

Most DBMS systems produce a log of activity. This log can be used to analyze such conditions as:

accounting information—time of batch start and end
application accounting job record
security violation log record—time/date/type
switched (dialup) connect log record
disconnect log record
database open
database close
record checkpoint type taken
record data communication checkpoint type taken
when unauthorized terminal deals into line
database error log record—error in DB structure

Perhaps most important, the DBMS log contains before and after images of all updates to the database. Although designed primarily for use in database recovery, these images can provide a reviewer with a complete audit trail of modifications to the database.

The analysis will provide an overview of use of the database facility for adequacy of control analysis.

- **DBMS Trace and Dump Routines**

  The trace and dump capability can help to perform integrity tests:

  Traces, inserted into a program, can show all the calls handled by DBMS. Traces can be initiated by programs or by request of the console operator.

  Dump routines can dump pools, buffers, queues, and I/O areas when an abnormal end occurs. These routines can also dump the contents of explicitly requested locations.

- **Data Dictionary System-Generated Test Decks and Test Transactions**

The data dictionary system can be used to generate test decks and test databases. These can be used to determine if the data processed by the DDS is consistent with that in application programs.

- **Security History Logs**

The primary value of security analysis using security history tapes is in an on-line environment. These logs include an identification of all resources for which password protection is performed. They identify 1) transactions, 2) terminals (physical and logical), or 3) programs which are password protected. This focuses the reviewer's attention on the consistency of security between programs, terminals, and transactions (i.e., some terminals *may* password protect a program while another *may not*).

- **Database Exits**

Most DBMSs provide exits for the inclusion of specially coded routines to perform functions not available using standard DBMS features.

- **DBMS Utility Software**

Most DBMSs include a number of utility programs. The extent and capabilities provided by these utility programs vary depending on the DBMS.

Step 6—Develop A Database Integrity Opinion

The reviewer should carefully document the findings of the internal control review and any database integrity tests. These findings should be clearly supported by the work done by the reviewer.

Based on the findings, the reviewer may wish to make one or more recommendations for improving controls over database integrity. These recommendations should be as specific as possible and written in an unambiguous style.

The findings and recommendations should be documented in writing and sent to the individual responsible for the activity or activities being reviewed.

APPENDIX A—DATABASE CONTROLS

DATABASE ACTIVITY **End User Interface to DBMS** **No. 1**

NAME OF CONTROL **Program Modification and Maintenance Control**

DESCRIPTION

Ensures that the proper change is installed in the proper version. The control also ensures that the proper program version is placed into operation at the correct time. This control normally involves establishing program version number control. Several versions of the same program can exist on both the source program library and the object program library. Changes to the program, and versions of the program being placed into production, are all controlled on version number.

EVIDENCE

- Version number standards defining the allocation and use of version numbers
- Source program library version number control listings
- Object program library version number listings
- Program change requests cross-referenced to source program version number
- Object program production cross-referenced to version number by date

HOW TO COLLECT EVIDENCE

- Examine program change requests to determine they are referenced to version number
- Examine control listings produced by object program library and source program library software package control listings
- Examine console typewriter log indicating the production version number of the object program in operation, and then compare that to the version that is scheduled to be in production

358-178 O - 82 - 5

DATABASE ACTIVITY **End User Interface to DBMS** **No. 2**

NAME OF CONTROL **Adequacy of Programmed Input Validation Checks**

DESCRIPTION

Input validation checks take on greater significance in a database environment. This is because many programs use the same data for processing. Thus, the need for increased reliability. Input validation checks include reasonableness checks, limit checks, range checks, comparison to acceptable values in a table, cross-reference checks between fields, and anticipation checks. In a database environment, the checks should be documented in the data dictionary.

EVIDENCE

- Input validation check descriptions included in the data dictionary
- Audit program input validation specification
- Results of input validation testing
- Application systems that automatically generate audit programs from data dictionary specifications

HOW TO COLLECT EVIDENCE

- Examine data dictionary documentation
- Examine input validation programs and supporting validation specifications
- Test input validation programs by preparing a representative sample of test transactions to verify that the programs function according to specifications
- Interview data control clerks to determine the types of problems occurring due to inadequate input validation

---

DATABASE ACTIVITY **Operation of the DBMS** **No. 3**

NAME OF CONTROL **Access Authorization Control**

DESCRIPTION

Access authorization control ensures that only authorized individuals gain access to database resources. Access control in a database environment is normally automated through the implementation of user profiles. These profiles provide an index showing what resources an individual is authorized to access. These user profiles can be as specific as the situation warrants. Advanced DBMSs can restrict individuals to specific functions such as "read only" and can further restrict to the value of the field accessed. For example, a given user might have read and update access for pay rate fields of $300 per week or less, read only access for fields of between $300 and $1,000 per week, and no access for fields of more than $1,000 per week.

EVIDENCE

- User profiles cross-referencing individuals to resources
- Access authorization sheets signed by a security officer or equivalent
- DBMS documentation outlining security implementation procedures
- Security violation listings

HOW TO COLLECT EVIDENCE

- Extract and examine security violations from security logs
- Examine security profiles and documentation authorizing those profiles
- Test the security of the system by attempting to access data elements for which the individual accessing is not authorized

DATABASE ACTIVITY **Operation of the DBMS** **No. 4**

NAME OF CONTROL **Data Error Handling**

DESCRIPTION

Data error handling is the procedures and timeliness of examining and correcting detected errors. This process can be partly manual and partly automated. The automated segment uses default attributes, which make corrections automatically and then produce messages asking people to verify the correctness of the automated correction procedures.

EVIDENCE

- Error correction procedures
- Error correction logs indicating when corrections were made and who authorized the correction
- Listings of errors
- Error suspense files, such as a file of error messages awaiting correction

HOW TO COLLECT EVIDENCE

- Examine error correction logs to validate the timeliness and properness of corrections
- Examine completeness of error detection and correction procedures
- Extract and examine the types of errors, and length of time the error has existed, on error suspense files

---

DATABASE ACTIVITY **Operation of the DBMS** **No. 5**

NAME OF CONTROL **Remote Data Transmission Control**

DESCRIPTION

The terminal, or remote site, needs to establish control over data transmitted to the central site. This control normally involves a count of messages, as well as a control over the value, such as dollars, transmitted. In addition, the control also provides assurance that the message is transmitted accurately.

EVIDENCE

- Documentation of local data transmission control procedures
- Documentation of remote terminal operating and correction procedures
- End of transmission period reconciliation documentation

HOW TO COLLECT EVIDENCE

- Examine remote terminal operating, error detection, and other control procedures
- Prepare and transmit test transactions to verify the proper functioning of the terminal control procedures
- Interview terminal operators regarding the adequacy of the control procedures and the type of control problems encountered

DATABASE ACTIVITY **Operation of the DBMS** **No. 6**

NAME OF CONTROL **Central Data Transmission Control**

DESCRIPTION

Central data transmission control ensures the accuracy and completeness of the communication system for the entire network. The central function has responsibility for polling the terminals and for maintaining control by terminal so that the users can receive control information at the end of a transmission period. The central data transmission control normally is implemented using vendor-purchased software.

EVIDENCE

- Documentation of the central communication system implemented features
- Central communication control logs
- Terminal sign on, sign off procedures
- Communication log

HOW TO COLLECT EVIDENCE

- Examine and verify the adequacy of the control procedures in a central communication system
- Extract and examine the control information in the communication logs
- Examine and investigate the types of errors occurring in the central communication processing

---

DATABASE ACTIVITY **Operation of the DBMS** **No. 7**

NAME OF CONTROL **Processing Intent**

DESCRIPTION

The intent of processing should be clearly defined. This is normally defined at the transaction level and should explain the purpose of each transaction and the type of processing that occurs on that transaction. This documentation should be located so that all of the processing intent for a single transaction is easy to obtain.

EVIDENCE

- Transaction flow analysis flowcharts and documentation
- System documentation
- System flowcharts

HOW TO COLLECT EVIDENCE

- Examine system flowcharts and documentation
- Develop transactions flow analysis flowcharts
- Develop matrices that follow the flow of the transaction through programs and indicate in the boxes of the matrices the type of processing occurring in each program.

DATABASE ACTIVITY **Operation of the DBMS** **No. 8**

NAME OF CONTROL **Concurrent Data Control**

DESCRIPTION

Concurrent data control ensures that data elements will not be misprocessed due to two or more users processing the same data element concurrently. Most database management systems provide a control that limits change to one program at a time. If a second user wishes to change a data element that is in the process of being changed, that second user is temporarily denied access to the data element.

EVIDENCE

- DBMS concurrent update control procedures
- Application program control procedures that validate the propriety of the DBMS controls

HOW TO COLLECT EVIDENCE

- Examine and assess the adequacy of the DBMS concurrent update control procedures
- Examine and review the application control procedures
- Conduct a test that attempts to update a data element while that data element is in the process of being updated by another user

---

DATABASE ACTIVITY **Operation of the DBMS** **No. 9**

NAME OF CONTROL **Deadlock Detection and Resolution**

DESCRIPTION

Deadlock occurs when two users engage in a processing situation in which each is holding a data element wanted by the other and will not release that data element until it receives the data element the other user is holding. For example, user A has data element one and wants data element two; while user B has data element two and is holding that until user A frees data element one. Most commercially-produced DBMSs have routines to detect and resolve deadlocks.

