

July 2009
External Version I

Assessing the Reliability of Computer-Processed Data



Contents

Preface		1
Section 1	Introduction	3
Section 2	Understanding Data Reliability	4
Section 3	Deciding Whether a Data Reliability Assessment Is Necessary	6
Section 4	Determining the Extent of the Assessment	9
Section 5	Planning a Data Reliability Assessment	13
Section 6	Steps in the Assessment	15
Section 7	Making the Data Reliability Determination	23
Section 8	Including Appropriate Language in the Report	29
Appendix I	Collecting Information for Reliability Assessments	31
Appendix II	Sample Interview Questions and Issues Related to Process and System Controls	35

Figures

Figure 1: Factors That Help Decide Whether to Use Data	3
Figure 2: Determining the Need for a Data Reliability Assessment	6
Figure 3: The Framework of the Data Reliability Assessment Process	12
Figure 4: Steps in Assessing Data Reliability	15
Figure 5: Making the Final Determination	24

Abbreviations

GAGAS	Generally accepted government auditing standards
GPRA	Government Performance and Results Act

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

Preface

Computer-processed data from outside sources are often central to audit reports. While these data are simply another type of evidence to rely on, assessing them may require more technical effort than other types. Computer-processed data, resulting from computer processing or entering data into a computer system, can vary in form. They may be data in electronic files or tables in published reports, including paper copies. (More specific examples are discussed in section 2.)

Intended to demystify the assessment of computer-processed data, this guide is consistent with the Yellow Book—the 2007 Government Auditing Standards—which defines generally accepted government auditing standards (GAGAS), and it replaces the 2002 *Assessing the Reliability of Computer-Processed Data*.¹

Various tests of sufficiency and appropriateness are used for all types of evidence to assess whether the evidence standard is met. Because assessing computer-processed data requires more technical tests, it may seem that such data are subject to a higher standard of testing than other evidence. This is not the case. For example, we apply many of the same tests of sufficiency and appropriateness that we apply to other types of evidence, but in assessing computer-processed data, we focus on one test in the evidence standard—appropriateness. Appropriateness includes validity and reliability, which in turn includes the completeness and accuracy of the data.

This guide therefore provides a flexible, risk-based framework for data reliability assessments that can be geared to the specific circumstances of each engagement. The framework gives structure to planning and reporting, facilitates the right mix of skills on each engagement, and ensures timely management acceptance of assessment strategies. The framework is built on

- making use of existing information about the data,
- conducting only the amount of work necessary to determine whether the data are reliable enough for your purposes,

¹Comptroller General of the United States, *Government Auditing Standards: July 2007 Revision*, [GAO-07-731G](#) (Washington, D.C.: Government Accountability Office, July 2007), and GAO, *Assessing the Reliability of Computer-Processed Data*, [GAO-03-273G](#) (Washington, D.C.: October 2002).

- maximizing professional judgment, and
- bringing the appropriate people, including management, to the table at key decision points.

The ultimate goal of data reliability assessment is to determine whether you can use the data for your intended purposes. This guide is designed to help you make an appropriate, defensible assessment in the most efficient manner. With any related questions, call Sidney Schwartz, the Director of the Center for Design, Methods, and Analysis in the Applied Research and Methods team, at (202) 512-7387.



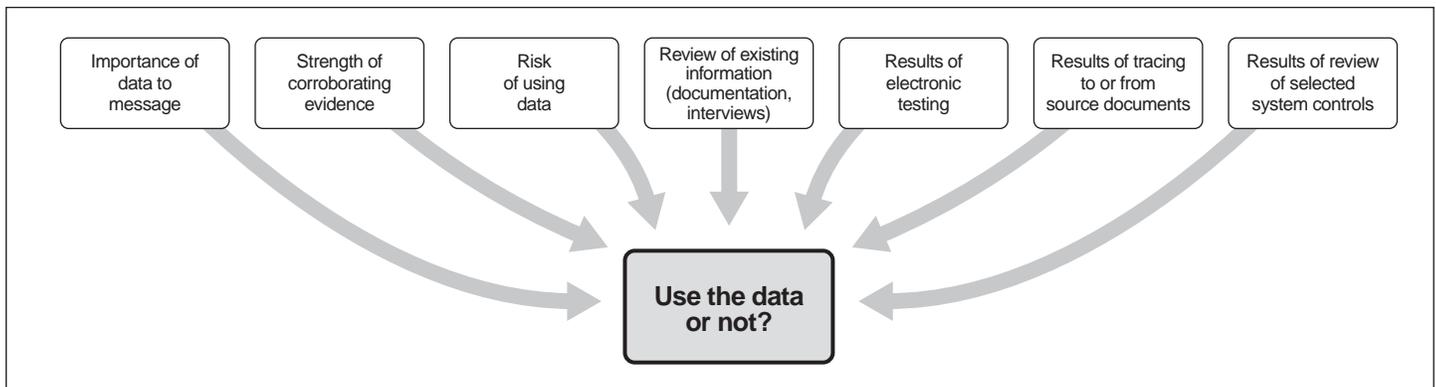
Nancy Kingsbury
Managing Director, Applied Research and Methods

Section 1: Introduction

This guide explains what data reliability means and provides a framework for assessing the reliability of computer-processed data. It includes guidance on determining when to do a data reliability assessment, factors contributing to the extent of the assessment, and suggestions for steps to take in conducting the assessment.

The ultimate goal of a data reliability assessment is to gather and evaluate the information needed to make the following decision: Can we use the data to answer the research question? Figure 1 gives an overview of the factors that help inform that decision. Not all the factors in the figure may be necessary for all research projects.

Figure 1: Factors That Help Decide Whether to Use Data



Source: GAO.

In addition, the guide suggests appropriate language for different circumstances in reporting the results of your assessment. Finally, it describes in detail all the stages of an assessment.

Section 2: Understanding Data Reliability

For the purposes of this guidance, data reliability refers to the accuracy and completeness of computer-processed data, given the uses they are intended for. Computer-processed data may be data (1) entered into a computer system or (2) resulting from computer processing. In this guide, “data” always means computer-processed data.

Computer-processed data can vary in form—from electronic files to tables in published reports. The definition of computer-processed data is therefore broad. Some specific examples of computer-processed data are

- data extracts from databases, data warehouses, or data repositories;
- data maintained in Microsoft Excel or Access or similar commercial products;
- data extracts from enterprise software applications supported by information technology departments or contractors;
- public use data or other replicated detail or summary-level databases accessible through an application other than the original source system;
- data collected from forms and surveys on Web portals; and
- data summarized in a report or copied from a table in a document.

While the focus here is on computer-processed data, some of the principles and assessment tasks also apply to other kinds of data.

This guide will help you design a data reliability assessment appropriate to your project’s purpose and then evaluate the results of the assessment. According to the Yellow Book, auditors should assess the sufficiency and appropriateness of computer-processed information, regardless of whether this information is provided to auditors or they extract it independently.¹ A data reliability assessment should be performed for computer-processed data that materially support findings, conclusions, or recommendations.

¹Comptroller General of the United States, *Government Auditing Standards*, section 7.23–27, pp. 134–37, and section 7.65, p. 151.

In this context, reliability means that data are reasonably complete and accurate, meet your intended purposes, and are not subject to inappropriate alteration.

