United States General Accounting Office

GAO

Office of Policy

September 1990

Assessing the Reliability of Computer-Processed Data

Preface

Auditors and evaluators rely on data to accomplish their assignment objectives. In today's computer age, more and more of the data available to them are computer-based and processed. Such data may come from a microcomputer, minicomputer, or mainframe and may range from a collection of questionnaire responses to large national data bases.

In considering the use of computer-based data, the following logical questions arise:

- How do the data relate to the assignment's objective(s)?
- What do we know about the data and the system that processed them?
- Are the data reasonably complete and accurate?

The Government Auditing Standards—generally referred to as the "Yellow Book"—provide the standards and requirements for financial and performance audits. A key standard covers the steps to be taken when relying on computer-based evidence.

The purpose of this guide is to help GAO staff meet the Yellow Book standard for ensuring that computer-based data are reliable. The guide also provides a helpful conceptual framework to expedite job performance and help staff address standards for assessing internal controls and compliance with applicable laws and regulations.

The key steps in assessing reliability are:

- Determine how computer-based data will be used and how they will affect the job objectives.
- Find out what is known about the data and the system that produced them.

- Obtain an understanding of relevant system controls, which can reduce the risk to an acceptable level.

- Test the data for reliability.

- Disclose the data source and how data reliability was established or qualify the report if data reliability could not be established.

The work described in this guide should normally be done by auditors and evaluators as an essential part of assignment planning. However, in those cases where computer specialist skills are needed, every effort should be made to secure these skills.

The major contributors to this guide were Dan Johnson and Charles M. Allberry. For further assistance, please call 275-6172.

Werner Grosshans
Assistant Comptroller General
for Policy

Contents

Chapter 5 Case Study: Guaranteed Student Loans

Appendixes

Tables

Abbreviations

ADP	automated data processing
DMTAG	Design, Methodology, and Technical Assistance Group
GAO	General Accounting Office
IG	Inspector General
OSM	Objectives, scope, and methodology
TAG	Technical Assistance Group

Chapter 1

Introduction

This chapter discusses

- standards and requirements for using computer-based evidence contained in GAO's "Yellow Book",
- the purpose of this guide,
- distinctions between a full system review and a more limited effort,
- when (during the assignment) data reliability should be determined including options to consider when data is unreliable,
- who should determine data reliability, and
- definition of terms.[1]

Government Auditing Standards

As part of the evidence standard for performance audits, GAO's Government Auditing Standards (the Yellow Book) and chapters 4 ("Standards") of the General Policy Manual and the Project Manual include requirements for determining the reliability of computer-based information.

The Yellow Book gives the following guidance:

When computer-processed data are an important or integral part of the audit and the data's reliability is crucial to accomplishing the audit objectives, auditors need to satisfy themselves that the data are relevant and reliable. This is important regardless of whether the data are provided to the auditor or the auditor independently extracts them. To determine the reliability of the data, the auditors may either (a) conduct a review of the general and application controls in the computer-based systems including tests as are warranted; or (b) if the general and application controls are not reviewed or are determined to be unreliable, conduct other tests and procedures.

[1] This guide supercedes the publication, Assessing the Reliability of Computer Output (AFMD-81-91) dated June 1981.

When the reliability of a computer-based system is the primary objective of the audit, the auditors should conduct a review of the system's general and application controls.

When computer-processed data are used by the auditor, or included in the report, for background or informational purposes and are not significant to the audit results, citing the source of the data in the report will usually satisfy the reporting standards for accuracy and completeness set forth in this statement.

Using This Guide

This guide helps staff ensure that their use of computer-based data meets Yellow Book requirements. It applies to both performance and financial assignments.

Staff should not assume that computer-based data are reliable. When using computer-processed data as evidence, staff must take steps to provide reasonable—not absolute or complete—assurance that the data are valid and reliable. Effectively carried out, the steps discussed in this guide will provide that assurance. They will not—nor do they need to—ensure that all data errors are detected.

The effectiveness of carrying out the steps in this guide depends on judgment in determining how much to rely on system controls, how to test data, and how much testing to do. Errors in judgment have undesirable consequences—too much audit effort wastes valuable resources, while too little jeopardizes the credibility of our work.

System Review Versus a Limited Approach

There are basically two approaches to assessing the reliability of computer-based data, the **system review** generally performed by specialists and the more **limited approach** (which this guide addresses) designed for evaluators/auditors.

A **system review** assesses and tests all controls in a computer system for the full range of its application functions and products. These reviews (1) examine a computer system's general and application controls, (2) test whether those controls are being complied with, and (3) test data produced by the system. While this approach provides the best understanding of a system's design and operation, it tends to be time consuming. When the assignment's objective(s) dictate a complete system review, specialists should be consulted.

The **limited review** is targeted to particular data. As a result, it normally requires a less extensive understanding of general and application controls. Pertinent controls are examined to the extent necessary to judge the level of data testing needed to determine data reliability. This can usually be performed by generalist staff.

For most assignments using computer-based evidence, the more limited approach described in this guide is adequate. However, if GAO staff use a specific set of computer-based data for many different assignments during an extended period, the length and cost of a full system review may be warranted. Such a review (periodically updated) might be less expensive in the long run than individual determinations of data reliability using the procedures in this guide.

When Data Reliability Should Be Determined

The reliability of computer-based data should be determined early in the planning phase of an assignment. If an assignment relies on computer-based evidence, staff must know if the data are reliable. If the data are **not** sufficiently reliable to meet the assignment's objective(s), they cannot be used as the primary evidence and staff will need to plan alternative approaches. The following options should be considered and discussed with management and, as necessary, with customers:

- Seek evidence from other sources. Staff would need to determine the reliability of such data.
- Collect primary data to meet the assignment's objective(s), rather than use secondary source data. This would be possible only if the work could be completed in time to meet requester's needs.
- Redefine the assignment's objective(s) to eliminate the need to use unreliable data.
- Use the data, but explain their limitations and refrain from drawing unreasonable conclusions or recommendations. It is preferable to draw no conclusions or recommendations.
- Terminate the assignment if no other alternative is possible.

Assignment proposals should include adequate staff time and identify the specific skills necessary to complete reliability determinations in a timely manner.