EVIDENCE

- Documentation of DBMS deadlock detection and resolution procedures
- Listing of detected unresolved deadlock conditions

HOW TO COLLECT EVIDENCE

- Examine and verify the adequacy of DBMS deadlock detection and resolution procedures
- Create a deadlock condition as a test, to determine if the detection and resolution features function properly

DATABASE ACTIVITY **Data Administration** **No. 10**

NAME OF CONTROL **Assignment of Responsibilities**

DESCRIPTION

A database environment involves maintaining data independently of the application systems that use that data. This implies that many tasks in the development and operation of application systems would now be performed by new individuals. These individuals must be assigned specific responsibility and be made accountable for their actions. Responsibilities that were formerly performed by the systems analyst and programmer are now divided between them and the database administration function. Also, some user responsibilities are transferred to the database administration function.

EVIDENCE

- Database administration charter
- Systems analyst/programmer-delegated responsibility
- User-delegated responsibility

HOW TO COLLECT EVIDENCE

- Evaluate and assess the charter and responsibilities for the database administration function, the systems analyst/programmer, and the user
- Evaluate the functions actually performed by the involved individuals versus their assigned responsibilities

---

DATABASE ACTIVITY **Data Administration** **No. 11**

NAME OF CONTROL **Segregation of Duties**

DESCRIPTION

The operation of a database involves computer operations, the database administrator, the systems analyst/programmer, the user, and normally systems programmers specializing in the technical operation of the DBMS. In addition, some organizations have a security officer. In any reorientation of duties, too much responsibility may be given to the database administrator. Especially in a highly centralized environment, responsibilities should be divided so that no one individual can control the results of processing.

EVIDENCE

- Data processing organizational chart
- Job descriptions in the database administration function

HOW TO COLLECT EVIDENCE

- Evaluate and assess the adequacy of the segregation of duties based upon the organizational chart and job descriptions
- Review job performances to verify whether or not they comply to the authorized segregation of duties

DATABASE ACTIVITY **Data Administration** **No. 12**

NAME OF CONTROL **Operation Documentation**

DESCRIPTION

The operation of the database involves several new functions. These include organization of the database, reorganization of the database, and generation and maintenance of the DBMS. These are all technical procedures necessitating documentation of the methods of performing the procedures. In many instances, the procedures are performed using software packages which themselves need to be documented. The documentation is needed to assure continuity of processing in case of problems or personnel turnover.

EVIDENCE

- Organization and reorganization documentation
- DBMS documentation
- Computer operation database operating procedures, including restart/recovery

HOW TO COLLECT EVIDENCE

- Evaluate and assess the adequacy of operation documentation
- Conduct a test in which operators unfamiliar with the operation are asked to operate the database using only the operation documentation
- Compare the actual operation documentation versus the vendor-recommended operation documentation

---

DATABASE ACTIVITY **Data Administration** **No. 13**

NAME OF CONTROL **Output Control**

DESCRIPTION

Multiple users request common information from databases. The information might be requested by application programs, utility programs, or query transactions. However, because database information can be updated by groups independent of those using the data, there can be misinterpretations as to the reliability and timeliness of data. Therefore, output controls must not only restrict access to the authorized individuals, but must communicate to the users the reliability and timeliness of the data they are obtaining.

EVIDENCE

- Output access profiles
- Data dictionary output reliability and timeliness descriptions
- Descriptive information included in reports
- Query language procedures explaining output reliability and timeliness

HOW TO COLLECT EVIDENCE

- Evaluate and review output procedures to assess that they convey the appropriate reliability and timeliness information
- Evaluate and assess the adequacy of the output access procedures
- Initiate one or more queries using a query language to evaluate the completeness of explanatory information regarding the output information used
- Verify the integrity of the output received versus independent control totals maintained by database users

DATABASE ACTIVITY **Data Administration** **No. 14**

NAME OF CONTROL **Rotation of Duties**

DESCRIPTION

Individuals working with databases may be in a position to abuse the data. In some environments, this temptation can be reduced by rotating individuals to different functions. For users, this may mean dividing the database into segments and then rotating clerical people from one segment to another. In the database administration function, it may mean shifting technical people from one technical aspect of the operation of the database to another. In computer operations, it may mean shifting operators among various applications so they do not continuously run the same application.

EVIDENCE

- Rotation of duty plans and procedures
- Notices of transfer of personnel among duties

HOW TO COLLECT EVIDENCE

- Evaluate and assess the rotation of duty plans and procedures
- Verify the movement of people to determine compliance to the rotation of duty plans and procedures

---

DATABASE ACTIVITY **Data Administration** **No. 15**

NAME OF CONTROL **Processing Performance Standards**

DESCRIPTION

In order for a database organization to achieve promised performance, specific processing performance standards must be established and plans developed to achieve the standards. This process requires the continual monitoring of actual performance versus standards.

EVIDENCE

- Processing performance standards
- Procedures for monitoring processing performance standards
- Results of monitoring procedures

HOW TO COLLECT EVIDENCE

- Evaluate and assess the reasonableness of the processing performance standards
- Compare the organization's processing performance standards to what vendors state are realistic performance standards
- Compare actual performance versus standards, and investigate the causes of differences

DATABASE ACTIVITY **Data Administration** **No. 16**

NAME OF CONTROL **Risk Management Team**

DESCRIPTION

A risk management team identifies and assesses the severity of risk in a database environment. The risk assessment team is normally comprised of users, database analysts, control-oriented personnel such as auditors, and security personnel. This team may be formed for a one-time risk analysis process, or it may convene whenever conditions change, such as the study of a potential new application.

EVIDENCE

- Risk analysis team makeup
- Risk analysis team policies and procedures
- Risk analysis team reports

HOW TO COLLECT EVIDENCE

- Evaluate and assess the adequacy of the makeup of the risk analysis team and their plans and procedures
- Evaluate and assess the completeness and reasonableness of the risk analysis reports
- Conduct an independent audit to identify new risks, or to reassess the severity of identified risks
- Conduct an audit to verify losses associated with the identified risks

---

DATABASE ACTIVITY **Data Definition** **No. 17**

NAME OF CONTROL **Centralized Coordination of External Schema**

DESCRIPTION

The external schema is important in establishing levels of performance, and flexibility to extend applications. The external schema should take into account both present and future information needs of the organization. The organization of that information should then be designed to optimize the use of information in the database. This design should be centrally coordinated.

EVIDENCE

- Policies and procedures for external schema design
- Documentation of the external schema

HOW TO COLLECT EVIDENCE

- Evaluate and assess the adequacy of control over the design and implementation of the external schema
- Interview users to determine the adequacy of the information in, and organization of, the external schema

DATABASE ACTIVITY **Data Definition** **No. 18**

NAME OF CONTROL **Data Element Responsibility**

DESCRIPTION

Each data element should have one individual or job position accountable for it. The individual has the responsibility for authorizing access to the data element, and assuring the integrity of the data element.

EVIDENCE

- Data dictionary
- Job accounting system

HOW TO COLLECT EVIDENCE

- Review, or extract from, the data dictionary the responsibility segment of each data element to ascertain that an individual is responsible for that data element
- Prepare confirmations from the data dictionary to send to the responsible individual to verify that he or she accepts that responsibility
- Extract from job accounting systems users of selected data elements. This listing should be sent to the responsible individual to confirm that all users of that data element have authority to access the element. Differences should be investigated

---

DATABASE ACTIVITY **Data Definition** **No. 19**

NAME OF CONTROL **Conceptual Data Independence**

DESCRIPTION

Conceptual data independence implies that data needs are developed independently of the application systems that use the data. This does not mean that application systems do not feed input to data creation but, rather, the authority to create and modify data is independent of the applications. In agencies where this is practiced, this normally involves a strong data administration function. A data administrator is frequently a member of senior management.

EVIDENCE

- Data administration function responsibility
- Data definition procedures
- Data dictionary
- Application system data definition division

HOW TO COLLECT EVIDENCE

- Examine data administration function to review the data definition policies to determine if they are independent of the application systems personnel
- Examine the information in the data dictionary to determine compliance to the data administration data definition policies
- Examine the data, and data definitions used in application systems, to verify compliance with the data independence policies and procedures

DATABASE ACTIVITY **Data Definition** **No. 20**

NAME OF CONTROL **Data Dictionary System**

DESCRIPTION

A data dictionary system is a documentation tool for defining data and its use. Many DDSs are software packages available from vendors. The objective of the DDS is to standardize the definition and use of data. The DDS also can be used to define organization, reorganization, access to data, and other operating information needed to implement a database environment.

EVIDENCE

- Data dictionary policies and procedures
- Data dictionary documentation
- Data dictionary file

HOW TO COLLECT EVIDENCE

- Evaluate and assess the adequacy of the data dictionary policies and procedures
- Extract information from the data dictionary file and other documentation to verify that the implemented data dictionary is in compliance with the data dictionary policies and procedures
- Test the DDS by entering and/or using data defined in the data dictionary

---

DATABASE ACTIVITY **Data Definition** **No. 21**

NAME OF CONTROL **Active Data Dictionary System**

DESCRIPTION

An active data dictionary system connects the DDS to the DBMS in a production environment. A DDS can be off-line and used solely as a documentation tool. However, in an active mode application systems cannot access or define data unless those data definitions are processed through the DDS. This is one of the strongest controls in a database environment since it can enforce access rules in addition to enforcing standardized definitions. This concept may not be completely practical with currently available software.