- Completeness refers to the extent that relevant records are present and the fields in each record are populated appropriately.
- Accuracy refers to the extent that recorded data reflect the actual underlying information.
- Consistency, a subcategory of accuracy, refers to the need to obtain and use data that are clear and well defined enough to yield similar results in similar analyses. For example, if data are entered at multiple sites, inconsistent interpretation of data entry rules can lead to data that, taken as a whole, are unreliable.

While this guide focuses only on the reliability of data in terms of completeness and accuracy, other data quality considerations are just as important. In particular, consider validity. Validity (as used here) refers to whether the data actually represent what you think is being measured. For example, if we are interested in analyzing job performance and a field in the database is labeled “annual evaluation score,” we need to know whether that field seems like a reasonable way to gain information on a person’s job performance or whether it represents another kind of evaluation score.

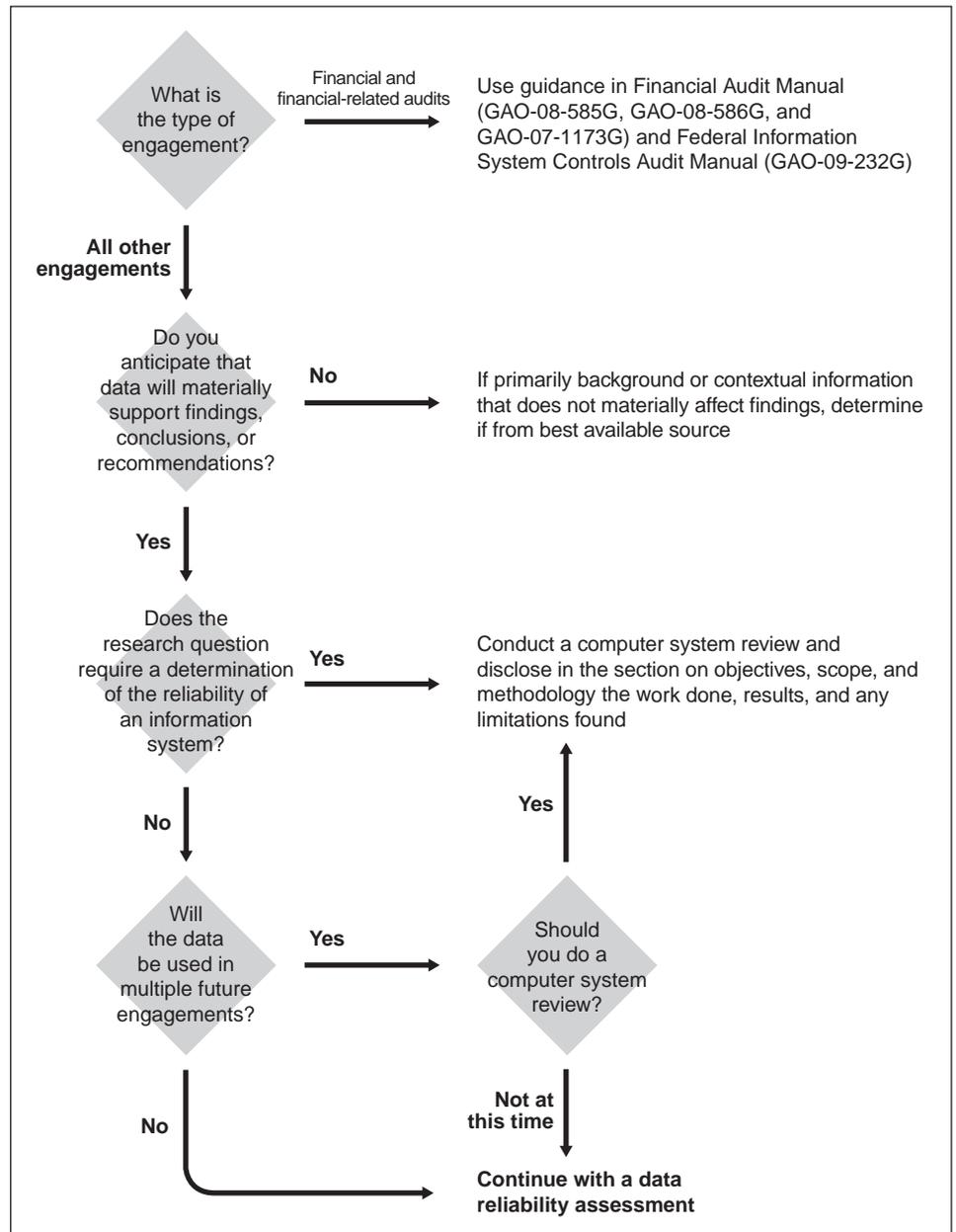
Consider data validity and reliability issues early on a job. Data analysts, methodologists, information technology specialists, statisticians, and other technical specialists can assist you.

Assessments of reliability are made in the broader context of the particular characteristics of your research project and the risk associated with the possibility of using insufficiently reliable data. A decision that computer-processed data are reliable does not necessarily mean that the data are error-free. Errors are considered acceptable in this circumstance: You have assessed the associated risk and conclude that the errors are not substantial enough to cause a reasonable person, aware of the errors, to doubt a finding, conclusion, or recommendation based on the data.

Section 3: Deciding Whether a Data Reliability Assessment Is Necessary

To decide whether a data reliability assessment is necessary, consider the planned use of the data. Figure 2 illustrates the decision process.

Figure 2: Determining the Need for a Data Reliability Assessment



Source: GAO.

Conditions Requiring Data Reliability Assessment

You should assess reliability if the data to be analyzed are intended to materially support your findings, conclusions, or recommendations. Keep in mind that a finding may include only a description of the condition, as in a purely descriptive report. Remember, too, that data can include record-level data, summary or aggregate data, and estimates or projections based on computer-processed data.

In your audit plan, you should discuss briefly how you plan to assess data reliability, as well as any limitations that may exist because of shortcomings in the data.

Conditions Not Requiring Data Reliability Assessment

You do not need to assess the reliability of data if their use in the report does not materially affect findings, conclusions, or recommendations. In most circumstances, information presented as background, context, or example does not require an assessment. For example, data not needing an assessment might simply set the stage for reporting the project's results or provide information that puts the results in proper context. Such information could be the size of the program or activity you are reviewing. While such data may not need an assessment, you should still ensure that they are from the best available sources.

For instance, a finding might include the number of uninsured Americans and you might want to put this number in the context of the overall U.S. population. While the estimate of the number of Americans who are uninsured would require a data reliability assessment of some kind, as long as the estimate of the U.S. population were determined to have come from a reliable source (for instance, the U.S. Census), this number would not require an assessment.

Sometimes data that seem like background information may materially affect the findings. If data in the report appear to provide context but also serve as an impetus for the audit or are likely to be subjected to a high degree of scrutiny, you should conduct an assessment. For example, if an estimate of the amount of dietary supplements Americans take is presented as a basis for conducting an audit of a regulatory agency, you should conduct a data reliability assessment to be reasonably confident of the estimate's accuracy.