Who Should Evaluate Computer-Based Data Reliability

This guide is designed for the use of evaluators/auditors. If expert help is needed, however, in carrying out this more limited approach, it should be obtained promptly. As with all evidence, evaluators/auditors are responsible for its reliability; computer-based data should be no different. The basic tests of evidence apply. It should be best evidence, competent, relevant and sufficient. In evaluating the competence of evidence the evaluator/auditor should carefully consider whether any reason exists to doubt its validity, completeness, and accuracy.

Terms Defined

Definitions of terms used in this guide are as follows:

Data reliability: A state that exists when data are sufficiently complete and error free to be convincing for their purpose and context. It is a relative concept that recognizes that data may contain errors as long as they are not of a magnitude that would cause a reasonable person, aware of the errors, to doubt a finding or conclusion based on the data.

Computer system controls: Policies and procedures that provide reasonable assurance that computer-based data are complete, valid, and reliable. They include general and application controls.

General controls: The structure, methods, and procedures that apply to the overall computer operations in an agency. They include organization and management controls, security controls, and system software and hardware controls.

Application controls: Methods and procedures designed for each application to ensure the authority of data origination, the accuracy of data input, integrity of processing, and verification and distribution of output.

Systems review: An assessment of general and application controls, test of the degree of compliance with those controls, and appropriate data tests.

Compliance testing: Verifying whether controls are being complied with during the system's operation. Compliance testing does not directly test whether particular computer data are valid and reliable.

Data testing: Testing to determine if particular data produced by a computer system are valid and reliable. Data testing does not establish the existence or adequacy of system controls or whether such controls are being complied with, but may reveal indications of control weaknesses.

Source record: Information, in manual or electronic form, which is the basis for original entry of data to a computer application.

Attribute test: An examination of a data element for a logical or defined characteristic; also referred to as an unconditional test. For example, the status of a loan application must be "approved", "denied", or "pending".

Relationship test: A comparison of values to validate a logical or defined correlation; also referred to as conditional tests. For example, an invoice date must be the same as or earlier than the related payment date.

Data element: An individual piece of information that has definable parameters (e.g., a social security number).

Data record: A collection of data elements relating to a specific event, transaction, or occurrence (e.g., name, age, social security number, school, date enrolled, loan date, loan amount, amount repaid, and loan balance).

Data file: A collection of data records relating to a specific population (e.g., student loan applications for Maryland schools).

Attributes: Characteristics of a data element defined by the data dictionary (e.g., numeric or alpha, acceptable values, and length).

Chapter 2

Assessing Reliability Risk, Understanding System Controls, and Determining Data Testing Requirements

This chapter introduces the process and decision points for conducting a reliability assessment of computer-processed data. It examines the elements which influence the level of data testing required including

- a conceptual framework,
- the planned use of the data relative to the assignment's objective(s),
- the existing knowledge base relating to the data and system, and
- the adequacy of system controls.

Conceptual Framework

When computer-processed data are being considered for use in an assignment, staff must initially determine the reliability risk—the risk that the data are unreliable for the planned use. As illustrated in table 2.1, reliability risk is determined by considering both planned use and present knowledge of the data or the computer system.

Table 2.1: Factors in Developing Reliability Risk

Planned use of data	+	Knowledge/ experience with data or system	=	Reliability risk
Sole Support to Meet Objectives		Unfavorable/ Nonexistent		High
		Adequate		Moderate
		Favorable		Moderate to Low
Corroborative support		Unfavorable/ Nonexistent		Moderate
		Adequate		Low
		Favorable		Very Low
Background		[Not a mitigating factor at this level]		Very Low

The second step (illustrated in table 2.2) is to understand system controls and determine if they lower the reliability risk. If system controls are strong, they can lower the reliability risk to an acceptable/ prudent level and decrease the data testing that would normally be required in a high risk environment.

Table 2.2: Factors in Determining Extensiveness of Data Testing

Reliability risk	+	Assessment of system controls	=	Extensiveness of reliability risk
High		Weak/Not Determined Adequate Strong		High High to Moderate Moderate to Low
Moderate		Weak/Not Determined Adequate Strong		Moderate Moderate to Low Low
Low		Weak/Not Determined Adequate Strong		Low Low to Very Low Very Low
Very Low		[Generally not necessary and not cost effective]		Very Low

Details of assessing reliability risk and determining the extensiveness of data testing needed to reduce that risk to an acceptable level appear in the sections that follow.

Planned Use of Data

When an assignment requires computer-processed data, the first step is to decide how the data will be used—how will they contribute to meeting an assignment's objective(s)?

Normally, data are used as

- the sole evidence supporting a finding,

- corroborative or supporting evidence, or
- background information.

If computer-processed data are the sole support for an assignment's objective(s), the need for confidence in their reliability is greatest. For example, assume GAO is asked to determine whether mine safety inspections are being made within a legislatively prescribed time frame. The agency under review has information in a computerized data base that directly addresses this question. If GAO plans to use information in that data base without corroborating evidence, establishing the reliability of the data base is critical to the assignment's objective(s).

When computer-based data are supported by other evidence, the need for complete confidence in that data varies depending on how effectively the other evidence—standing alone—could support the finding. For example, staff discussions with union representatives might reveal that regular mine inspections were not occurring, but such discussions were unable to clearly establish the interval between inspections. These discussions corroborate information in the agency's computerized data bases and add to its persuasiveness. The finding still leans heavily on the computerized data base, and determining its reliability is important.

The lowest risk of using computer-based data occurs when the data are used in the report for background or informational purposes and are not vital to audit results. In these cases, citing the data source in the report and ensuring that the data are the best available will satisfy reporting standards for accuracy and completeness unless there is reason to believe that inaccuracies in the data would jeopardize the report's credibility.

Knowledge/ Experience With System or Data

After deciding how the computer-based data will be used, the next step is to find out what is already known about the data and the system that processed them. This information combined with the planned use of the data, determines the reliability risk.