EVIDENCE

- Data policies and procedures
- Active data dictionary system documentation, policies, and procedures
- Job accounting system log

HOW TO COLLECT EVIDENCE

- Assess the data dictionary system to verify compliance to the data policies and procedures
- Extract information from job accounting systems to verify that the active DDS is used in the production environment
- Perform a test which attempts to enter or access data in the database without going through the active DDS

DATABASE ACTIVITY **Security/Access** **No. 22**

NAME OF CONTROL **Physical Barrier**

DESCRIPTION

A physical barrier is a structure that prevents unauthorized individuals from accessing the database and/or accessing terminals that can access the database. Examples of physical access are locked rooms, guards at entrances to database resources, or key locks activated by magnetically-encoded cards.

EVIDENCE

- The physical site
- Physical barrier security procedures

HOW TO COLLECT EVIDENCE

- Examine the adequacy of the physical barrier
- Test the functioning of the physical barrier by attempting to enter a secure area undetected

---

DATABASE ACTIVITY **Security/Access** **No. 23**

NAME OF CONTROL **Surveillance**

DESCRIPTION

Surveillance is the observation of the functioning of the area in which the database resides and/or terminals having access to the database. Surveillance is normally performed by supervisors or trained security personnel. Surveillance can be continuous or periodic.

EVIDENCE

- Job descriptions indicating surveillance responsibility
- Location of responsible individuals in a suitable location for surveillance
- Surveillance procedures

HOW TO COLLECT EVIDENCE

- Observe the individuals performing the surveillance function
- Examine job descriptions to verify that surveillance is a part of the job, and evaluate the adequacy of surveillance procedures
- Test the adequacy of surveillance by attempting to gain undetected access to the database resources

DATABASE ACTIVITY Security/Access **No. 24**

NAME OF CONTROL **Database Malfunction Reporting**

DESCRIPTION

Malfunction reporting is the formalization of the database error reporting process. Malfunction reporting normally involves a form that identifies problems or malfunctions, identifies the cause of the malfunction, and makes recommendations as to the recommended course of action. In some organizations, this function is performed by a group of specialists who do the error analysis, but not the correction.

EVIDENCE

- Database malfunction reporting reports
- Database malfunction reporting procedures
- Results of database malfunction reporting

HOW TO COLLECT EVIDENCE

- Examine malfunction reporting reports and procedures to determine the adequacy of the procedures
- Examine the results of malfunction reporting to determine that the procedures have been followed
- Review the malfunction reports to determine that problems are being corrected on a timely basis
- Examine machine logs to identify problem conditions to verify that there is a malfunction report for the conditions tested

---

DATABASE ACTIVITY Security/Access **No. 25**

NAME OF CONTROL **Natural Disaster and Environmental Protection**

DESCRIPTION

Studies by computer vendors have shown that many computer center problems are associated with natural disaster and environmental protection. These involve such conditions as water overflow problems on floors above the computer room, floods of computer centers in flood prone areas, and small fires. Investigation should be undertaken to identify the natural disaster and environmental risks, and then to develop appropriate procedures and measures to reduce the probable loss should those disasters occur.

EVIDENCE

- Identification of emergency situation
- Natural disaster and environmental risk analysis procedures
- Natural disaster and environmental protection procedures

HOW TO COLLECT EVIDENCE

- Examine natural disaster and environmental protection risk analysis, the results of the risk analysis procedures, and the protective procedures
- Examine other measures adopted to reduce the probable loss

DATABASE ACTIVITY **Security/Access** **No. 26**

NAME OF CONTROL **Maintenance Plan**

DESCRIPTION

Maintenance occurs on both the database hardware and the database software. During these maintenance procedures, the data in the database may be accessible to the maintenance personnel. Maintenance procedures should be designed to minimize the risk of maintenance personnel either intentionally or unintentionally accessing or modifying the database.

EVIDENCE

- Maintenance agreement with vendors or other contractors
- Maintenance operating procedures
- Procedures governing contractor on-line interface to an organization's hardware

HOW TO COLLECT EVIDENCE

- Examine and assess the adequacy of the contractual and operating maintenance procedures
- Observe contractor maintenance to verify that it is performed in accordance with contract agreements
- Examine hardware and the associated controls governing contractor on-line capabilities to access an organization's hardware

---

DATABASE ACTIVITY **Security/Access** **No. 27**

NAME OF CONTROL **Security Officer Function**

DESCRIPTION

The security officer is an individual or group having the responsibility for security in a database environment. This may be a full- or part-time function. The function is responsible for the documentation of security over the database, and the monitoring of the security procedures that enforce access specifications. The security officer normally is external to the data processing function. The function is described in Office of Management and Budget Circular A-71, Transmittal Memorandum No. 1, [OMB 78].

EVIDENCE

- Security officer job descriptions
- Security officer procedures
- Results of security officer investigations

HOW TO COLLECT EVIDENCE

- Examine and assess the adequacy of the security officer job description and procedures
- Review the findings and recommendations of the security officer to determine reasonableness, acceptance by concerned groups, and the support provided the function by senior management
- Independently assess the adequacy of security

DATABASE ACTIVITY **Security/Access** **No. 28**

NAME OF CONTROL **Security Profile**

DESCRIPTION

The security profile matches user need with database resources. The profile can be by both user and database resource. A user profile indicates all of the resources accessible to that user. A database resource profile indicates all of the users that can have access to a designated resource. The objective of the security profile is to implement management's security policy through database technology.

EVIDENCE

- Security profile documentation
- Security profile as included in the DBMS, the data dictionary, or security software system
- Security log

HOW TO COLLECT EVIDENCE

The implemented security profile should be compared to the authorized profile to determine compliance between management intent and practice. The security log should be examined to verify first that security procedures are being followed, and second to identify actual violations. The examiner can attempt to obtain unauthorized data.

DATABASE ACTIVITY **Security/Access** **No. 29**

NAME OF CONTROL **Passwords**

DESCRIPTION

Passwords are identifiers used by people to gain access to database resources. Passwords can be any combination of characters, or may be special words known only to the individual in the system, such as the maiden name of an individual's mother. Passwords are normally changed periodically. The individual to whom the password is assigned is the only individual who should know that password. The password file should be well protected.

EVIDENCE

- Password procedures
- Computer password file
- Security log

HOW TO COLLECT EVIDENCE

The password procedures should be tested through observation and test. The use of passwords, and protection given them in practice, should be assessed to determine if it is adequate. In addition, attempts should be made to violate the password procedures.

DATABASE ACTIVITY **Systems Development** **No. 30**

NAME OF CONTROL **Database Administration Function**

DESCRIPTION

The database administration function has the responsibility for the performance and control of the implemented database. The DBA function can be a part- or full-time function. The DBA normally has the responsibility for structuring the schema, determining the features in the DBMS that will be utilized, and working with users to optimize applications interfacing with the database. The database administrator frequently administers the data dictionary, if one exists.

EVIDENCE

- Database administrator job description
- Database administration procedures
- Database administrator entries into the data dictionary
- DBMS documentation and features implemented by the database administrator

HOW TO COLLECT EVIDENCE

- Examine and assess the adequacy of the database administrator job description and procedures
- Interview users regarding their assessment of the adequacy of the performance of the database administration function
- Measure the actual performance of database utilization versus organizational database objectives
- Examine the completeness and accuracy of database administrator DBMS documentation. Segments of this documentation should be included in the data dictionary.

DATABASE ACTIVITY **Systems Development** **No. 31**

NAME OF CONTROL **Application System Testing**

DESCRIPTION

Application system testing is the testing of the application system interface with the database. The testing verifies that the DBMS is providing accurate and complete data to the application system and that the data is being properly returned to the DBMS.

EVIDENCE

- Detailed test plan describing the steps to be performed during testing
- Test data
- Results of testing with corrective action

HOW TO COLLECT EVIDENCE

- Evaluate the adequacy of the test plan
- Evaluate the completeness of the test data, especially in testing program limits and error conditions
- Evaluate the proper functioning of the system based upon the testing results as compared to system specification

DATABASE ACTIVITY **Systems Development** **No. 32**

NAME OF CONTROL **Formal Design Process**

DESCRIPTION

A formal design process outlines all of the steps and procedures needed to be followed during the developmental process. Many organizations call this formal design process structured design or system development life cycle. The objective is to utilize procedures that will minimize effort and maximize the probability of building a successful system. A discussion of this process for a database environment is contained in FIPS PUB 77 [NBS 80a].

EVIDENCE

- Formal design procedures
- Project plans including the formal design steps in the plan
- Completed documents required by the formal design process

HOW TO COLLECT EVIDENCE

- Examine and evaluate the adequacy of the formal design process
- Examine the developmental procedures and products to verify that the process is being followed

---

DATABASE ACTIVITY **Systems Development** **No. 33**

NAME OF CONTROL **Top Management Checkpoints**

DESCRIPTION

Top management checkpoints are formal points are formal points throughout the developmental process at which management will review progress and reevaluate whether or not to continue system implementation. Some organizations only allocate resources from checkpoint to checkpoint. This provides top management with the opportunity to abort or change an unsuccessful project. The number of checkpoints normally varies with the size and importance of the project. Such recommitments of management support are particularly important in a database environment that requires central coordination of authority.

EVIDENCE

- Top management checkpoint procedures
- Documentation indicating scheduled checkpoint reviews
- Project reports providing the information needed for a checkpoint review
- Results of management checkpoint review decisions

HOW TO COLLECT EVIDENCE

- Examine the checkpoint procedures and the adequacy of those procedures
- Review the checkpoint process to determine whether or not checkpoint procedures have been followed
- Examine completed project documentation to verify that all the checkpoint steps were executed prior to the project going into production

DATABASE ACTIVITY **Systems Development** **No. 34**

NAME OF CONTROL **System Implementation Standards**

DESCRIPTION

System implementation standards govern the methods for documenting systems, documenting data, developing program specifications, writing programs, testing programs, converting programs, approving changes to programs, and performing the other related procedures deemed necessary for the successful implementation of a database application system.