In addition, if an audit relies on information that is used for widely accepted purposes and is obtained from sources generally recognized as appropriate, it may not be practical or necessary to conduct procedures to verify the information. Such information could include, for example,

economic statistics that government agencies issue for adjusting for inflation or other such information authoritative organizations issue. Deciding to use such information without further assessment calls for professional judgment by individuals with appropriate knowledge of the nature of the information and how it is being used in the audit (for example, technical specialists).

Finally, for financial audits, you should not follow this guidance in assessing data reliability. For financial audits, which include financial statements and financial-related audits, you should follow the *Financial Audit Manual and the Federal Information System Controls Audit Manual*.¹ In an information system review, all controls in a computer system—for the full range of application functions and products—are assessed and tested. This includes

1. examining the general and application controls of a computer system,²
2. testing whether those controls are being complied with, and
3. testing data produced by the system.³

Information technology specialists can help you design an appropriate information system review, given your research question, and connect you with the resources you need.

¹See GAO and President's Council on Integrity and Efficiency, *Financial Audit Manual*, vol. 1, [GAO-08-585G](#) (Washington, D.C.: July 2008), vol. 2, [GAO-08-586G](#) (Washington, D.C.: July 2008), and vol. 3, [GAO-07-1173G](#) (Washington, D.C.: Aug. 28, 2007), and GAO, *Federal Information System Controls Audit Manual*, [GAO-09-232G](#) (Washington, D.C.: February 2009).

²General controls refers to the structure, policies, and procedures—in all or a large segment of an organization's information systems—that help ensure proper operation, data integrity, and security. Application controls refers to the structure, policies, and procedures that apply to individual application systems, such as inventory or payroll.

³Guidance for reviewing general and application controls is in GAO, *Federal Information System Controls Audit Manual*.

Section 4: Determining the Extent of the Assessment

The ultimate goal of a data reliability assessment is to determine whether you can use the data to answer the research questions. Perform assessments only for the portions of the data that are relevant to the project. You may need to assess only a few elements of a database or you may need to assess many variables in various modules of a data collection system. The extent of an assessment depends on the

- expected importance of the data to the final report,
- strength or weakness of any corroborating evidence, and
- anticipated level of risk in using the data.

Expected Importance of the Data in the Final Report

In making an assessment, consider the data in the context of the final report:

- Will the project team depend on the data alone to answer a research question?

If the data are the sole source of information leading to findings and recommendations, a more extensive assessment may be necessary than if you have strong corroborating evidence.

- Will the data be summarized or will detailed information be reported?

Although the data elements underlying the summary data still need to be assessed, the presentation of more detailed information may require a deeper assessment. If you plan to report detailed information, then the assessment should focus on whether the data are reliable at the level you plan to report. For example, if you need to report only total dollars spent, you may have to do an assessment that does not go as deep as if you planned to report on expenditures in specific categories.

- Is it important to have precise data?

Do you need to do an assessment that allows you to report approximate data or do you need to do a more in-depth assessment that would allow you to report exact numbers? For example, when assessing the ability of charities to respond to a disaster, is it enough to know that resources will shelter a range of 400,000 to 500,000 people or do we need to know the exact figure?

Corroborating Evidence

Consider the extent to which corroborating evidence exists and will independently support the findings, conclusions, or recommendations. Corroborating evidence is independent evidence that supports information in a database or derived from one. Such evidence, if available, can be found in alternative databases or expert views. Corroborating evidence is unique to each review, and its strength—or persuasiveness—varies.

For help in deciding the strength or weakness of corroborating evidence, consider the extent to which the corroborating evidence is

- consistent with Yellow Book standards of evidence—sufficiency and appropriateness;
- able to provide crucial support;
- drawn from multiple sources;
- drawn from multiple types of evidence, such as testimonial, documentary, and physical; and
- independent of other sources.

Risk Level in Using the Data

Risk is the likelihood that using data of questionable reliability could have substantial negative consequences on the decisions of policymakers and others. To do a risk assessment, consider the following risk conditions, in which the data

- could be used to inform legislation, policy, or a program that could have substantial effect;
- could be used to inform important decisions by individuals or organizations with an interest in the subject;
- will be the basis for numbers that are likely to be widely quoted, as in the statement, The United States owes the United Nations about \$1.3 billion for the regular and peacekeeping budgets;
- are relevant to a sensitive or controversial subject;
- have been judged for their quality by experts or external stakeholders who have taken positions on the information.

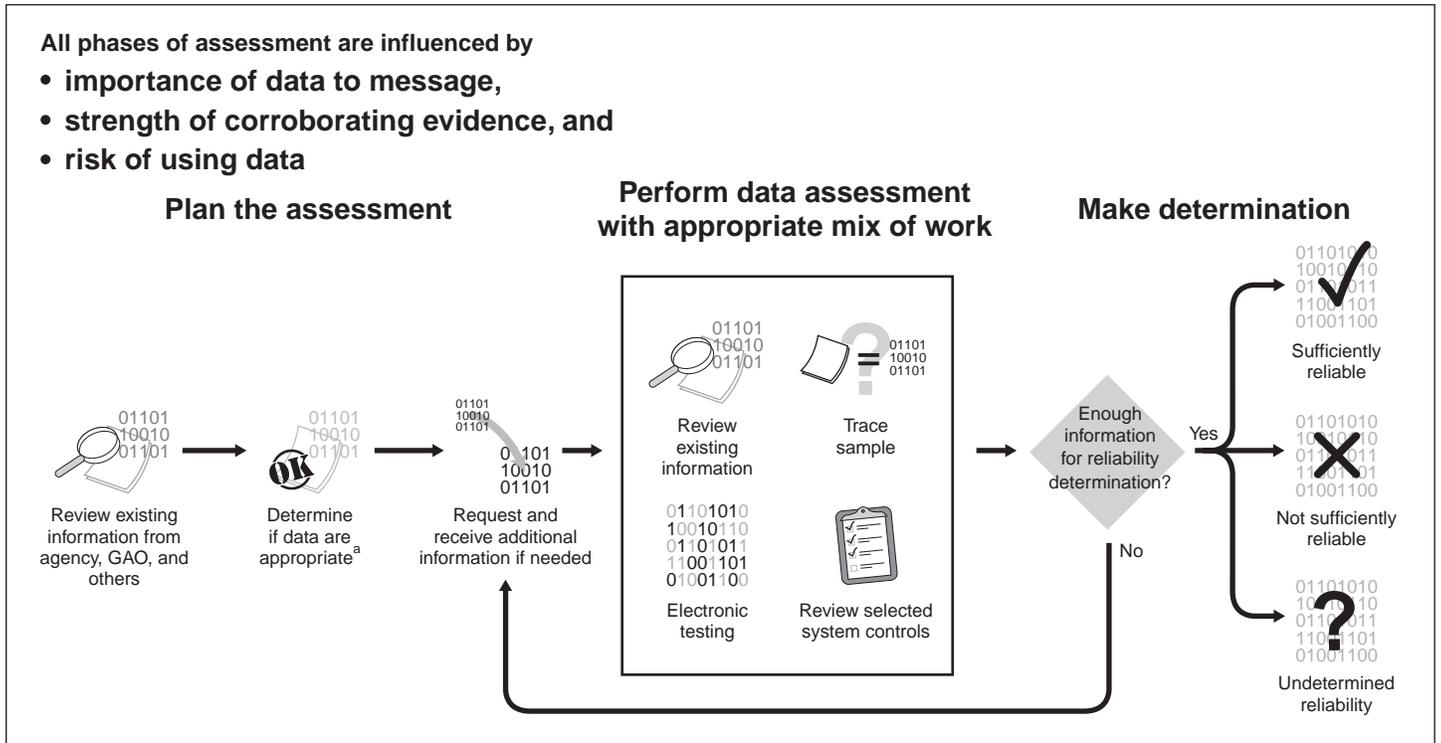
Bear in mind that any one condition may have more importance than another, depending on the project.