The following examples illustrate ways in which staff can learn more about the data or the system controls:

- GAO used the same data to support a prior finding after adequately establishing their reliability. The risk of using the data in a current report would be low. But updating would be needed to ensure that the data had not changed since they were last used.
- GAO recently established the adequacy of system controls used to process data critical to the assignment's objective(s). After determining that no significant changes had occurred in the system since the assessment, the reliability risk would be low. System controls could be considered good, and minimal data testing would be required.
- In a recent report, GAO cited information developed from a different application of the same computerized data base. Work previously done to determine the adequacy of general controls after updating could reduce the present data's reliability risk. Additional work would need to be done to establish the adequacy of relevant application controls and the level of data testing required.
- The inspector general or other audit/evaluation group studied the system controls or used the data. The results of the work could establish reliability risk, but the Yellow Book's due professional care requirement involving reliance on work performed by others would need to be met. (See Government Auditing Standards, pp. 3-14 through 3-16.)

System Controls

While some data testing is always necessary when computer-based evidence is used to meet an assignment's objective(s), satisfactory system controls can reduce the data testing required to establish reliability. In such cases, less data testing is needed than when those controls are weak or undetermined.

According to the Yellow Book,

> **The degree of testing needed to determine data reliability generally increases to the extent that the general or application controls were determined to be unreliable or were not reviewed.**

Understanding System Controls

Staff should understand system controls and their purposes to determine whether they can be relied on to reduce data testing. This understanding includes both **general** and **application controls** that relate to assignment evidence.

An understanding of **general controls** would include knowledge of the following items which affect data reliability.

- Management commitment to system design and operation: This includes management's methods for monitoring and following up on performance, including corrective action on internal audit recommendations and on user complaints.
- Organization of the system functions, including assignment of responsibilities and separation of duties: This provides that key duties and responsibilities in authorizing, processing, recording, and reviewing transactions are assigned to different individuals.
- Physical security of the computer facility and its components, including restrictions on access: Restricting access helps ensure data reliability by reducing the risk of unauthorized data entry or modification.
- Supervision: Effective supervision requires a clear communication of duties and responsibilities, regular oversight—particularly at critical points—and periodic performance evaluations.

In understanding **application controls**, staff should consider matters such as the following:

- procedures to ensure that application software and subsequent modifications are authorized and tested before implementation;
- frequency of system modification and the reasons for it;
- whether program changes are controlled and promptly documented;
- the review, approval, control, and editing of source transactions to ensure completeness and prevent error;
- tables used in computer processing, their sources, and the frequency of updating;
- the existence of current narrative system descriptions and flowcharts;
- reconciliation of output records with input entries;
- error detection and correction procedures;
- data user's views of data reliability; and
- internal audit reports and other evaluations or studies.

Regardless of how well-conceived and designed system controls may be, they are ineffective if applied incorrectly and inconsistently. For example, a system may have a control that requires a data quality control group to verify that source data are accounted for and that they are complete and accurate, have been appropriately authorized, and transmitted in a timely manner. But if that group is bypassed, the control contributes nothing to ensuring the integrity of data entry.

Many reasons exist for bypassing or overriding controls such as time pressures, fatigue, boredom, inattention—or even collusion for personal gain. As a result, staff should select the most significant control procedures and confirm adherence to them. Although it is unnecessary to test all procedures, staff should conduct sufficient tests to afford a reasonable basis for reducing testing by relying on the adequacy of controls. Observing the work environment for an ordered and businesslike atmosphere can be helpful.

Documentation of a well-controlled system should be complete and current. Absence of such documentation may indicate that controls do not exist or, if they do, that they are not understood or adequately applied. Other red flags that suggest vulnerability to data errors include

- old systems with high program maintenance;
- large volumes of data;
- frequent processing and updating activity;
- numerous transaction types and sources;
- large number of coded data elements;
- high employee turnover (e.g., data entry clerks, operators, and analysts) and inadequate training;
- complex or messy data structures; and
- lack of ADP standards, especially related to security, access, and program change control.

Discussions with knowledgeable agency personnel can provide an effective beginning in gaining an overall system understanding. Their testimonial evidence, however, should be corroborated through independent observations or tests whenever possible.

Relying on System Controls to Reduce Data Testing

Some data testing is essential whenever computer-based data will be used as evidence. Even when system controls are well designed and generally adhered to, data accuracy is not ensured. While staff can rely on good controls to reduce data testing, control reviews cannot substitute for data testing.

After reviewing controls, staff should evaluate their strength, that is, whether controls can be reasonably expected to prevent errors and to detect those that do occur. This evaluation determines whether extensive, moderate, or minimal data testing is needed.

Staff should keep the purpose of reviewing the controls in mind as they progress. If it is determined that (1) system controls cannot be relied on to limit data testing or (2) continuing the controls review is more costly than expanding data testing, the review should cease. In this case, staff must proceed with data testing as if system controls were weak or nonexistent.

Documenting the Basis for Extensiveness of Testing

The workpapers should be documented to disclose:

- What assignment objective(s) will computer-processed data likely support?
- How will the data support that objective?
- Will that objective be supported by other evidence? What is the other evidence?
- What is known about the data?
- What did staff do to understand the system and its controls?
- Did staff determine the reliability of system controls? If so, are the controls strong, adequate, or weak?

Chapter 3

Data Testing

This chapter discusses

- the objectives and methods of data testing,
- the appropriateness of varying testing levels, and
- factors to consider when using computer-assisted testing techniques.

Objectives and Methods of Data Testing

Yellow Book standards require evidence (regardless of its source or format) to be competent, relevant, and sufficient. Data reliability focuses on assessing the competency of data. Data testing is intended to establish that evidence relied on is suitably accurate for its specified purpose.

While it is unlikely that any computer system contains error-free data, the concept of reliability does not require perfect data. It should, however, include steps to assess data completeness, data authenticity, and the accuracy of computer processing.

Tests of data completeness confirm that the universe contains all data elements and records relevant to the assignment's objective(s) and to the period covered by the audit. Missing data is particularly harmful if it represents a specific segment of the total population (e.g., all grant recipients from California).

An analysis of data authenticity determines if the computer-based data accurately reflect the source records.[1] This means that information in source records should match that entered in computer-based records and that each computer-based record should be supported by a source record.

Steps aimed at the accuracy of computer processing are designed to verify that all relevant records were

[1] Appropriate steps should also be taken to insure that the information contained in source records is factual. If this is not done, related limitations on the data should be fully disclosed in the report.

completely processed and that computer processing met the intended objectives.

There are two varying approaches to testing computer-based data. They are characterized as auditing **around** the computer or auditing **with** the computer. The appropriate approach or combination of approaches is dependent on the nature of the related system.