EVIDENCE

- System implementation standards
- Procedures governing waivers and deviations from standards
- Procedures governing enforcement of standards
- Project documentation representing the implementation of standards

HOW TO COLLECT EVIDENCE

- Evaluate and assess the adequacies of the standards and the procedures governing the standards
- Review application systems to determine that standards are followed. This may include:

  Review of systems documentation
  Development of extract programs to review source program libraries and data dictionaries to determine adherence to standards
  Analysis of operational data using audit software to validate compliance to standards

---

DATABASE ACTIVITY **Systems Development** **No. 35**

NAME OF CONTROL **Database Standards**

DESCRIPTION

Database standards govern the documentation of data, the implementation of DBMSs, and the utilization of the interfaces to the DBMS. The standards include such items as use of passwords, structure of passwords, definition of data, interface of the data dictionary to the DBMS, reorganization, restart and recovery, organization of the schema, and standards on how to deviate from the standards.

EVIDENCE

- Database standards
- Procedures governing the use and deviation from database standards
- The database as the end product of the implementation of the standards

HOW TO COLLECT EVIDENCE

- Examine and assess the adequacy of the database standards and the procedures governing the use of those standards
- Evaluate the database to ascertain that the standards have been utilized, which could include:

  Extracting information on the data dictionary regarding DBMS standards
  Using a database verifier to examine the integrity of the database
  Testing the database to verify performance standards
  Using query languages to investigate the use of standards in the operation of the database

DATABASE ACTIVITY Systems Development **No. 36**

NAME OF CONTROL Training of Personnel

DESCRIPTION

The training of personnel is needed to ensure individuals controlling or interfacing the DBMS have acquired the appropriate skills. All people involved in database technology need some training in order to properly optimize and control the database.

EVIDENCE

- Training curriculums recommended by database vendors
- Training plans
- Training schedules for courses and individuals
- Assessment of skills of trainees by course instructors

HOW TO COLLECT EVIDENCE

- Evaluate the amount of training provided versus vendor-recommended training
- Analyze frequency and types of problems occurring that are attributable to individual errors and misjudgments
- Compare actual training to training plans
- Compare actual proficiency of individuals to desired levels of proficiency

---

DATABASE ACTIVITY Systems Development **No. 37**

NAME OF CONTROL System Documentation

DESCRIPTION

System documentation includes all of the documentation needed to operate successfully in a database environment, and to assure the continuity of processing. Documentation in a database environment includes data dictionary documentations, schema and subschema documentation, reorganization documentation, database verifier documentation, and documentation governing the operational performance of the DBMS. In on-line databases, documentation should also include security, privacy, and access capabilities and restrictions.

EVIDENCE

- System documentation standards and procedures
- Operating and interface documentation
- Actual application system documentation

HOW TO COLLECT EVIDENCE

- Examine and assess the adequacy of the documentation standards and procedures
- Evaluate compliance of operating documentation to standards. This normally includes master terminal operation documentation, access and security documentation, DBMS operation and reorganization documentation, and interface documentation.
- Assess the adequacy of documentation on the interface between the application system and database

DATABASE ACTIVITY **Systems Development** **No. 38**

NAME OF CONTROL **Review Board**

DESCRIPTION

A review board is a group independent of the database administrator and the application development team. The objective of the review board is to determine that the database standards and procedures are being followed, and that the implemented systems are meeting the needs of the user. In some organizations, these review boards are called quality assurance, in others, system assurance groups.

EVIDENCE

- Review board operating standards
- Results of review board reviews
- Review board job descriptions and authority

HOW TO COLLECT EVIDENCE

- Examine and evaluate the adequacy of the review board functions and authority
- Evaluate operational systems to verify that the results of the review helped produce an application system that complied with the organization's database standards and procedures
- Review operational systems to determine that those database functions and application systems that should have been reviewed were reviewed

---

DATABASE ACTIVITY **Systems Development** **No. 39**

NAME OF CONTROL **Government Reporting Requirements**

DESCRIPTION

Development of procedures to assure that the agency complies with Federal law, such as the Brooks Act, and regulations promulgated by GAO, GSA, OMB, etc. The database must be examined to ascertain that it contains the necessary information to fulfill agency reporting requirements, and that the data is accurate and complete.

EVIDENCE

- Regulatory agency reporting requirements
- Application system documentation specifying compliance procedures for the reporting requirements
- Regulatory agency reports

HOW TO COLLECT EVIDENCE

- Examine reports to verify compliance with regulatory requirements
- Use the query language to verify that the database contains the needed information

DATABASE ACTIVITY **Systems Development** **No. 40**

NAME OF CONTROL **Personal Privacy Requirements**

DESCRIPTION

The Privacy Act of 1974 requires Federal agencies to protect the privacy of individuals. Procedures need to be established to ensure that data collected about an individual for one purpose is not used for another purpose without the consent of that individual. In addition, procedures governing the appropriate retention and destruction of such records must be implemented.

EVIDENCE

- Personal privacy requirements and procedures
- Database procedures regarding protection of individual information
- Privacy information destruction periods and procedures
- Security measures designed to ensure privacy

HOW TO COLLECT EVIDENCE

- Evaluate and assess the security procedures and measures
- Evaluate the destruction procedures for compliance with privacy regulations
- Attempt access to private information without proper authorization to test the adequacy of the privacy procedures
- Attempt to extract private information after the date on which it should be destroyed

DATABASE ACTIVITY **Backup/Recovery/Reorganization** **No. 41**

NAME OF CONTROL **Audit Trail**

DESCRIPTION

An audit trail in a database environment is comprised of both the application audit trail and the DBMS log audit trail. The objective of the audit trail is to substantiate transaction processing, support financial or other critical totals, and to provide a means to reconstruct the database in the event of a system crash or major processing error. One complexity of the database audit trail is that it is, in fact, divided into two segments.

EVIDENCE

- DBMS log, documentation, and procedures
- DBMS procedures to interpret and print log
- Application system audit trail documentation and procedures
- Audit trail media retention procedures

HOW TO COLLECT EVIDENCE

- Examine the DBMS, application, and retention procedures for audit trails
- Test the ability to produce the detailed records supporting critical totals
- Test the audit trail to ascertain that a trail exists between a source record and critical totals
- Conduct audits using audit trail information as evidence. This normally involves the use of audit software to extract information for audit investigation.
- Examine the DBMS procedures and retention periods to determine if they are adequate for the organization's uses of the DBMS log
- Perform a review after each recovery procedure to verify that the information contained on the log was adequate to ensure an accurate and complete database recovery.

DATABASE ACTIVITY Backup/Recovery/Reorganization **No. 42**

NAME OF CONTROL Recovery Procedures

DESCRIPTION

In a database environment, the integrity of the database can be lost independently of application system failures. The database loss can be due to hardware problems, DBMS operating problems, reorganization problems, or as a result of users interacting with the database or its operating mechanism.

Recovery procedures provide both the documentation and the step-by-step tasks that must be performed to recover after a database failure. Recovery procedures are invoked when the integrity of the database has been lost. The recovery procedures normally begin at a point of known integrity, and then, using the before and after transaction images from the DBMS log, reconstruct processing from the point of known integrity to the point of known failure.

Backup data is that data not needed for production purposes, but accumulated for use in the event of a database failure. Backup data includes the DBMS log, copies of the database at fixed points in time, recovery procedures documentation, application system logs, etc.

EVIDENCE

- Operator's recovery manual
- User's recovery manual
- Recovery audit trail
- Database recovery procedures
- Database operating and security procedures
- DBMS data integrity control procedures
- DBMS log
- Backup copies of database
- Application program library
- Recovery operating procedures

HOW TO COLLECT EVIDENCE

- Review recovery documentation to determine if it is sufficient to conduct the recovery process
- Verify, at the completion of each recovery process, the adequacy of the backup data
- Examine and assess the adequacy of the database loss recovery procedures
- Simulate a disaster to test the adequacy of the recovery procedures
- Examine and assess the adequacy of the database data integrity procedures

DATABASE ACTIVITY **Backup/Recovery/Reorganization** **No. 43**

NAME OF CONTROL **Reorganizational Utilities**

DESCRIPTION

The reorganizational utilities are the documentation of the step-by-step tasks needed to be performed to restructure the database. The physical and logical database periodically needs to be restructured to meet the changing needs of the users. In addition, the space allocation formula may have to be changed to free up additional space for changing user requirements. Periodically, all the needed changes are put together and a database is reorganized in accordance with those desired changes. Due to the complexity of the process, reorganizational utility programs are needed to help the database administrator perform the process.

EVIDENCE

- Reorganization procedures
- Reorganizational utility documentation
- Reorganizational audit trail

HOW TO COLLECT EVIDENCE

The proper functioning of the reorganizational utility is normally verified using a database verifier. The verifier can determine that all the pointers are complete and that the database structure changes have been accomplished. In addition, normal DBMS statistics provide assurance that data was not lost during the reorganization processes.

DATABASE ACTIVITY **Backup/Recovery/Reorganization** **No. 44**

NAME OF CONTROL **Database Verifier**

DESCRIPTION

A database verifier is a software package that reviews the integrity of the database to ascertain that all designated paths through the database are complete. These paths are normally marked with pointers, and if a pointer contains a wrong address the data following that broken pointer is lost. Database verifiers are normally used after a database is reorganized or recovered.