The assessment process should take these factors into account, along with what is learned during the assessment. The process is likely to differ from one job to another. However, it should include sufficient work to allow the auditor to have a good understanding of how the data were collected, the systems they were extracted from, and the process and system controls related to the key data elements. Technical specialists can help you consider these factors and plan your work.

Figure 3 illustrates the overall framework of the process for data reliability assessment. The framework identifies several key stages in the assessment, as well as actions to take and decisions to expect as you move through the process. The framework allows you to identify the appropriate mix of assessment steps to fit the particular needs of the job. In most cases, not all the elements in figure 3 would be necessary to complete the assessment. (Specific actions for each stage are discussed in sections 6 and 7.)

Section 4: Determining the Extent of the Assessment

Figure 3: The Framework of the Data Reliability Assessment Process



Source: GAO.

^aAfter a review of initial information, you may determine that the data are not appropriate for answering the research question (for example, the database may not contain relevant data elements).

Section 5: Planning a Data Reliability Assessment

When you plan a data reliability assessment, you need to decide on the timing—when to perform the assessment—and how to document your plans for the assessment and the assessment itself. In addition, important decisions about obtaining data at the summary or record levels of detail will affect how you can use the data in the report and the depth of your data reliability assessment.

Timing an Assessment

Generally, a data reliability assessment is performed as early as possible on a project, preferably during the design phase. The audit plan helps by reflecting data reliability issues and any additional steps that still need to be taken in assessing the reliability of critical data. The audit team generally takes initial steps to test the data and review existing information about the data and the system that produces them before making the audit plan final. Examining this information early is also necessary to help the team determine whether the data would be appropriate for addressing the research question in the first place.

In some instances, the timing of the project may be very short. Section 6 has some suggestions for meeting data reliability assessment requirements in a short period of time.

Level of Detail of the Data

Record-level data give the greatest opportunity to analyze the data and fully assess their reliability. This opportunity may be most important for data that are key to your research objectives. Summary-level data or a subset of data still require a data reliability assessment, but testing and understanding of the data may be more limited. It will also be important to understand any process used for summarizing or extracting the data; you may need to request the computer code or queries used to derive the data. Obtaining the code used to derive the records allows you a greater ability to see whether the correct criteria were used in providing you with the records, decreasing the chance of missing records. In general, it is preferable to obtain record-level data because they permit a more comprehensive data reliability assessment.

For example, auditors might be reviewing the timeliness of agency decisions. If you obtained the detailed data for all decisions, you might be able to report timeliness data at the national, regional, and field office levels. In addition, with this record-level data, you could check their reliability to see if important information was missing or whether duplicate records were in the file. You could also determine, if you were given beginning and ending dates, whether the agency was calculating

timeliness accurately. The record-level data request could give you more reporting flexibility, more opportunities to find data problems which could lead to a recommendation, and a greater ability to use the data in the findings. A request for only national, summary-level data would not allow you to report data at the regional and field office levels, might not allow you to fully test data reliability, and depending on the intended use of the data, could preclude using the data in the findings section of the report.

Documenting the Assessment

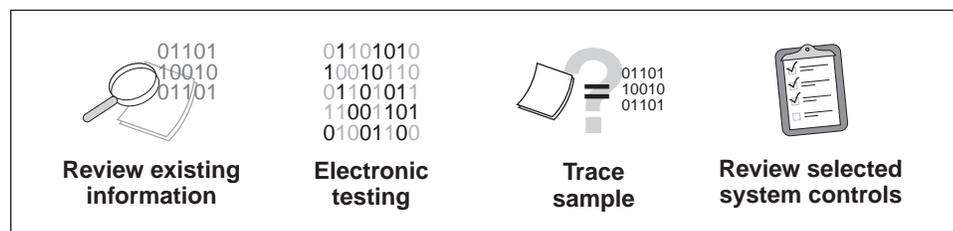
All work performed as part of the data reliability assessment should be documented and included in the project's documentation. Required documentation includes a plan for steps you will take in the assessment, as well as the results from all testing, documentation review, and interviews related to data reliability.

In addition, decisions made during the assessment, including the final determination of whether the data are sufficiently reliable for the overall purposes of the review, should be summarized in the documentation. The documentation should make clear what steps the project team took and what conclusions they reached.

Section 6: Steps in the Assessment

Data reliability as a process includes a range of possible steps, as shown in figure 4. Assessing data reliability can entail reviewing existing information about the data, including conducting interviews with officials from the organization being audited; performing tests on the data, including advanced electronic analysis; tracing to and from source documents; and reviewing selected system controls.

Figure 4: Steps in Assessing Data Reliability



Source: GAO.

Deciding which steps to take is an iterative process. Most often you may start with the relatively simple steps of reviewing existing information and basic testing. The outcome of these steps may lead you to take other steps in order to gather enough information.

The mix of steps you take depends on any potential weaknesses you identify as you proceed and circumstances specific to the job, such as the importance of the data to the review and corroborating evidence. Focus particularly on the aspects of the data that pose the greatest potential risk, especially for the more labor-intensive activities. Some audits may take an extremely short time to complete; this section provides some advice for this situation.

As discussed in section 5, these steps take place early in the project and include the audit team members, as well as appropriate technical staff. The time and extent needed to take any of or all these steps will depend on the project and the amount of risk involved.

Reviewing Existing Information

A review of existing information helps you determine what is already known about the data and the computer processing. The related information you collect can indicate both the accuracy and completeness of the entry and processing of the data, as well as how data integrity is maintained. This information can be in the form of reports, studies, or interviews with individuals who are knowledgeable about the data and the

system. Sources for related information include the U.S. Government Accountability Office (GAO), the agency under review, and others.

GAO

GAO may already have related information in its reports available at www.gao.gov. Consider whether information in any relevant GAO report is timely and appropriate for your uses.

GAO's Web site also provides other useful information. For example, in conducting the annual governmentwide consolidated financial audit, GAO's Information Technology team has been involved in reporting on the effectiveness of controls for financial information systems at major federal agencies, and relevant reports may be found on the site.

Agency under Review

Another source of information is the organization being reviewed. You can obtain documentation about a system, such as users' manuals, data dictionaries, system documentation, table layouts, codebooks, and data quality assurance program materials. You can also ask officials questions about their system and how it is used. You can often learn initial information about data and data reliability by interviewing agency officials and computer system specialists.

Ideally, as you engage in a project, interviews take place early. You can often identify potential reliability issues with the data in the initial steps of the assessment from interview questions, before you have done further assessment work. Interviewing agency officials early about how appropriate the data are for your research questions can help you make decisions as you plan further work to assess the reliability of the data. Interview questions focus on the completeness and accuracy of the data and the internal controls surrounding the information system that produces the data. Use what you know about the program under review and the computer system to focus interview questions on the specific issues that most directly affect the reliability of the data you plan to use in the audit.