Auditing Around the Computer

Auditing around the computer assumes that techniques and procedures the computer uses to process data need not be considered as long as there is a visible audit trail and/or the result can be manually verified. This approach bypasses the computer in either of two ways.

In the first way, computer output is compared to or confirmed by an independent source. This approach confirms computer-processed data with third parties or compares data with physical counts, inspections, records, files, and reports from other sources. Physical counts and inspections can verify quantity, type, and condition of tangible assets. Reports on government programs and activities issued by outside contractors, universities, audit and privately-funded organizations, and others can contain a useful basis for comparison.

Examples of sources from which confirmation can be obtained include

- banks (cash balances on hand or amounts of loans);
- warehouses (assets stored or volume of transfers);
- training institutions (number of students or dollar volume of contracts);
- common carriers (rates for freight shipments or volume of passengers between selected locations);
- medical facilities (daily rates for patient care or types of outpatient services);
- private business concerns (billings for utility services or wholesale prices of generic drugs); and

- other government agencies (checks cancelled by a U.S. Treasury Department disbursing center or statistics on an agency's use of General Services Administration automobiles).

Staff can also conduct common-sense examinations of printed data output to reveal potential reliability problems. These inspections can establish data reliability when a low to very low level of data testing is required. When a moderate to high level of testing is required, these tests should be supplemented by more extensive procedures. The following questions are examples of common-sense data tests:

- Are amounts too small (cost per mile to operate a 1-ton truck equals $.004)?
- Are amounts too large (a student loan for $150,000)?
- Are data fields complete (a loan payment amount is blank)?
- Are calculations correct (inventory value is a negative amount)?

Although confirmations and comparisons directly test the accuracy of computer output and effectively disclose fictitious data, they may not detect incomplete data input. When data completeness is in doubt, confirmations or comparisons should be supplemented by tracing a sample of source records to computer output.

The second way to bypass the computer in confirming data reliability is to select source transactions, manually duplicate the computer processes, and compare the results with computer output. Examples include

- benefit payments for selected grant recipients,
- loan balances and delinquent amounts,
- resale prices of foreclosed and repossessed properties, and
- salary payments.

Although this approach can test the completeness of computer output as well as the accuracy of computer processing, it does not disclose fictitious data (i.e., data that have been entered into the computer but are not supported by source records). If fictitious data are an issue, tracing data from the computer to source records should be considered.

The usefulness of auditing around the computer diminishes as the number and complexity of computer decisions increase. It may be impractical when sophisticated data processing activities are involved.

Auditing With the Computer

Auditing with the computer means that computer programmed tests are used, in part, to measure data reliability.

After determining the completeness and accuracy of computer input by manually tracing data to and/or from a sample of source records, this approach uses auditor-developed computer-programmed tests to examine data reasonableness and identify defects that would make data unreliable.

An advantage of auditing with the computer is that it can be used regardless of the computer system's complexity or the number of decisions the computer makes. Auditing with the computer is also fast and accurate, permitting a much larger scope of testing than would be practical with other methods.

The first step in developing computer-programmed tests is to identify what computer information is to be used as evidence and what data elements were used to produce it. Staff should test all data elements that affect the assignment's objective(s).

When an audit-significant data element is derived (i.e., calculated by the computer based on two or more data elements), staff should also test the source data elements. For example, the element "net pay" might be planned for use as evidence to meet an assignment's objective(s). Review of the system's data dictionary shows that a computer program uses three other data elements to calculate net pay—"hourly rate", "hours worked", and "deductions". Errors in any of these data elements would make "net pay" incorrect. Therefore, staff should determine the accuracy of each.

After identifying the relevant data elements, the data dictionary can be examined to define the attributes of each and identify rules which each should meet. If a data element fails these requirements, the computer may exclude it or process it in a way that does not ensure an accurate result. Computer programs frequently have default logic that may cause a missing or defective data element to be erroneously processed.

For example, data to be entered into a computer may identify whether a project is ongoing or completed. If the data element is not entered for a specific record, a computer program prescribes treatment of the missing data. The record could be put in an error file until the missing data is provided, or a programmed assumption could be made about its status (i.e., if the status is blank, then the project is ongoing). If that assumption is incorrect in enough records, that data element will be unreliable.

Understanding a data element also makes it possible for staff to develop reasonableness assumptions that can be programmed as common-sense tests—for example, can a student loan recipient be a 12-year-old? Common-sense tests do not establish that a data element is erroneous. They raise red flags for follow-up. Although it is possible for a 12-year-old to be a college student, it is unlikely. (Other examples of common sense tests are included on page 22.)

Data attributes should also consider expected relationships among data elements. Although developed independently, a data element may have a reasonable relationship to another data element. For example, some kinds of medical procedures are age- or gender-related. Determining and testing relationships can reveal errors by disclosing irrational or unlikely relationships such as a hysterectomy on a male patient.

When staff have learned about each of the data elements that affect the information relied on, tests are developed to detect errors. Tests are of two types: those that disclose failures of data elements to meet established requirements and those that disclose illogical relationships. (See appendix I for discussion and examples of these test types).

After data tests are developed, the computer is programmed to apply them. The programmed data tests must be validated and tested to ensure that errors revealed during the data testing are the result of incorrect data and not the result of invalid test programs.

Data tests can be developed without knowledge of the technical design of the data base, its structure, and layout. This knowledge, however, is needed to program the tests. If assignment staff are unfamiliar with the necessary programming techniques, support is available from their division's design, methodology, and technical assistance group (DMTAG) or region's technical assistance group (TAG).

Whether a microcomputer or a mainframe should be used to process data tests depends on factors such as the size of the data base, the number and complexity of data tests, required processing speed, computer accessibility, and team expertise. If a mainframe is required, staff will almost certainly need to get support from their DMTAG or TAG.

Commonly available retrieval or analysis applications may be used for programming tests. These include products such as Lotus 1-2-3, dBASE, SAS, SPSS, and DYL-280. While some programs have been successfully used in testing data bases of over a million records, staff should take care to ensure that test requirements are properly matched to the application and to the operating environment (micro- versus mainframe computer).