EVIDENCE

- Documentation of the functioning of the database verifier
- Output listing of results from operating the database verifier
- Operating log indicating the database verifier has been executed

HOW TO COLLECT EVIDENCE

- Examine the results of executing a database verifier
- Test the operation of the database verifier by "breaking a pointer" and then running the verifier to determine if it identifies the broken pointer
- Examine the documentation of the functioning of the database verifier

DATABASE ACTIVITY **Backup/Recovery/Reorganization** **No. 45**

NAME OF CONTROL **Application System Failure Procedures**

DESCRIPTION

Failures in a database environment can be attributable to both the DBMS and the application system. In the event of failures in the application system, database processing may be only partially complete. The procedures include those steps to reinitiate processing, determine the integrity of the application data queues, and back out or complete partially completed processing.

EVIDENCE

- Application system failure documentation
- Application system failure audit trail

HOW TO COLLECT EVIDENCE

The application system failure procedures should be periodically tested. If an application system failure has not occurred recently, it may be valuable to simulate a failure midway through system processing.

DATABASE ACTIVITY **Backup/Recovery/Reorganization** **No. 46**

NAME OF CONTROL **Backup Databases**

DESCRIPTION

Backup databases are copies of databases at restart points—points where the integrity of the database is assured and from where recovery can commence. The backup database is normally made with a dump utility which copies the image of the database onto a new file.

EVIDENCE

- Documentation of the procedures for creating backup databases
- Documentation to substantiate the structure of the data on the database
- Backup database retention procedures

HOW TO COLLECT EVIDENCE

- Examine the backup database procedures and retention period documentation for adequacy
- Perform a physical examination to verify the existence of the backup database
- Create a disaster testing situation to verify that the operations personnel can recover processing using the backup database

APPENDIX B—CHECKLIST FOR VERIFYING DATABASE INTEGRITY

INTEGRITY ISSUE: #1. Inadequate Assignment of Responsibilities

#	Question	YES	NO	If NO, Reviewer Should
1.	Are the DBA's activities restricted to administration (e.g., not permitted to operate the computer, unsupervised access to the computer room, etc.)?			Define the activities performed by the DBA and note by each one the potential risk to the organization, if any.
2.	Is the access of database administration personnel and other technical personnel subject to the same password control as that of any other user?			Analyze the DBMS log, security log, or job accounting log to determine what data these individuals are accessing.
3.	Are programmers restricted from accessing the DBMS supporting libraries?			Determine which programmers are accessing which libraries and for what purpose. Then base the risks the accesses cause the organization upon this list.
4.	Is there adequate division of responsibilities between the functions of database administration, computer operations, application programming, and systems analysis?			Identify areas of too much concentration of responsibility and list the risk to the organization from that concentration.

INTEGRITY ISSUE: #2. Inaccurate or Incomplete Data in a Database

#	Question	YES	NO	If NO, Reviewer Should
1.	Are the data validation rules documented in a data dictionary?			Determine the extent of data validation rules and whether or not they are reasonable.
2.	Does the database administrator have counts over physical records, segments, or equivalent units in the database?			Determine the procedures for verifying the accuracy and completeness of the database and, if inadequate, make appropriate recommendations.
3.	Does each data element or equivalent have one individual accountable for its accuracy and completeness?			Identify the key data elements for which an individual is not accountable and make recommendations to management to assign accountability.
4.	Are procedures established to ensure consistency among redundant data?			Identify key elements of redundant data for which procedures are inadequate to assure consistency. Compare the redundant items to determine the magnitude of the problem and make recommendations accordingly.
5.	Is the accuracy and completeness of the database immediately verified following each recovery?			Determine how data integrity is verified following recovery and if the procedure is inadequate make recommendations to strengthen the process.

INTEGRITY ISSUE: #3. Losing an Update to a Single Data Item

#	Question	YES	NO	If NO, Reviewer Should
1.	Does your organization's DBMS have a control to "lockout" multiple concurrent updates?			Determine the procedure used and make a judgment regarding its adequacy.
2.	Does your DBMS have an option to break the "deadly embrace"?			Determine the procedure used and make a judgment regarding its adequacy.
3.	Does your organization have a formal procedure to determine the sequencing of events so that data will not be lost or miscalculated due to an improper processing sequence?			Determine the procedure used and make a judgment regarding its adequacy.

INTEGRITY ISSUE: #4. Inadequate Audit Trail

#	Question	YES	NO	If NO, Reviewer Should
1.	Are users involved in specifying the database audit trail?			Recommend that a formal database audit trail methodology be established that involves users.
2.	Is critical information kept in accordance with specified retention requirements?			Make the responsible individuals aware of the required retention periods.
3.	Is a procedure established to properly identify retention periods on all audit trail information?			Work with the database administrator to develop an audit trail retention procedure.
4.	Have control-oriented personnel reviewed any condensation of the DBMS log to ensure control information is not deleted too soon?			Review with the database administrator the need for retaining control information on the DBMS log.
5.	Has sufficient data been retained to satisfy the provision of the Privacy Act?			Make the responsible people aware of the audit trail provision of the Privacy Act [FONG 77].

INTEGRITY ISSUE: #5. Unauthorized Access to Data in a Database

#	Question	YES	NO	If NO, Reviewer Should
1.	Is there one individual responsible for database security?			Review with management the advantages of appointing a database security officer (need only be a part-time position).
2.	Has the classification of each data element been determined?			Work with the database administrator to develop a procedure so that the classification of data is included in the data documentation.
3.	Has a security profile been developed which matches user needs with data?			Review the current method to determine its adequacy, and if inadequate, recommend that a security profile be developed.
4.	Are the full security features of the database being used?			Determine if those features would help improve data security, and, if so, recommend their use.
5.	Are procedures operational that enforce access rules?			Recommend such a procedure be established, as access rules are meaningless without an enforcement vehicle.
6.	Are security violators identified and punished?			Identify the frequency of violations and recommend to management a more stringent violation policy.

INTEGRITY ISSUE: #6. Inadequate Service Level

#	Question	YES	NO	If NO, Reviewer Should
1.	Have system users defined their service requirements?			Identify through a survey if user service requirements are a problem and make recommendations accordingly.
2.	Have procedures been established to monitor these user established service requirements?			If requirements are established, recommend procedures be established to monitor those requirements.
3.	Can the amount of resources available to users be altered if one or more users consumes sufficient resources to degrade service to other users?			If user service is a problem, recommend procedures to encourage more efficient usage by applying surcharges during peak periods.

INTEGRITY ISSUE: #7. Placing Data in the Wrong Calendar Period

#	Question	YES	NO	If NO, Reviewer Should
1.	Can data be readily identified to the accounting period in which it belongs?			Recommend that data be time stamped if accounting cutoff is important for the applications using that data.
2.	Are procedures established to artificially create an accounting checkpoint at the end of major accounting periods for applications that run continuously?			Identify the magnitude of potential accounting cutoff violations and make recommendations accordingly.
3.	Does the database administrator oversee the accounting cutoff procedures for databases involving financial or other time dependent data having multiple users?			Recommend that the database administrator job responsibilities be expanded to include oversight for accounting cutoffs.

INTEGRITY ISSUE: #8. Failure of DBMS to Function as Specified

#	Question	YES	NO	If NO, Reviewer Should
1.	Is each DBMS release thoroughly tested by DBA staff?			Recommend that a test procedure be established and implemented to test the DBMS.
2.	Is the DBMS vendor or other company contractually responsible for maintenance?			Identify how the DBMS maintenance is performed and if it appears inadequate, recommend a maintenance contract be negotiated.
3.	Have procedures been established to identify DBMS failures so that maintenance personnel can be notified?			Recommend that a formal procedure be established to identify DBMS problems and call in appropriate maintenance personnel.
4.	Has an expected failure rate been identified for the DBMS and actual failures measured against the expected rate?			Request the DBA to establish acceptable levels of DBMS failure and monitor against those failure rates.
5.	Are formal reports prepared each time the DBMS fails to function as specified?			Recommend that a DBMS failure notification form be established, completed, and that management be notified of the frequency and types of failure.

INTEGRITY ISSUE: #9. Fraud/Embezzlement

#	Question	YES	NO	If NO, Reviewer Should
1.	Have control-oriented personnel reviewed the adequacy of database technology controls?			Recommend that database technology be periodically audited by an independent control-oriented group.
2.	Have formal procedures been established to document frauds and embezzlements?			Recommend that a formal procedure be established to document the causes and scope of each database technology fraud or embezzlement.
3.	Are database personnel aware of the most common methods of computer fraud and embezzlement?			Present a course or provide material to database personnel on computer fraud and embezzlement causes.

INTEGRITY ISSUE: #10. No Independent Database Audits

#	Question	YES	NO	If NO, Reviewer Should
1.	Has database technology been reviewed by an independent audit department within the last 12 months?			Recommend that an audit be requested to review the adequacy of controls over database technology.
2.	If reviewed by auditors, are the auditors adequately trained in database technology?			Recommend a training plan to the auditors to improve their database technology skills.
3.	If an audit report has been issued, has the database administration group acted upon all of the recommendations?			Recommend that prompt action be taken on all audit recommendations.