In addition, agency officials are often aware of evaluations of their computer data or systems and usually can direct you to them. However, keep in mind that information from agency officials may be biased. Consider asking appropriate technical specialists to help in evaluating this information. (Appendixes I and II have sample questions on document requests, accuracy and completeness concerns, and process and system control issues.)

Agency information also includes reports under the Federal Managers' Financial Integrity Act and the Clinger-Cohen Act, Government Performance and Results Act (GPRA) plans and reports, and Chief Information Officer and Inspector General reports.¹ Some of this information can be found in agency home pages on the Web.

Other Sources

Other sources include organizations and data users, as well as libraries of relevant literature. To help you identify them, you can use a variety of databases and other research tools that include the Congressional Research Service Public Policy Literature Abstracts and other organizations' Web sites. Additionally, agency officials may be able to identify outside users of their data.

Statistics collected and published by federal government statistical agencies constitute a significant portion of the available information about the U.S. economy, population, natural resources, environment, and public and private institutions. Standards and guidelines governing federal statistical agencies are intended to ensure that their surveys and studies are designed to produce reliable data as efficiently as possible and that their methods are documented and results presented in a manner that makes the data as accessible and useful as possible. In most cases, federal statistical agencies have information on their statistical collection procedures and methods readily available on the Internet. Often, this published information serves as much of the documentation you will need to review in conducting your data reliability assessment.

Although data that federal statistical agencies collect are generally reliable for their purposes, you must still assess whether these data are sufficiently reliable for your purpose. For example, census data indicate how many natural-born children are living with respondents, but these data are not reliable for determining how many natural-born children a respondent has ever had, because some children might be living independently or with other relatives or living in college or the military.

¹See Federal Managers' Financial Integrity Act of 1982, Pub. L. 97-255, Sept. 8, 1982, 96 Stat. 814, 31 U.S.C. § 3512; Clinger-Cohen Act of 1996, Pub. L. 104-106, divs. D, E, Feb. 10, 1996, 110 Stat. 642, 679, 40 U.S.C. § 1401 et seq.; Government Performance and Results Act of 1993, Pub. L. 103-62, Aug. 3, 1993, 107 Stat. 285, 31 U.S.C. § 1101; and Federal Information Security Management Act of 2002, 44 U.S.C. § 3541 et seq.

It is also possible to inappropriately use otherwise reliable federal statistical data. For example, an audit team might want to determine from Current Population Survey data the proportion of law enforcement officers who are Asian. Because this information is at the intersection of two separate subpopulations—race and occupation—the number of people will be too small to be reliable because of the sampling design used to collect these data. Consider these kinds of data reliability issues when planning to use federal statistical agency data.

Performing Data Testing

Data testing can be done by applying logical tests to electronic data files or paper copies of reports. For record-level electronic data, you can use computer programs to test all entries of key data elements in an entire data file.² Keep in mind that you test only the data elements you plan to use in your review.

For paper copy or summarized data—provided by the agency or retrieved from the Internet—ask for the electronic data file that was used to create them. If you are unable to obtain electronic data, use the paper copy or summarized data and, to the extent possible, manually apply the tests to all instances of key data elements or, if the report or summary is voluminous, to a sample of them.

Whether you have an electronic data file or a paper copy report or summary, you can apply the same types of tests to the data. The tests you conduct will vary for each assessment and can include

- checking total number of records provided against agency totals;
- testing for missing data, either entire missing records or missing values in key data elements;
- looking for duplicate records;
- looking for invalid or duplicate identifiers;

²An in-depth discussion of quality assurance practices to be used in electronic testing and analyses is beyond the scope of this guide. It is nonetheless important to perform appropriate checks to ensure that you have obtained the correct file. All too often, auditors receive an incorrect file (an early version or an incomplete file). Appropriate steps include counting records and comparing totals with the responsible agency or source.

- testing for values outside a designated range;
- looking for dates outside valid time periods or in an illogical progression;
- following up on troubling aspects of the data—such as extremely high values associated with a certain geographic location—found while analyzing the data;
- testing relationships between data elements (sometimes by merely doing a cross tabulation), such as whether data elements follow a skip pattern from a questionnaire; and
- verifying that computer processing is accurate and complete, such as testing a formula used in generating specific data elements, or testing to ensure that edit checks are working correctly.

Depending on what will be tested, this testing can require a range of programming skills—from creating cross tabulations on related data elements to duplicating an intricate automated process with more advanced programming techniques. Consider asking appropriate technical specialists to help in conducting this testing.

Be sure to keep a log of your testing to include in the project's documentation.

Tracing to and from Source Documents

When record-level data are available, tracing a sample of data records to source documents helps you determine whether the computer data accurately and completely reflect these documents. In deciding what and how to trace, consider the relative risks of overstating or understating conclusions drawn from the data. For example, if you are particularly concerned that questionable cases might not have been entered into the computer system and that, as a result, the degree of compliance may be overstated, consider tracing from source documents to the database. However, if you are more concerned that ineligible cases have been included in the database and that, as a result, the potential problems may be understated, consider tracing from the database back to source documents.

The reason to trace only a sample is that sampling saves time and cost. To be useful, however, the sample should be random and large enough to estimate the error rate within reasonable levels of precision. Tracing an

appropriate random sample can allow you to estimate the error rate and the magnitude of errors for the entire data file. It is this error rate that helps you determine the data reliability. (Consult statisticians to help you select the sampling method most suited to your project.)

Generally, every data file has some degree of error—here, example 1 shows error rate, example 2 magnitude of errors:

Example 1. In a random sample, 10 percent of the data records have incorrect dates, and those dates are off by an average of 3 days. Depending on what the data are used for, 3 days may not compromise reliability.

Example 2. The value of a data element was incorrectly entered as \$100,000 rather than \$1,000,000. The documentation of the database showed that the acceptable range for this data element was between \$100 and \$5,000,000. Therefore, the electronic testing would have confirmed that the value of \$100,000 fell within that range. In this case, the error could be caught not by electronic testing but only by tracing the data to source documents.

Tracing to Source Documents

Consider tracing to source documents when (1) they are available relatively easily or (2) the possible magnitude of error is especially critical.

To trace a sample to source documents, match the entered data with the corresponding data in the source documents. In attempting to trace entered data back to source documents, several problems can arise. Source documents may not be available because they were destroyed, were never created, or are not centrally located.

Several options are possible if source documents are not available. For documents that were never created—for example, when data may be based on electronic submissions—use interviews to obtain related information, any corroborating evidence obtained earlier, or a review of the adequacy of system controls.

Tracing from Source Documents

Consider tracing from source documents instead of, or in addition to, tracing a sample to source documents when you have concerns that the data are not complete. To trace a sample from source documents, match the source documents with the entered data. Such tracing may be appropriate to determine whether all data are completely entered.

However, if source documents were never created or are now missing, you cannot identify the missing data.

Reviewing Selected System Controls

Your review of selected system controls—the underlying structures and processes of the computer where data are maintained—can provide some assurance that the data are sufficiently reliable. Examples of system controls are limits on access to the system and edit checks on data entered into the system.³ Controls can reduce to an acceptable level the risk that a significant mistake could occur and remain undetected and uncorrected. Limit the review to evaluating the specific controls that can most directly affect the reliability of the data in question.