Various Levels of Data Testing

As stated in chapter 2, the level of data testing depends on the reliability risk (based on data use and experience with the data) and staff judgment of the adequacy of system controls. The greater the reliability risk, the more assurance is required to reduce the risk to an acceptable level.

If a low level of data testing is adequate to establish the reliability of computer-processed data, it may be most appropriate to test only those items which in the auditor's judgment are most likely to have errors. At this level of testing, reliance for data acceptability rests primarily on staff judgment of system controls. Data tests provide some confirmation that relied-on system controls were operating effectively. A judgmental sample size, which is randomly selected, can give this confirmation but will not define the confidence or precision levels achieved by the testing.

If data test results detect no errors or suggest an error rate that is acceptable for the data's planned use, the data could be considered reliable. If, however, the test error rate is high, staff evaluation of system control adequacy—on which reliance was placed—may have been in error. In this case, sample size and scope of testing should be increased or a statistically valid approach used to provide a defensible basis for a decision on data reliability.

If moderate to high data testing is needed, reliance is primarily on data testing rather than on system controls. Sufficient tests should be performed to reasonably assure detection of significant errors. If sampling methods are used, an adequate sample size would be necessary to permit appropriate precision levels to be calculated and support the test results.

A number of statistical approaches are discussed and illustrated in Transfer Paper 6, Using Statistical Sampling. The statistical approach depends on whether GAO needs only to determine whether the error rate is acceptable or whether it is necessary to quantify the error rate.

Special Considerations in Computer-Programmed Data Tests

Because of the computer's speed, computer-programmed tests (used in auditing with the computer to detect data defects and inconsistent relationships) are usually not sampled but run against all records for each data element tested. Only when using very large data bases would it be necessary to limit testing to a sample of records. The testing level (high, moderate, or low) normally relates to the number of tests applied rather than to the number of data elements or records tested. If low-level data testing is adequate, it might be limited to those tests that disclose failures of data elements to meet established requirements. Moderate to high testing levels would contain a wider variety of tests, including increased use of relationship tests. See appendix I for a discussion of various data tests.

In using results of computer-processed data tests, staff should consider whether the same record or data element failed more than one data test. If so, the error rate may need to be adjusted. The following examples illustrate this situation:

Assume that for the data element, "loan balance", staff conducted two tests on a universe of 100 records. A range test counted any loan balance below $0 or greater than $10,000 as an error. A derivation test defined an error as any loan balance which did not equal "original loan amount" plus "interest charges" minus "loan payments to date". Results were as follows:

Test	Data errors
Range	5
Derivation	0

Since all errors relate to one test, the error rate is 5 percent.

But assume the following results for the same tests.

Test	Data errors
Range	5
Derivation	5

In the second example, each test identified failures. Based on these results, from 5 to 10 percent of the data are defective. The actual error rate depends on whether a record failed one or both tests. If a 10-percent rate would cause the data to be unreliable, staff would need to make additional tests to determine if the same records were defective in the various tests.

Data tests that detect inconsistent relationships between data elements establish the likelihood of error, but do not identify which data element is defective. Staff must run additional tests or perform other audit work to determine which data element to rely on. Similarly, the failure of a data element to meet an expected attribute signals a potential error. Additional follow-up (e.g., discussions with knowledgeable agency personnel) may identify acceptable explanations. Only after defective data are confirmed can the error rate be correctly calculated.

Whenever an error rate is unacceptable, staff may consider two actions to make the data usable:

- Repair the defective data elements. By doing this, the acceptability of the corrected data error rate could be determined.
- Exclude the defective data records from the assignment universe. By doing this, the data element used to support audit findings, conclusions, or recommendations includes only data not found to be defective. This approach is inappropriate, however, when the data exclusion would introduce a systemic bias in assignment results. (See General Policy Manual and Project Manual, chapter 10, "Methodology," for a discussion of systemic and random bias.)

Chapter 4

Reporting on Data Reliability

This chapter discusses the reporting requirements when using computer-based data to meet the assignment's objective(s). In addition, it suggests sample report language for cases in which the data are

- reliable,
- unreliable but still usable,
- unreliable and not usable, and
- not assessed for reliability.

Reporting on Computer-Based Evidence

Completeness and accuracy reporting requirements of the Yellow Book and GAO's Communications Manual (12.8) require that data sources and the methods used to determine data reliability should be stated in the report. When material is included in a report for background or informational purposes and is insignificant to audit results, staff can normally meet this reporting standard by citing the data source in the report.

For computer-processed data which is critical to the assignment's objective(s), the report should assure readers that the information relied on is credible and reliable. Specifically, it should

- identify the scope of work done when system controls are relied on to reduce data testing;
- describe the testing of the computer-processed data, including the tests performed, their purpose, and the error rates disclosed; and
- present any factors known to limit the data's reliability and if significant, the sensitivity of the results to the accuracy of the data.

If sampling was used to determine data reliability, the description should include the purpose of the sample; the universe and sample sizes; the basis of the sample size (judgmental or statistical); the type of sample (simple random, stratified, and so on); confidence levels and precision; and errors detected.

Staff should include a summary of the above in the objectives, scope, and methodology (OSM) section of the report. Technical details of complex sampling methods and computer-programmed data tests may appear in the body of the report or in a technical appendix.

If data reliability was not determined or was not determined to the extent normally desired, the product should include a clear statement to that effect as well as a qualified conformity statement. In these cases, statements of negative assurance[1] may be useful. Auditors/evaluators should consider the appropriateness of presenting any conclusions or recommendations based on the data.

The following are examples of report language that can be used in the OSM to meet established reporting standards.

Reliable Data Is Used

"To achieve the assignment's objective(s) we extensively relied on computer-processed data contained in [cite data base used]. We assessed the reliability of this data including relevant general and application controls and found them to be adequate. We also conducted sufficient tests of the data. Based on these tests and assessments we conclude the data are sufficiently reliable to be used in meeting the assignment's objective(s)."

Unreliable Data Still Usable

"To achieve the assignment's objective(s) we extensively relied on computer-processed data contained in [cite the data base used]. Our review of system controls and the results of data tests showed an error rate that casts doubt on the data's validity.

[1] Negative assurance is a statement that nothing came to the auditor/evaluator's attention as a result of specified procedures that caused them to doubt the acceptability of the data. The auditor/evaluator, by using other data and information, came to the conclusion that the data could be relied on to achieve the assignment's objective(s).