INTEGRITY ISSUE: #11. Inadequate Documentation

#	Question	YES	NO	If NO, Reviewer Should
1.	Is a data dictionary system used as a data documentation tool?			If multiple users use database technology, recommend that a data dictionary be obtained.
2.	If a data dictionary system is used, does it interface with the DBMS?			If the interface capability exists, recommend that it be used.
3.	Are the database technology standards and procedures formally documented and distributed to involved parties?			Recommend that a formal database technology standards procedure be established and that the results be disseminated to all involved parties.
4.	Have the operation, reorganization, and recovery procedures been formally documented?			Recommend that the operations, reorganization, recovery procedures be documented.
5.	Has the database structure been documented?			Recommend that the database structure and recommended changes be documented.
6.	Has a procedure been established to document and act upon user requests for problem resolution or new capability been established?			Recommend that a formal controlled procedure be established so that users can document their concerns, potential problems, and requests for new capabilities.

INTEGRITY ISSUE: #12. Continuity of Processing

#	Question	YES	NO	If NO, Reviewer Should
1.	Has the estimated dollar value of loss due to database failure been estimated?			Recommend that the DBA estimate the losses due to the various types of database failures so that the needed backup and recovery procedures can be initiated.
2.	Have the recovery time requirements been specified?			Users should identify how quickly the database must be recovered for their application.
3.	Have alternate processing procedures been established where it is deemed that they are necessary?			Recommend that the database administration function and the users develop alternate processing procedures in the event of DBMS failure.
4.	Have the backup and recovery procedures been developed to meet the above specified user requests?			Recommend that the DBA and operations personnel develop the procedures to achieve user requirements.
5.	Have people responsible for backup and recovery been identified and the appropriate responsibility assigned?			Recommend that the involved parties in recovery be assigned and trained in their responsibilities.
6.	Have recovery procedures been practiced?			Simulate a DBMS disaster to verify that the recovery procedures work.
7.	Have procedures been developed to verify the integrity of data after a recovery process?			Recommend that procedures be developed to prove the integrity of the database immediately following recovery procedures.

INTEGRITY ISSUE: #13. No Cost/Benefit Analysis

#	Question	YES	NO	If NO, Reviewer Should
1.	Has management required that a cost/benefit analysis be performed before acquiring new database technology?			Recommend to management that cost/benefit analysis be performed before they approve the acquisition of new database technology.
2.	Are users required to go through a cost/benefit analysis before requesting changes to the database structure?			Identify the costs involved in modifying the structure and make recommendations accordingly.
3.	If cost/benefit calculations are made, is a post-installation analysis made to determine if the cost/benefit objectives were achieved?			Recommend that one individual be assigned accountable for monitoring cost/benefit calculations.

INTEGRITY ISSUE: #14. Lack of Management Support

#	Question	YES	NO	If NO, Reviewer Should
1.	If the agency has a data administrator, is this position held by a member of senior management?			Recommend that a member of senior management be designated data administrator (note this can be a part-time function).
2.	Is senior management involved in resolving data disputes between diverse users?			Recommend that senior management take an active role in the resolution of disputes.
3.	Is senior management involved in planning for database technology?			Recommend that one or more members of senior management be included on a database technology planning committee.
4.	Does senior management regularly receive reports regarding achievements and failures of database technology?			Recommend that regular reports be sent to senior management that identify database achievements and failures.

REFERENCES AND SUGGESTED READING

[ACCO 78] *Accountant*, "Evaluating a Data Base System," (Management information), (ENG.), Volume 178 (May 18, 1978) p. 668.

[ACM 71] Association for Computing Machinery, *CODASYL Data Base Task Group Report*—April 1971, New York.
The original CODASYL DBMS proposal.

[ADAM 76] Adams, Donald L. "System to Audit Aspects of the Data Dictionary," *EDPACS*, (May 1976) pp. 1-4.
An analysis of what a DDS is, and how it functions.

[AFIP 74] AFIPS Press, *AFIPS Systems Review Manual on Security*, Montvale, NJ (1974).
A very comprehensive checklist of security questions.

[AFIP 79] AFIPS Press, *Security: Checklist for Computer Center Self Audits*, Montvale, NJ (1979).

[AICP 77a] American Institute of Certified Public Accountants, *The Auditor's Study and Evaluation of Internal Control in EDP Systems*, New York (1977).
A framework for analyzing the control in an EDP environment is proposed.

[AICP 77b] American Institute of Certified Public Accountants, *Computer Services Guidelines—Management, Control, and Audit of Advanced EDP Systems*, New York (1977).
Audit and control standards are explained and defined.

[AICP 78a] American Institute of Certified Public Accountants *Tentative Report of the Special Advisory Committee on Internal Accounting Control*, (September 15, 1978).

[AICP 78b] American Institute of Certified Public Accountants, *Codification of Statements on Auditing Standards—Numbers 1 to 21*, New York (1978).
Auditing standards and interpretations are presented in a consolidated text.

[APPL 78] Applegate, J. Michael "Data Base Management—Getting Back to Basics," (Management advisory services) *CPA Journal*, Volume 48 (December 1978) p. 100.

[AUER 77] AUERBACH, *The Auditor and Data Base Management* (2-06-11), *Data Processing Management*, (1977).
Review of concerns and difficulties in auditing DBMSs.

[BCS 77] British Computer Society—Auditing by Computer Specialist Group, *Audit and Control of Database Systems*, London, England (July 1977).
Papers from three groups (external auditors, governmental administrators, and academicians) cover DBMS audit problems. A comprehensive listing of control and audit information is given.

[BECK 78] Becker, Hal B. "Let's Put Information Networks Into Perspective," *Datamation*, Volume 24 (March 1978) pp. 81-86.

[BENT 78] Bentley, Trevor "Everyone Needs a Data Base," *Management Accounting* (Eng.), Volume 56 (July/August 1978) p. 303.

[BERG 76] Berg, John, ed., *Data Base Directions—The Next Steps*, National Bureau of Standards Special Publication 451, Washington, DC.
Proceedings from NBS and ACM workshop in October, 1975. One session was on "Auditing and the Data Base," and a very concise statement of audit difficulties was developed.

[BJOR 75] Bjork, L. A., Jr. "Generalized Audit Trail Requirements and Concepts for Data Base Applications," *IBM Systems Journal*, (Number 3, 1975) pp. 229-245.
The use of audit trails for recovery and review is discussed.

[BONC 78] Bonczek, Robert H. "Aiding Decision Makers With a Generalized Database Management System: An Application to Inventory Management," *Decision Sciences*, Volume 9 (April 1978) pp. 228-245.

[BRAN 75] Branch, Don R. C. "Support Your Local Data Administrator," *Journal of Systems Management*,

(November 1975) pp. 6-12.
A control system for a large database management system is reviewed.

[BREB 75] Brebach, Gresham T. "Data Base Administration," *Price Waterhouse Review*, (No. 2, 1975) pp. 18-27.
The duties and responsibilities of a typical DBA are defined.

[BURN 76] Burns, Kevin J. "Keys to DBMS Security," *Computer Decisions*, (January 1976) pp. 56-62 (5).
Security considerations in a database environment are outlined.

[CHAM 77] Champine, G. A. "Six Approaches to Distributed Data Bases," *Datamation*, (May 1977) pp. 69-72.
Six corporate distributed database systems are contrasted.

[CICA 70] The Canadian Institute of Chartered Accountants, *Computer Control Guidelines*, Toronto, Ontario, Canada (1970).
Highly structured and now classic approach to computer control.

[CICA 75] The Canadian Institute of Chartered Accountants, *Computer Audit Guidelines*, Toronto, Ontario, Canada (1975).
A highly structured approach which has been widely used.

[COLE 78] Cole, Gerald D. *Design Alternatives for Computer Network Security*, National Bureau of Standards Special Publication 500-21, Volume 1. Washington, DC (January 1978).
The issues and problems involved in network security design are discussed.

[COMP 76] *Computing Surveys* (ACM), "Data-Base Management Systems," Volume 8 (March 1976).

[COXW 78] Cox, W. "DBMS: Dangerous But Manageable Systems," *Interpreter*, Volume 37 (May 1978) pp. 19-23.

[CURT 74] Curtice, Robert M. "Some Tools for Data Base Development," *Datamation*, (July 1974) pp. 102-106 (3).
Ways to expand the use of data dictionaries are suggested.

[CURT 75] Curtice, Robert M. "Data Independence in Data Base Systems," *Datamation*, (April 1975) pp. 65-71 (3).
The data independence concept as implemented in some current DBMSs.

[CURT 77] Curtice, Robert M. "Integrity in Data Base Systems," *Datamation*, (May 1977) pp. 64-68.
Various recovery and fallback techniques are reviewed.

[DATE 81] Date, C. J. *An Introduction to Database Systems. 3d Edition*, Reading, MA (Addison-Wesley, 1981).

[DAVI 68] Davis, Gordon B. *Auditing & EDP*, New York, The American Institute of Certified Public Accountants (1968).

[DEBL 77] DeBlasis, Jean-Paul, and Johnson, Thomas H. "Data Base Administration—Classical Pattern, Some Experience and Trends," *National Computer Conference Proceedings*, AFIPS 1977, pp. 1-7.

[DENN 79] Denning, Dorothy E., and Denning, Peter J. "Data Security," *Computing Surveys*, Volume 11, Number 3 (1979).

[DERE 78] Derensis, Paul R. "Civil Liabilities of Data Base Operators," *Practical Lawyer*, Volume 24 (July 15, 1978) pp. 25-38.

[EDPA 76] *EDP Analyzer*, "Integrity and Security of Personal Data," (April 1976) pp. 1-14.
An investigation of the implications of the Privacy Act on database management.