Choose areas for review on the basis of what is known about the system. Sometimes you identify potential system control problems in the first steps of the assessment. Other times, you may learn that source documents are not readily available. Therefore, a review of selected system controls is a good way to determine whether data were entered reliably. If needed, consult information system auditors or other technical specialists for help in evaluating system controls.

Using what you know about the system, concentrate on evaluating the controls that most directly affect the data. These controls will usually include (1) certain general controls, such as logical access and control of changes to the data, and (2) the application controls that help ensure that the data are accurate and complete, as well as authorized.

The steps for reviewing selected system controls are

- gain a detailed understanding of the system as it relates to the data and
- identify and assess the application and general controls that are critical to ensuring the reliability of the data required for the audit.

³For more information about system controls, and how specific controls contribute to internal control and the reliability of computer processed data, see GAO, *Standards for Internal Control in the Federal Government*, [GAO/AIMD-00-21.3.1](#) (Washington, D.C.: November 1999), and *Internal Control Management and Evaluation Tool*, [GAO-01-1008G](#) (Washington, D.C.: August 2001).

Working within Short Time Periods

In some instances, a project may have a time period that is very short. Despite this, you may have time to review existing information and test data that are critical for answering a research question. For example, you can question knowledgeable agency staff about data reliability or review GAO or Inspector General reports to quickly gather information about data reliability issues.

In addition, critical data elements can generally be tested electronically for obvious errors of completeness and accuracy in a short time on all but the most complicated or immense files. From that review and testing, you will be able to make a more informed determination about whether the data are sufficiently reliable to use for the purpose of your review and to decide whether further investigation is needed.

Section 7: Making the Data Reliability Determination

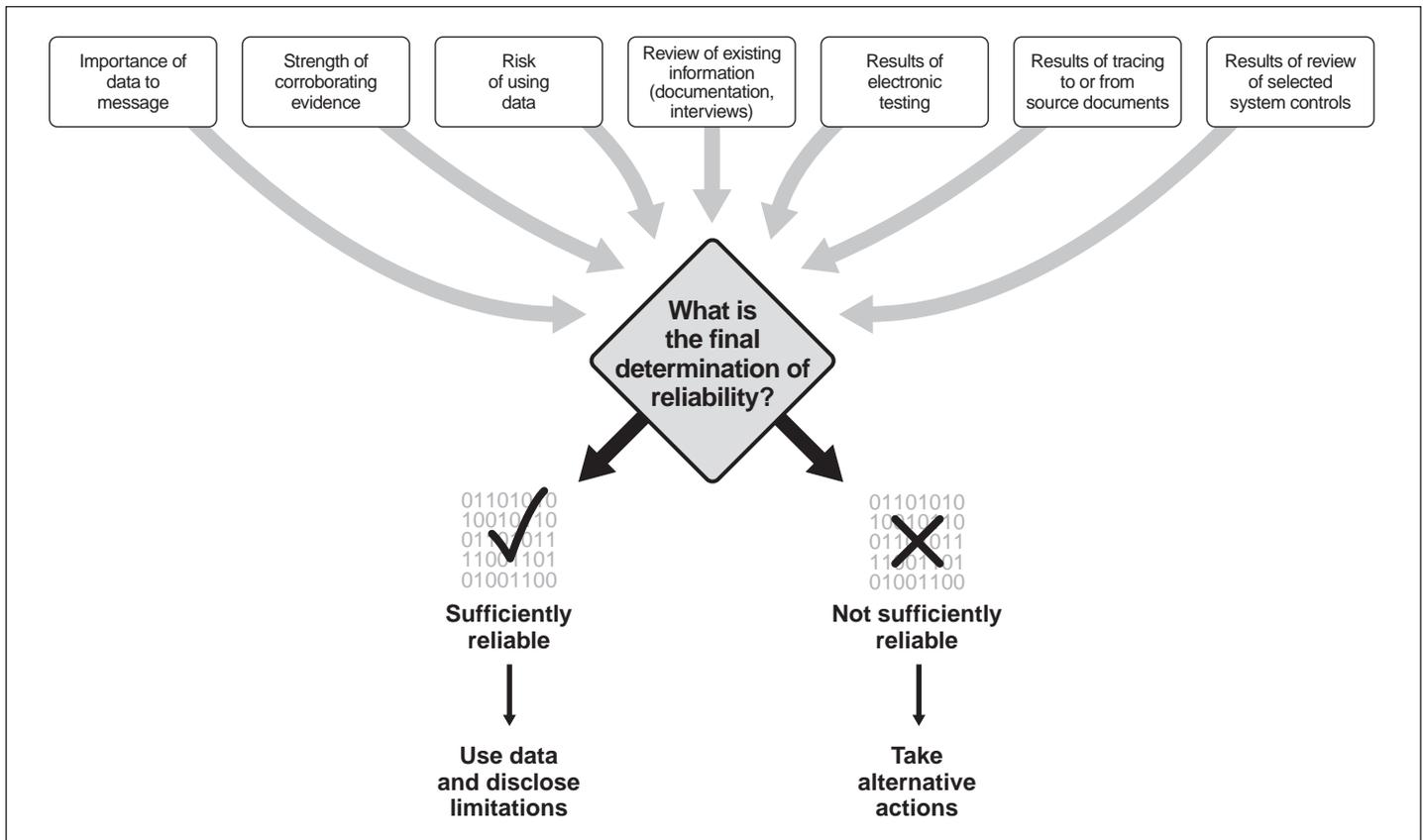
Review the results of your work periodically and decide whether (1) the data are sufficiently reliable for your job's purpose, (2) the data are not reliable for that purpose, or (3) additional work is needed before a determination can be reached. Keep in mind that you are not attesting to the overall reliability of the data or database. You are determining only the reliability of the data as needed to support the review's findings, conclusions, or recommendations. As you gather information and make your judgments, consult appropriate technical specialists for assistance.

Factors to Consider in the Determination

To determine whether the data reliability for the engagement is sufficient, consider all factors related to aspects of your engagement as well as assessment work performed to this point. As shown in figure 5 (and discussed in section 4), these factors include

- the expected importance of the data in the final report,
- corroborating evidence,
- level of risk of using the data, and
- the results of assessment work conducted so far.

Figure 5: Making the Final Determination



Source: GAO.

Considering the Results of Your Assessment Work

Before making a decision about the reliability of the data for your purposes, consider the results of all the steps you took in conducting the assessment. Appropriately document and review the results before entering into the decision-making phase of the assessment, because these results will, wholly or in part, provide the evidence that the data are sufficiently reliable—and therefore appropriate enough—or not sufficiently reliable for the purposes of your audit engagement. Remember that you may decide that you need to take further steps to come to a conclusion about the reliability of the data for your purposes.

Outcomes to Consider in the Assessment

The strength of corroborating evidence and the degree of risk can suggest different data reliability decisions. If the corroborating evidence is strong and the risk is low, the data are more likely to be considered sufficiently

reliable for your purposes. If the corroborating evidence is weak and the risk is high, the data are more likely to be considered not sufficiently reliable. If data testing did not raise any questions and answered all issues in the review of existing documentation, then the data are more likely to be considered sufficiently reliable for your purposes.