However, when these data are viewed in context with other available evidence, we believe the opinions, conclusions, and recommendations in this report are valid."

Unreliable Data Not Usable

"To achieve the assignment's objective(s) we extensively relied on computer-processed data contained in [cite the data base used]. Our review of system controls and the results of data tests showed an error rate that casts doubt on the data's validity. Since the assignment's objective(s) require specific statements based on this data and sufficient independent evidence is not available, we were unable to provide specific projections, conclusions, or recommendations.

Reliability Is Not Determined

"To achieve the assignment's objective(s) we extensively relied on computer-processed data contained in [cite the data base used]. We did not establish the reliability of this data because [cite the reason(s)]. As a result, we are unable to provide projections, conclusions, or recommendations based on this data.[2] Except as noted above, GAO's work was conducted in accordance with generally accepted government auditing standards."

If the reliability of critical data is not determined, an exception to the generally accepted auditing standards is necessary. Staff should discuss the circumstances with the Assistant Comptroller General for Planning and Reporting and obtain approval before final processing.

[2] There may be cases where sufficient other data could be relied on to draw conclusions and recommendations from such data, because the issues are broader (i.e., policy issues), where preciseness of data is not of paramount importance. In those rare cases, conclusions and recommendations may be appropriate, but full disclosure is needed. Staff should also consider the limitations discussed on page 20, footnote #1.

Chapter 5

Case Study: Guaranteed Student Loans

This chapter presents a case example of how to determine the reliability of computer-based evidence. It discusses appropriate steps for

- assessing the reliability risk,
- examining the adequacy of system controls, and
- performing data testing at both an extensive and minimal level.

Case Example

The following case illustrates how to apply the requirements, concepts, and principles discussed in this guide to an assignment. The circumstances of this case are hypothetical and are intended to illustrate the factors affecting the extent of data testing.

Assignment Objectives

Assume that GAO has been requested to review the Stafford Student Loan Program and determine if

- the Department of Education is paying the correct amount of interest and special allowance (interest subsidy) to lenders,
- payments are made to lenders in a timely manner, and
- interest payments are being made for defaulted loans.

Background

Under the program, private lenders make loans at lower-than-market interest rates to qualified students attending approved educational institutions. The Department of Education pays the interest while the student attends school and for a stipulated grace period thereafter. Education also funds special allowance payments during the life of the loan to provide lenders the difference between the loan interest rate and the rate on 90-day Treasury bills, plus 3-1/4 percent. If borrowers default on their loans, Education repays the loan (usually through state agencies) and stops paying interest and special allowances.

The Department of Education makes interest and special allowance payments directly to lenders based on detailed quarterly billings. Lenders' billings are entered into Education's computerized system, which summarizes and authorizes payments to lenders for interest and special allowances. A separate data base maintains information on defaulted loans.

Assignment Approach

Since the computer-based data compiled by Education contains information relating to interest payments and defaults, staff have identified it as a key source of evidence to support their objective(s). However, before beginning an analysis of this information, auditors/evaluators must assure themselves that the data are reliable. For example,

- Are individual loan amounts correct?
- Are interest calculations accurate?
- Do all records apply to the time period of our audit/evaluation?
- Are dates of loan defaults accurate?
- Are lender identification codes correct?

Reliability assessment procedures should include:

- determining the importance of the computer-based data in meeting the assignment's objective(s),
- determining what past experience and current knowledge is available about the data and the system which processes them,
- reviewing general and application controls to the extent they can be relied on to reduce the level of data testing, and
- developing and performing data tests.

These efforts are focused on providing reasonable assurance that the data does not contain significant errors which would undermine the credibility of our analyses and conclusions.

Determining Reliability Risk

The first step in meeting the case study objectives is to determine the reliability risk. This includes the risk that Education's computerized data do not accurately state amounts paid to lenders for interest payments and special allowances and the risk that default data do not accurately reflect the eligibility of loans for continuing interest payments. Reliability risk is determined by considering both the planned use of the data and the existing knowledge of the computer system and its data.

Planned Use of Data

In gauging how the planned use of computer-based data affects reliability risk, staff should consider matters such as the following:

- Will the data be important in determining the accuracy and appropriateness of payments made to lenders? Will the data merely provide background information or provide a context for the assignment's conclusions? Background information normally suggests a very low reliability risk.
- Is the computer-based data the only evidence available regarding payments made to lenders? Is the computer-based data part of a broader body of corroborating evidence? Evidence used as sole support suggests a high reliability risk, while the reliability risk of corroborative evidence is moderated by the strength of the other evidence.
- Is the issue of student loan payments and eligibility so sensitive that the accuracy of any data presented (even when used as background) is likely to be challenged? If there is reason to believe that the data's accuracy will be questioned, regardless of its use in the report, the reliability risk increases.

Knowledge and Experience With Data

The second component of reliability risk is recent experience or knowledge of the data and related system. Favorable experience and/or knowledge can reduce reliability risk, limit the review of system controls, and reduce data testing. Unfavorable experience and/or knowledge leads to increased doubts and requires greater assurance that data is accurate.

In compiling information about the data and its system the auditor/evaluator should address the following questions:

- Has GAO used this data base to provide supporting evidence in prior assignments? If so, what was our assessment of its reliability at that time?
- Has the Department of Education's Inspector General staff reviewed the related system or assessed the reliability of the data? If so, what recommendations, if any, did they make for improving system controls? Did Education officials take steps to implement these recommendations? What opinion, if any, did the IG express regarding data reliability?
- What do Education officials and users say about the data's accuracy? How frequently do they encounter errors with the data? How serious are these problems? Do they rely on the data in performing their duties or do they maintain separate manual records?
- Have lenders, state agencies, or loan recipients reported payment problems or concerns?
- Do corroborating sources of information tend to support or contradict the computer-based data?

When evaluated together, the planned use of the data and the current knowledge about it help the auditor/evaluator identify a level of risk. Lowering that risk to an acceptable level can be accomplished by performing detailed tests of the data. While the need for data testing can never be completely eliminated from an assignment, the extent of testing can potentially be reduced by assessing the system of controls.

Understanding System Controls

Understanding and assessing controls is a normal auditing activity. Strong system controls can diminish the reliability risk, thus reducing the amount of data testing needed to determine data reliability. In turn, knowledge and experience with the data can help direct the review of system controls to areas where they are most likely to be weak.