[EDPA 78] *EDP Analyzer*, "Installing a Data Dictionary," (January 1978) pp. 1-13.
A discussion of practical problems in using data dictionary systems.

[EDPA 80] EDP Auditors Foundation for Education and Research, *Control Objectives*, Hanover Park, IL (1980).
A framework for audit and analysis of all aspects of a data processing operation is presented.

[EMOR 76] Emory, John et al. *A Comprehensive Data Base Access Methodologies Design Guide*, Washington, DC, Defense Communication Agency (September 1976).
A text containing an extensive review of database design practices.

[EVER 77] Everest, Gordon C., and Weber, Ron, with revision by Plagman, Bernard K. "Data Base Support Systems and the Auditing Function," Document No. 22-05-10, *Data Base Management*, Auerbach Publishers, Inc., Pennsauken, NJ (1977) pp. 1-15.
The role of the auditor and the role of the DBA are discussed.

[FERN 76] Fernandez, Eduardo B., and Summers, Rita C. "Integrity Aspects of a Shared Data Base," *National Computer Conference Proceedings*, AFIPS (1976) pp. 819-827.
A model for implementing integrity rules is suggested.

[FINE 77] Fine, Leonard H. "Data Base: The Role of the Auditor," *South African Chartered Accountant*, Volume 13 (December 1977) pp. 409-412, 430.

[FINN 78] Finneran, Thomas R. "Data Base Systems Design Guidelines," *Journal of Systems Management*, Volume 29 (March 1978) pp. 26-30.

[FONG 77] Fong, Elizabeth, *A Database Management Approach to Privacy Act Compliance*, National Bureau of Standards Special Publication 500-10, Washington, DC (1977).

[FREE 77] Freeby, C. R. *A Survey of Data Dictionary Software Packages*, H. F. Sherwood & Associates (1977).
A European survey of users of data dictionary systems.

[GAO 79] Government Accounting Office, *Data Base Management Systems—Without Careful Planning There Can Be Problems*, (June 29, 1979).

[GLAD 75] Gladney, H. M., et al. "An Access Control Mechanism for Computing Resources," *IBM Systems Journal*, (Number 3, 1975) pp. 212-217.

[GRIM 77] Grimes, J. R., and Gentile, E. A. "Maintaining Internal Integrity of On-Line Data Bases," *EDPACS*, (February 1977) pp. 1-14.
An explanation of database audit programs used by Bell Telephone.

[GUID 73] GUIDE International Corporation, *The Data Base Administrator*, Chicago, IL (1973).
Identifies the DBA's responsibilities, organizational impact, and operating tools.

[GUID 74] GUIDE International Corporation, *Requirements for the Data Dictionary/Directory Within the GUIDE/SHARE Data Base Management System Concept*, Chicago, IL (1974).
The possible uses of the DDS are analyzed.

[GUID 77] GUIDE International Corporation, *Distributed Computing in the Early 1980's—The Environment and the Requirements*, Chicago, IL (1977).
Projects data processing needs in the 1980's and associated hardware and software.

[HAMM 76] Hammer, Michael "Error Detection in Data Base Systems," *National Computer Conference Proceedings*, AFIPS (1976) pp. 795-801.
An approach to detection and prevention of errors.

[HEIN 78] Heinrich, Frank *The Network Security Center: A System Level Approach to Computer Network Security*, National Bureau of Standards Special Publication 500-21, Washington, DC (1978).

[HONE 77] Honeywell Information Systems, *Computer Security and Privacy Symposium Proceedings, April 19-20, 1977*, Waltham, MA.
Twenty-three articles/speeches on various aspects of computer security and privacy implications.

[IBM 72] IBM Studies on Data Security initiated May 1972.
Data Security and Data Processing Volume 1, Introduction and Overview (G320-1370)
Data Security and Data Processing Volume 2, Study Summary (G320-1371)
Data Security and Data Processing Volume 3, Part 1, State of Illinois: Executive Overview (G320-1372)
Data Security and Data Processing Volume 3, Part 2, Study Results: State of Illinois (G320-1373)
Data Security and Data Processing Volume 4, Study Results: Massachusetts Institute of Technology (G320-1374)
Data Security and Data Processing Volume 5, Study Results: TRW Systems, Inc. (G320-1375)
Data Security and Data Processing Volume 6, Evaluations and Study Experiences: Resource Security Systems (G320-1376) White Plains, NY, IBM Corp (June 1974)

A very technical and detailed analysis of security needs.

[IIA 74] The Institute of Internal Auditors, *Modern Concepts of Internal Auditing—Auditing Fast Response Systems*, Altamonte Springs, FL (1974).
Identifies problems unique to fast response systems and suggests audit techniques.

[INFO 78] *Infosystems*, "Distributed System Aids Fiscal Control, (Users report) Volume 25 (March 1978) pp. 101-102.

[JARD 77] Jardine, Ronald A., ed. *The ANSI/SPARC DBMS Model*, New York, North Holland Publishing Co. (1977).
Proceedings of the Second SHARE Working Conference on DBMS in Montreal in April 1976. The ANSI/SPARC DBMS Model is discussed by a wide variety of participants.

[JENK 76] Jenkins, A. Milton, and Weber, Ron "Using DBMS Software As an Audit Tool: The Issue of Independence," *The Journal of Accountancy*, (April 1976) pp. 67-69.
Various ways of using DBMSs to analyze data are reviewed.

[LEFK 77] Lefkovits, Henry C. *Data Dictionary Systems*, Wellesley, MA, Q.E.D. Information Sciences, Inc. (1977).
Features and uses of data dictionary systems are discussed, and profiles provided for specific DDSs (LEXICON, CINCOM DDS DB/DC DDS, DATA MANAGER, DATA CATALOGUE, UCC TEN).

[LEON 77] Leong-Hong, Belkis, and Marron, Beatrice *Technical Profile of Seven Data Element Dictionary/Directory Systems*, National Bureau of Standards Special Publication 500-3, Washington, DC (1977).
Characteristics, features, and uses of DDSs are discussed.

[LYON 76] Lyon, John K. *The Database Administrator*, New York, John Wiley & Sons, (1976).

[MART 77] Martin, James *Computer Data Base Organization—Second Edition*, Englewood-Cliffs, NJ, Prentice-Hall (1977).

[MCFA 78] McFadden, Fred R. "Costs and Benefits of a Data Base System," *Harvard Business Review*, Volume 56 (January-February 1978) pp. 131-139.

[MEAD 76] Meadow, Charles T. *Applied Data Management*, New York, John Wiley & Sons, (1976).
Text discusses practical design principle for use in computer files.

[MINA 76] Minami, Dr. Warren N. "Data Administration: Key to Better Management." *Journal of Systems Management*, (May 1976) pp. 40-44.
The position and function of the data administrator are outlined.

[NBS 74a] National Bureau of Standards, *Guidelines for Automatic Data Processing Physical Security and Risk Management*, Federal Information Processing Standards Publication 31 (1974).

[NBS 74b] National Bureau of Standards, *Computer Security Guidelines for Implementing the Privacy Act of 1974*, Federal Information Processing Standards Publication 41 (1974).

[NBS 76a] National Bureau of Standards, *Guidelines for Documentation of Computer Programs and Automated Data Systems*, Federal Information Processing Standards Publication 38 (1976).

[NBS 76b] National Bureau of Standards, *Glossary of Terminology for Computer Systems Security*, Federal Information Processing Standards Publication 39 (1976).

[NBS 79a] National Bureau of Standards, *Guidelines for Documentation of Computer Programs and Automated Data Systems for the Initiation Phase*, Federal Information Processing Standards Publication 64 (1979).

[NBS 79b] National Bureau of Standards, *Guideline for Automatic Data Processing Risk Analysis*, Federal Information Processing Standards Publication 65 (1979).

[NBS 80a] National Bureau of Standards, *Guideline for Planning and Management of Database Applications*, Federal Information Processing Standards Publication 77 (1980).

[NBS 80b] National Bureau of Standards, *Guideline for Planning and Using a Data Dictionary System*, Federal Information Processing Standards Publication 76 (1980).

[NBS 81] National Bureau of Standards, *Guidelines for ADP Contingency Planning*, Federal Information Processing Standards Publication 87 (1981).

[NUSB 78] Nusbaum, Edward E., Bailey, Andrew D., and Whinston, Andrew B. "Data Base Management, Accounting and Accountants," *Management Accounting* (NAA), Volume 59 (May 1978) pp. 35-38.
A general explanation of DBMSs as they affect accounting.

[OMB 78] Office of Management and Budget, Circular No. A-71, Transmittal Memorandum No. 1 (July 27, 1978).

[ORRK 78] Orr, Kenneth T. "Procedures for Structured Data Base Design," *Infosystems*, Volume 25 (July 1978) pp. 78, 80, 82.
Software update.

[PAPE 80] Paperwork Reduction Act of 1980, Public Law 96-511 (1980).

[PATR 78] Patrick, Robert L., *Performance Assurance and Data Integrity Practices*, National Bureau of Standards Special Publication 500-24, Washington, DC (1978).
This report identifies 67 practices currently in use to control a sophisticated computer environment.

[RENE 77] Reneau, J. Hal "Auditing in a Data Base Environment," *The Journal of Accountancy*, (December 1977) pp. 59-65.
Access controls in a database environment are suggested.

[ROBE 78] Robey, Daniel, and Zeller, Richard L. "Factors Affecting the Success and Failure of an Information System for Product Quality," *Interfaces*, Volume 8 (February 1978) pp. 70-75.