The overall determination is a professional judgment that the project team makes in discussions with team management and technical specialists.

The determination categorizes the data as sufficiently reliable, not sufficiently reliable, or of undetermined reliability. Each category has implications with respect to whether you need to take further steps in the assessment and whether you can use the data for your intended purposes.

Sufficiently Reliable Data

You can consider the data sufficiently reliable when you conclude the following: The results of your work (including testing results and reviews of existing information) provide assurance that (1) the likelihood of significant errors or incompleteness is minimal and (2) the use of the data would not lead to an incorrect or unintentional message. You could have some problems or uncertainties about the data, but they would be minor, given the research questions and intended use of the data.

In certain cases, after collaboration with the producers of the data, you may be able to make corrections that make the data sufficiently reliable for your purposes. You may also be able to alter your research question or planned use of the data to take into account any data limitations discovered. When your final determination indicates that the data are sufficiently reliable, use the data.

Not Sufficiently Reliable Data

You can consider the data to be not sufficiently reliable when you conclude the following: The results of your work indicate (1) significant errors or incompleteness in some of or all the key data elements and (2) that using the data would probably lead to an incorrect or unintentional message, given the research questions and intended use of the data.

When the determination indicates that the data are not sufficiently reliable, consider seeking evidence from other sources, including alternative computerized data—the reliability of which would also be assessed—or original data in other forms, such as surveys, case studies, or expert interviews.

Coordinate with the requester if your attempts to seek reliable evidence from other sources are unsuccessful. Inform the requester that such data, necessary in order to respond to the request, are unavailable. Reach an agreement with the requester to

- redefine the research questions to eliminate the need to use the data,
- use the data with appropriate disclaimers, or
- end the engagement.

Remember that you and your audit team are responsible for deciding what data to use. Although the requester may want information based on insufficiently reliable data, you are responsible for ensuring that data are used appropriately to respond to the requester. If you decide you must report data that you have determined are not sufficiently reliable for the engagement's purpose, make the limitations of the data clear, so that incorrect or unintentional conclusions will not be drawn. Consult with appropriate management on your project before you agree to use data that are not sufficiently reliable.

Sometimes, when conducting data reliability work, you encounter issues that might lead you to consider recommending changes to the data or data system. Consider further investigating data reliability issues where there is a strong likelihood that the data problems you have found could (1) materially change publicly disseminated agency information; (2) materially change organizational decisions where the organization uses these data; (3) materially misrepresent an agency's program or an organization's operational inputs, clients, or outcomes; (4) call into question whether the entity was in compliance with federal laws or regulations; or (5) undermine internal controls over high-risk operations or financial resources.

However, if the data reliability issues are the result of the auditor's attempting to use the data for purposes other than those the organization uses them for and if they do not result in issues outlined above, then recommendations might not be warranted, unless the auditor can make a strong case that the data should be sufficiently reliable for the use the auditor intended. A strong case might be that these data are essential to document a condition critical to effective decisions or operations where an agency is not currently using these data.

When the types of data reliability issues described above exist, consider making a recommendation that addresses the data problems or issuing a management letter to the audited organization. A management letter addresses management or operational issues that were found but that are beyond the substance of the audit.

Data of Undetermined Reliability

In your assessment of work performed so far, you may be unable to determine whether or not the data are sufficiently reliable. For example, the review of some information or testing may have raised questions about the data's reliability, or the work has provided too little information to judge reliability. In these cases, you may need to do additional work to determine reliability. If you are unable to perform additional work, the data are of undetermined reliability.

You can consider the data to be of undetermined reliability if specific factors are present—such as limited access to the data source, a wide range of data that cannot be examined with current resources, data limitations that prevent an adequate assessment, short time periods, the deletion of original computer files, or a lack of access to needed documents.

For example, you may have limited or no access to information about the data source. This is particularly likely when international agencies, other countries, or private organizations produce data or when there are privacy concerns with the data. It can occur where there is no audit authority to ask for more information or when insufficient information exists in the form of source documents or documentation about the data. In such cases, an attempt is made to gather as much information as possible, by contacting data owners or users or by looking for corroborating evidence, before concluding that the data are of undetermined reliability. Finding sufficient corroborating evidence, for example, may enable you to determine that the data are reliable enough for your purposes.

Alternatively, a wide range of data may have been gathered that is impossible to examine, such as in a survey of 50 state organizations asking for data that may have been collected differently within each state. You might then try to determine the overall reliability of the information, but may have insufficient resources to examine it all.

Finally, you may have conducted a data reliability assessment and still be unable to determine whether the data are sufficiently reliable, because data limitations prevented you from doing this. For example, you might

have found that financial data of interest are self-reported by other countries, affected by differences in exchange rates, and based on varying definitions. These limitations and lack of further access to the countries might prevent you from determining the reliability of the data.

To minimize last-minute crises, address data reliability issues in the planning phase of engagements, set realistic deadlines, and be prepared to ask for more time to assess data if it arrives later than expected. Inadequate planning earlier in the engagement is not a sufficient reason to use data of undetermined reliability, particularly if the data are being used as key evidence. Even though you may sometimes work within extremely tight time periods or may have received data or supporting documentation very late in an engagement, you will not want to use data that can lead to an incorrect message. GAO follows this principle, for example, to help ensure that GAGAS is met.

As noted with regard to insufficiently reliable data, when you decide that the data are of undetermined reliability, inform the audit's requester that sufficiently reliable data needed to respond to the request are unavailable. Remember that you and your audit team are responsible for deciding what data to use. Although the requester may want information based on data of undetermined reliability, you are responsible for ensuring that appropriate data are used. Consult with appropriate team management before you agree to use data of undetermined reliability. If you decide to use such data, clearly state their limitations, so that incorrect or unintentional conclusions will not be drawn.

Section 8: Including Appropriate Language in the Report

You should include in the report's methodology section a statement about having conformed to generally accepted government auditing standards. These standards include the appropriateness of the data being used. You conform to GAGAS by discussing in the report what you did to assess the data, disclose any data concerns, and make a judgment about the reliability of the data used in the report.

Further, in the methodology section, discuss your assessment of data reliability and the basis for your determination. The language in this discussion will depend on whether the data are sufficiently reliable, not sufficiently reliable, or of undetermined reliability. You may need to discuss the reliability of the data in other sections of the report as well. Whether you do so depends on how important the data are to the message. (Appendix III has samples of reporting language.)

Sufficiently Reliable Data

Present your basis for determining that the data are sufficiently reliable, given the research questions and intended use of the data. This presentation includes (1) noting the kind of assessment you relied on, (2) explaining the steps in the assessment, (3) describing any corrections made to the data, and (4) disclosing any data limitations. Such disclosure of limitations includes

- telling why using the data would not lead to an incorrect or unintentional message,
- explaining how limitations could affect any expansion of the message, and
- pointing out that any data limitations are minor in the context of the engagement.

Not Sufficiently Reliable Data

Present your basis for determining that the data are not sufficiently reliable, given the research questions and intended data use. This presentation should include the kind of assessment you relied on and explain the steps in the assessment. In this explanation, (1) describe the problems with the data, as well as why using them would probably lead to an incorrect or unintentional message, and (2) state that the data problems are significant or potentially significant. In addition, if the report contains a conclusion or recommendation supported by evidence other than these data, state this fact. Finally, if the data you assessed are not sufficiently reliable, consider whether to include this finding in the report and

recommend that the audited organization take corrective action (section 7 discusses factors to consider).