System controls must be considered in terms of both general and application controls. Work should include gaining an understanding of those controls and observing that significant controls are being followed.

A review of general controls should include the following questions:

- Does Education's management take an active role in decisions affecting ADP functions?
- Do external auditors and/or the IG routinely conduct reviews of ADP functions? Have Education officials implemented all past audit recommendations related to ADP operations?
- Does Education's organization provide adequate separation of duties within the ADP operation?
- Does Education have standards for documenting ADP functions?
- Do formal procedures exist for requesting, approving, testing, and implementing system changes?
- Are appropriate measures in place to physically secure Education's computer facility and control user access to the system and data files?

A review of application controls should consider:

- Does Education have formal documentation which identifies procedures for data collection, authorization, input, and error handling?
- Does Education's system perform edit checks on data prior to combining them with the existing data base? If so, what are those edits?
- Is data which fails to meet input requirements identified, corrected, and re-entered to the system in a timely manner?

- Are reconciliations performed to insure that all source input is accounted for?
- Are system outputs reconciled against inputs to account for all data?

The amount of time and effort expended in understanding and assessing system controls is directly related to the potential reduction on detail data testing. The "cost" of system control tasks should not outweigh the "benefits" of reduced data testing.

The strength of system controls falls into a range with the following end points.

- Strong controls: This judgment assumes missing or ineffective controls (if any) are minor; the overall system could be expected to detect and correct any significant data errors.
- Weak controls: This judgment assumes that missing or ineffective controls provide an opportunity for significantly incorrect data to be introduced to the data base. Control deficiencies could pervade the entire system or affect only parts of it.

Data Testing

By considering the strength of system controls in relation to the reliability risk, a level of data testing is established. The type of tests are dictated by the nature of the data and the ultimate data analysis to be conducted.

Case 1: Extensive Testing

Assume that auditors/evaluators have determined that Education's computer-based data is the only existing source of payment data. Since neither GAO nor the IG have done any recent work with this data, the reliability risk is high. The auditors/evaluators have further determined that general and application controls are inadequate. In this instance, the results of data testing alone must provide the basis for reliance. Therefore, the number and scope of tests will be extensive.

After conducting procedures to determine that information contained on the lender billing statements is factual, staff should conduct tests to determine the accuracy and completeness with which that data was entered into the computer. This testing should generally be based on statistically valid sample sizes and methods. Specifically, tasks would include

- matching computer-based records against corresponding source records to measure the data input error rate, and
- matching source records against corresponding computer-based records to determine that all relevant data had been entered into the computer.

Computer-assisted procedures could then be performed on all computer-based records to verify that

- billing and payment dates fall within the assignment's time frame,
- key data elements are present in all records (i.e. billing date, payment date, payment amount, loan balance, and so on),
- there are no negative payment amounts or zero loan balances, and
- payment amounts and loan balances fall within "reasonable" ranges.

Further automated tests could be designed to

- re-compute lenders' interest calculations,
- sort and summarize payments by lender to identify duplicate records,
- match lenders against Education's list of eligible institutions,
- compare payment dates against billing dates to determine that billing dates precede payment dates,
- compare loan status against default date to insure that all defaulted loans contain a default date, and
- compare loan status against payment amount to identify records showing payments on defaulted loans.

In addition, staff should review the automated error file to determine if it includes billings for the period that have not been processed.

The failure of a data element or record to pass a reliability test does not prove the data is incorrect. It merely identifies a potential matter for further investigation.

The results of these tests and the follow-up investigations will provide numeric error rates. Based on the error rate and the seriousness of errors, the auditor/evaluator will make a judgment about the data's reliability.

Case 2: Minimal Testing

Although the circumstances of this case do not lend themselves to a discussion of minimal data testing, assume that GAO staff used data from the same data base to support report findings within the last 6 months. At that time, we concluded that system controls were strong and the data was reliable. Under this scenario, the reliability risk would be low. An extensive system control assessment would not be performed. Reliance would be placed primarily on our prior knowledge and experience with the data. However, even at this low risk level, some testing should be performed to update the results of previous work and detect any conspicuous errors.

Our understanding of the system controls should be updated to determine

- what, if any, modifications have been made to the system,
- that critical controls are still being adhered to, and
- that any previous recommendations relating to system controls have been implemented.

Tracing computer records to source records and vice versa to show completeness and accuracy of data input could be accomplished through use of small (judgmental) randomly selected samples.

Computer-assisted procedures, aimed at locating large errors, would verify that

- all billing and payment dates fall within the assignment's time frame,
- key data elements are present in all records (i.e. billing date, payment date, payment amount, loan balance, and so on),
- there are no negative payment amounts or zero loan balances, and
- all payment amounts and loan balances fall within "reasonable" ranges.

If these basic tests produced significant error rates, the scope of testing would be expanded. Otherwise, based on the updating of prior reliability work, auditors/evaluators would conclude the data is reliable.

Appendix I

Examples of Data Tests

This appendix describes some data tests which should be considered in developing an overall testing plan. The number and combination of tests performed for a given assignment will be influenced by the required level of testing, the complexity and size of the data base, and established time frames.

Unconditional Data Tests

The following are examples of data tests that disclose failures of data elements to meet established requirements:

- Derivation tests identify data errors by using formulas or tables to recalculate computer-generated data elements.
- Mode tests disclose data that are defective because they do not comply with the numeric or alpha requirement for the data element.
- Pattern tests disclose data errors evidenced by inconsistencies of a specific pattern of digits and characters. Calendar date checks are a pattern test that has considerable significance for some data elements.
- Presence/absence tests disclose data that are defective because they lack required information or include information when they should not.
- Sign tests detect data defects that result from an inappropriate positive or negative value.
- Value/range/limit tests detect data that are defective because they are not within a required set of specific values; a set of values that fall into a given range; or a set of values encoded in a list, table, or file.

It is generally useful to test audit-significant data elements against each of the requirements defined for them. (Consult the data dictionary.)