[ROBI 78] Robinson, Stephen L. "DBMS' Label Stuck on Too Many Packages?," *Computerworld*, (April 17, 1978) p. 34.
The capabilities of software packages which are designated "DBMS" are explained.

[ROSS 76] Ross, Ronald G. "Placing the DBA," *Journal of Systems Management*, (May 1976) pp. 25-33.
An analysis of a DBA's need to perform both high-level and detailed design work.

[ROSS 77] Ross, Ronald G. "Monograph Series No. 5, An Assessment of Current Data Base Trends," *Data Base Management*, Q.E.D. Information Sciences, Inc., Wellesley, MA, (1977).
Database trends and vendor offerings are discussed in connection with remote computing, mini databases, relational modeling, and CODASYL specifications.

[RUTH 77] Ruthberg, Zella G., and McKenzie, Robert G., eds. *Audit and Evaluation of Computer Security*, National Bureau of Standards Special Publication 500-19, Washington, DC (1977).

[RUTH 80] Ruthberg, Zella G., ed. *Audit and Evaluation of Computer Security II*, National Bureau of Standards Special Publication 500-57, Washington, DC (1980).

[RZEP 76] Rzepka, William E. *Considerations in the Design of a Secure Data Base Management System*, Griffiss Air Force Base, NY, Rome Air Development Center (March 1976).
Study notes that there are various tradeoffs when designing security into a DBMS.

[SCHU 77] Schussel, George "The Role of the Data Dictionary," *Datamation*, (June 1977) pp. 129+ (4).
The advantages and disadvantages of various data dictionary features are analyzed.

[SCOT 78] Scott, George M. "Auditing the Data Base, Down the Tortuous Transaction Path," *CA Magazine* (Canada), Volume 111 (October 1978) pp. 52-59.

[SENK 77] Senko, M. E. "Data Structures and Data Accessing in Data Base Systems Past, Present, Future," *IBM Systems Journal*, (Number 3, 1977) pp. 208-255.
This article contains a discussion of general DBMS trends and standardization attempts from an historical perspective. The bibliography reflects a comprehensive review of literature on database management systems.

[SEVE 77] Severino, Elizabeth F. "Databases and Distributed Processing," *Computer Decisions*, (March 1977) pp. 40-42 (2).
Centralized and distributed database processing are compared.

[STAT 74] Statland, Norman *Data Security Considerations Within a Data Base Management System*, unpublished paper from Price Waterhouse & Co. (September 1974).
Brief review of security problems in a DBMS.

[STAT 78] Statland, Norman, and Winski, Ronald T. "Distributed Information Systems, Their Effect on Your Company," *Price Waterhouse Review*, (Number 1, 1978) pp. 54-63.
The effect of smaller, distributed computers on one typical firm is discussed.

[TGSD 77] Task Group for the Study of Data Bases, *Data Base and the Accountant*, (translated from Dutch to English) circa 1977.
The implications of various audit and control techniques are studied.

[TOME 78] Tomeski, Edward A., and Sadek, Konrad "Molding the Organizational Shape: Set Theory in Systems Design," *Data Management*, Volume 16 (September 1978) pp. 42-47.

[TSIC 76] Tsichritzis, D., and Lochovsky, F. *Data Base Management Systems*, New York, Academic Press (1976).

[TSIC 78] Tsichritzis, D., and King, A., ed. *The ANSI/X3/SPARC DBMS Framework Report of the Study Group on Database Management Systems*, Montvale, NJ, AFIPS Press (1978).
This article presents a framework identifying components of a DBMS which can be standardized.

[VICK 77] Vickers, W. Harry "What to Look for in Distributed (Source) Data Processing," *National Computer Conference Proceedings*, AFIPS (1977) pp. 973-975.
Database and distributed system concepts are reviewed.

[WALS 78] Walsh, Myles E. "Update on Data Dictionaries," *Journal of Systems Management*, Volume 29 (August 1978) pp. 28-37.

[WEBE 76] Weber, Ron "Implications of Database Management Systems for Auditing Research," unpublished paper, University of Minnesota Management Information Systems Research Center, circa 1976.
A review of the implications of the AICPA Audit Standards on database environments.

[WILL 75] Williams, John W. O. "Data Banks," *Data Management*, (July 1975) pp. 24-28.
The Privacy Act of 1974 and the public's concern for privacy are discussed.

[WINK 76] Winkler, Maj. Anthony J., et al. *The Data Administrator's Handbook*, USAF Academy, CO, U.S. Department of Commerce (1976).
Identifies tools and methods available to the DBA.

[WIOR 78] Wiorkowski, Gabrielle K., and Wiorkowski, John J. "Does A Data Base Management System Pay Off?," *Datamation*, (April 1978) pp. 109-114 (4).
Summarizes a user survey of the impact of generalized DBMSs on ADP operations.

[YOSA 77] Yosaki, Edward K., Sr. "The Many Faces of the DBA," *Datamation*, (May 1977) pp. 75-79.
The problems of placing the DBA in an organization are explored.

U.S. GOVERNMENT PRINTING OFFICE : 1982 O - 358-178

NBS TECHNICAL PUBLICATIONS

PERIODICALS

JOURNAL OF RESEARCH—The Journal of Research of the National Bureau of Standards reports NBS research and development in those disciplines of the physical and engineering sciences in which the Bureau is active. These include physics, chemistry, engineering, mathematics, and computer sciences. Papers cover a broad range of subjects, with major emphasis on measurement methodology and the basic technology underlying standardization. Also included from time to time are survey articles on topics closely related to the Bureau's technical and scientific programs. As a special service to subscribers each issue contains complete citations to all recent Bureau publications in both NBS and non-NBS media. Issued six times a year. Annual subscription: domestic $16; foreign $20. Single copy, $3.75 domestic; $4.70 foreign.

NOTE: The Journal was formerly published in two sections: Section A "Physics and Chemistry" and Section B "Mathematical Sciences."

DIMENSIONS/NBS—This monthly magazine is published to inform scientists, engineers, business and industry leaders, teachers, students, and consumers of the latest advances in science and technology, with primary emphasis on work at NBS. The magazine highlights and reviews such issues as energy research, fire protection, building technology, metric conversion, pollution abatement, health and safety, and consumer product performance. In addition, it reports the results of Bureau programs in measurement standards and techniques, properties of matter and materials, engineering standards and services, instrumentation, and automatic data processing. Annual subscription: domestic $11; foreign $13.75.

NONPERIODICALS

Monographs—Major contributions to the technical literature on various subjects related to the Bureau's scientific and technical activities.

Handbooks—Recommended codes of engineering and industrial practice (including safety codes) developed in cooperation with interested industries, professional organizations, and regulatory bodies.

Special Publications—Include proceedings of conferences sponsored by NBS, NBS annual reports, and other special publications appropriate to this grouping such as wall charts, pocket cards, and bibliographies.

Applied Mathematics Series—Mathematical tables, manuals, and studies of special interest to physicists, engineers, chemists, biologists, mathematicians, computer programmers, and others engaged in scientific and technical work.

National Standard Reference Data Series—Provides quantitative data on the physical and chemical properties of materials, compiled from the world's literature and critically evaluated. Developed under a worldwide program coordinated by NBS under the authority of the National Standard Data Act (Public Law 90-396).

NOTE: The principal publication outlet for the foregoing data is the Journal of Physical and Chemical Reference Data (JPCRD) published quarterly for NBS by the American Chemical Society (ACS) and the American Institute of Physics (AIP). Subscriptions, reprints, and supplements available from ACS, 1155 Sixteenth St., NW, Washington, DC 20056.

Building Science Series—Disseminates technical information developed at the Bureau on building materials, components, systems, and whole structures. The series presents research results, test methods, and performance criteria related to the structural and environmental functions and the durability and safety characteristics of building elements and systems.

Technical Notes—Studies or reports which are complete in themselves but restrictive in their treatment of a subject. Analogous to monographs but not so comprehensive in scope or definitive in treatment of the subject area. Often serve as a vehicle for final reports of work performed at NBS under the sponsorship of other government agencies.

Voluntary Product Standards—Developed under procedures published by the Department of Commerce in Part 10, Title 15, of the Code of Federal Regulations. The standards establish nationally recognized requirements for products, and provide all concerned interests with a basis for common understanding of the characteristics of the products. NBS administers this program as a supplement to the activities of the private sector standardizing organizations.

Consumer Information Series—Practical information, based on NBS research and experience, covering areas of interest to the consumer. Easily understandable language and illustrations provide useful background knowledge for shopping in today's technological marketplace.

Order the **above** *NBS publications from: Superintendent of Documents, Government Printing Office, Washington, DC 20402.*

Order the **following** *NBS publications—FIPS and NBSIR's—from the National Technical Information Services, Springfield, VA 22161.*

Federal Information Processing Standards Publications (FIPS PUB)—Publications in this series collectively constitute the Federal Information Processing Standards Register. The Register serves as the official source of information in the Federal Government regarding standards issued by NBS pursuant to the Federal Property and Administrative Services Act of 1949 as amended, Public Law 89-306 (79 Stat. 1127), and as implemented by Executive Order 11717 (38 FR 12315, dated May 11, 1973) and Part 6 of Title 15 CFR (Code of Federal Regulations).

NBS Interagency Reports (NBSIR)—A special series of interim or final reports on work performed by NBS for outside sponsors (both government and non-government). In general, initial distribution is handled by the sponsor; public distribution is by the National Technical Information Services, Springfield, VA 22161, in paper copy or microfiche form.