Conditional Data Tests

The following are examples of tests that compare two data elements that have a logical relationship:

- If college graduation date is given, the type of degree must be identified.
- If loan date is between July 1, 1989, and September 30, 1989, the interest rate must be 12.5 percent.
- Loan approval date must be the same as or later than the loan application date.
- If order quantity is greater than 5,000, the discount rate must be 40 percent.
- If payments to an individual under a given entitlement program exceed $10,000 in fiscal year 1988, the eligibility code must be "C."
- The number of program graduates must equal the number enrolled minus program dropouts.

These tests are not limited to comparisons of two data elements in the information system's data base. They can include data rules that compare particular data elements with program or legislative criteria or with information from another data system.

In developing data rules, staff should consider whether reverse relationships exist among data elements. When information systems are developed, data rules built into the system establish requirements for data elements and for relationships among them. At times, reverse relationships are not considered, and reversing data rules is not part of system logic. In those cases, the likelihood of data errors is increased.

Well-thought-out reverse rule tests can effectively disclose data inconsistencies (overlooked in systems design) that have contributed to data base contamination over time. A data rule could, for example, test the requirement that if status is deceased, the date of death must be present and valid. A reverse data rule could reasonably test that if a date of death is present and valid, the status must be deceased.

Staff must exercise care, however, because seemingly reasonable reverse relationships do not always exist. For example, the rule, "if status is eligible, then annual income must be less than $10,000," could be tested. But eligibility restrictions may involve factors other than income, for example, age. If that is the case, the reverse data rule—"if annual income is less than $10,000, then status must be eligible"—could not be used.

Special Considerations in Understanding Computer System Controls

This appendix presents a sample of possible questions relating to general and application controls. They are intended to help relate the internal control approaches generally followed in performance audits to the computer environment.[1]

General Controls

General controls apply to all computer processing carried out at a facility and are independent of specific applications. They relate to organization; system design, development, and modification; and security.

Organization

Does top level management take an active role in ADP functions?

Does the ADP function received continuing audit coverage?

Is there evidence of effective actions to follow-up on past audit recommendations?

Is there adequate separation of duties within the ADP operation? The following functions are usually performed by a different individual or group:

- system analysis,
- application programming,
- acceptance testing,
- program change control,
- data control,
- source transaction origination,
- system software maintenance,
- computer files maintenance, and
- computer equipment operation.

[1] Further guidance is available in GAO's Evaluating Internal Controls in Computer-Based Systems, June 1981 (under revision).

System Design, Development, and Modification

Controls in this category are intended to insure that systems meet user needs, are developed economically, are thoroughly documented and tested, and contain appropriate internal controls. Review tasks might include the following questions.

Does the agency have a formal approach for system development?

Are users involved in the development of system requirements?

Do standards exist for documenting different ADP functions?

Is the system documentation current and does it include:

- functional requirements documents,
- data collection requirements,
- design characteristics of the systems and component subsystems,
- a user manual,
- a system operating manual,
- the strategy for testing the computer-based system including test procedures and evaluation criteria, and
- test analyses reports documenting test results and findings?

Are requests for modifications to existing programs documented and approved by appropriate management levels?

Security

These controls should provide assurances that computers and the data they contain are properly protected against theft, loss, unauthorized access, and natural disaster? Reviews might consider:

Is a periodic risk analysis performed and documented?

Have responsibilities for computer security been formally assigned?

Is access to the computer room controlled through use of some physical device (i.e., locked door, security badges, etc.)

Are two persons present in the computer room at all times?

Is the responsibility for storing magnetic data clearly documented?

Does the agency have an emergency disaster recovery plan?

Is the disaster recovery plan periodically tested?

Is computer software used to control access to the computer system by identifying and verifying people who try to gain access?

Application Controls

Controls which are incorporated directly into individual applications are intended to insure accurate and reliable processing. They address the three major operations of data input, data processing, and data output.

Data Input

Controls in this category are designed to insure that data is converted to an automated form and entered into the application in an accurate, complete, and timely manner. Review tasks might address the following questions.

Do documented procedures exist for entering data into the application?

Are controls in place which permit the number of records input to the application to be reconciled against the number presented for entry?

Do all source records contain some indication of authorization (either physical or electronic)?

Are security measures in place to limit access to input terminals and validate user sign-on?

Is data validation and editing performed on all data fields before entry into the system?

Are uses of methods to override or bypass data validation and editing procedures recorded and analyzed for appropriateness and correctness by supervisory personnel?

Do documented procedures exist that explain the process of identifying, correcting, and reprocessing data rejected by the application?

Is all data that does not meet edit requirements rejected from further processing and written to an automated suspense file?

Is the automated suspense file used to control follow-up, correction, and reentry of rejected data?

Is the automated suspense file regularly analyzed to determine the rate of data input error and the status of uncorrected records?

Are corrective actions taken when error rates become too high?

Are counts of rejected items produced and reconciled with accepted records to account for all input?

Data Processing

Processing controls are designed to insure that data is handled by the computer in an accurate, complete, and timely manner. Review tasks might include the following questions.

Do documented procedures exist to explain the methods for proper data processing of each application program?

Does a history log record events performed by the computer and its operators during application processing?

Are application programs secured against direct input from operator consoles?

Do on-line systems protect against concurrent file updates?

Are controls in place to prevent operators from circumventing file checking routines?

Are file completion checks performed to make sure that application files have been completely processed?

Do processing controls make sure that output counts from the system equal input counts to the system?

Is relationship editing performed between input transactions and master files to check for appropriateness and correctness before updating?

Data Output

Output controls are used to insure the integrity of system output and the correct and timely distribution of outputs. Review tasks could address the following questions.

Do documented procedures exist that explain the procedures for balancing, reconciling, and distributing output products?

Are users questioned periodically to determine their continued need for the product?

Is each output product labelled to identify the product name, recipient's name, and time and date of production?

Do documented procedures exist that explain methods for reporting, correcting, and reprocessing output products with errors?

Are input record counts and controls totals reconciled against output record counts and control totals to insure that no data was lost or added during processing?

Are system outputs reviewed for completeness and accuracy before release to users? Does this review include reconciling record counts and control totals?

Are source documents retained and stored in a logical sequence for easy retrieval?

Ordering Information

The first five copies of each GAO report are free. Additional copies are $2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary. Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

U.S. General Accounting Office
P.O. Box 6015
Gaithersburg, MD 20877

Orders may also be placed by calling (202) 275-6241.