Data of Undetermined Reliability

Present your basis for assessing that the data are of undetermined reliability. Include such factors as the deletion of original computer files, data limitations that prevent an adequate assessment, short time periods, and the lack of access to the data source or to needed documents. Explain the reasonableness of using the data—for example, the data are supported by credible corroborating evidence, are widely used by outside experts or policymakers, or are used to present a general indication and not to support specific findings.

In addition, make the limitations of the data clear, so that incorrect or unintentional conclusions will not be drawn from them. For example, indicate how using these data could lead to an incorrect or unintentional message. Finally, if the report contains a conclusion or recommendation supported by evidence other than these data, state this.

Appendix I: Collecting Information for Reliability Assessments

This appendix suggests ways to help you think about questions related to data reliability assessments. It includes sample documentation requests and interview questions. Using your own judgment, select or modify items according to the relevance to your research objectives. Not all items will apply in every case; focus on the specific data elements that you will be using.

Data reliability assessment is often iterative, requiring some revisiting of issues as they arise in interviews, electronic testing, and data analysis. Once you have obtained the data, you may see unexpected elements or characteristics (for instance, a date or text entries in a numeric field). In such cases, it may be necessary to contact the source again.

It may be helpful to obtain documentation about the data if it is available, whether from a large and complicated system or a simple spreadsheet, and to review it before questioning individuals responsible for and familiar with the data. Established systems are likely to have many processes documented. Some documentation may be available on the Internet.

When information is not available beforehand, it can be requested in an interview. However, reviewing the documentation may require follow-up interviews to resolve questions brought up during document review.

Relevant documentation to request could include:

- information on a system's purpose and structure, such as user manuals, system flow charts, or design specifications;
- information on data elements (or fields) in the system, their definitions, descriptions, codes, and values (as in a data dictionary);
- financial statement audit reports, if data are used in the entity's financial statements;
- the survey form used to collect the data, if applicable;
- reviews of the quality of the data, including
 - Inspector General or internal audit reports,
 - internal reviews and studies,

- contractor or consultant studies,
- reports of congressional hearings or copies of congressional testimony related to the data, and
- summaries of ongoing or planned audits, reviews, or studies of the system or data.

Consider asking officials in an interview or written request some of the following questions if they are relevant and cannot be obtained from documentation you may have reviewed:

- When was the system created, and what is its purpose?
- How does the organization use the data from the system?
- Who are its primary users? How do users access the system?
- How and where are data collected? Who is responsible for data entry?
- How current are the data? How frequently are data entered?
- Who has access to enter or update information in the database?
- What procedures ensure that the data system consistently captures all data occurrences (records, observations) and all data elements? Is there written documentation of these procedures?
- Does the system have any edit checks or controls to help ensure that the data are entered accurately? For instance,
 - Does someone review at least a sample of data entries to ensure that key fields are accurate, nonduplicative, and sensible? (For example, the date an injury claim was filed should precede the date of adjudication.) If so, how often?
 - Are there electronic safeguards, such as error messages for out-of-range entries or inconsistent entries?
 - What are the procedures for follow-up if errors are found, and who is responsible for correcting them?

- Do systematic reviews or exception reports examine accuracy and present error rates? How frequently?
- Have there been changes to any of these procedures (including how a data element is defined, entered, or maintained) over the period of time for which you are requesting data?
- Has the system had problems that would affect the quality of the data, such as system crashes during which data were lost?

To assess the reliability of the data for your purposes, it may be useful to discuss with agency officials or other users of the data, such as academic researchers, how you intend to use the data. In that discussion, consider asking the following questions:

- What is your opinion of the quality of the data, specifically their completeness and accuracy? Are there any data limitations such as data elements that are often incomplete or incorrect?
- How would any limitations affect the intended use of the data?
- Are there concerns about timeliness or usability?
- Are there any purposes for which the data should not be used?
- What steps have others taken to clean or otherwise improve the data in order to conduct an analysis (for example, imputation of missing fields, weighting)?
- Is the organization taking any action to correct problems?

In asking these questions, you are looking for information on known limitations of the data. You are not looking for confirmation that the data are reliable. You must use your judgment to make the assessment.

You may be using data from statistical databases or data derived from samples or surveys, such as the Current Population Survey. If so, you may also need information on the following (which, for established systems, may be publicly available from the source):

- population definition;
- sample design;
- description of data editing procedures, including imputation, if used;
- impact of imputation;
- unit and item nonresponse rates;
- nonsampling error;
- comparability with related data, if any;
- information on limitations obtained from users, not producers, if applicable.

In developing your interview questions or information request, incorporate the questions or documents from above that are relevant for your assessment. You can start an interview or information request with language like the following, specifying the purpose of the request and data to be used:

We are conducting a review of _____. In this review, we plan to use data from your agency's ____ database or ____ program. We are following government auditing standards which require that we assess the reliability of data we use in our products. Therefore, we would like to ask you questions about the completeness and accuracy of the data and the information system that produces the data. The data fields we are interested in using are _____ for the purpose of _____.

Appendix II: Sample Interview Questions and Issues Related to Process and System Controls

Your detailed understanding and review of selected process and system controls can help ensure that the data are sufficiently reliable. Process controls refer to an organization's policies and procedures that could affect the accuracy and completeness of data. System controls refer to the underlying structures and programming of the computer system that could affect the accuracy and completeness of data. Process and system controls differ but often interact. Both should be considered the internal controls surrounding the organization's input and use of data.

Process and system controls can reduce to an acceptable level the risk that significant data mistakes could occur and remain undetected and uncorrected. You can often identify potential process and system control problems in an assessment's initial steps through interview questions aimed at program officials and computer system specialists. The issues and questions below provide some additional guidance on developing interview questions as they relate to system and process controls.

Interviewing an agency's officials about process and system controls can help you make decisions about whether you need to plan further work to assess the reliability of the data. Use what you know about the program under review and the computer system to focus interview questions on the specific process and system controls that most directly affect the reliability of the data you plan to use.

Process Controls

Process controls that could affect the accuracy and completeness of data include, among others, training, case control, guidance, incentive structure, interaction with stakeholders, management reviews, and system changes.

Training

Is data system training made available to users entering data into the system? What is the quality of the data system training? How is the training implemented—for example, do all new users have to go through the training? Is refresher training made available?

Case Control

Are procedures in place to ensure that all cases are entered into a data system? Can a case or transaction be processed without being entered into the data system? Can a case move to the next step of a process without

having been entered into the data system? Are procedures in place to prevent the duplicate recording of the same record?

Guidance

Does the agency or organization provide clear guidance for data entry in grey areas? For example, if a case could be accurately described in more than one way, is there guidance on how the case should be categorized when entered into the data system?

Incentive Structure

How does measuring employee or agency performance affect the quality of data entered into the system? For example, if employees are measured on the timeliness of case processing, could they enter incorrect dates into the system, indicating that cases were completed in a timely manner when in fact they were not?

Interaction with Stakeholders

Do users of the data or individuals whose programs are the subject of data records receive periodic updates regarding data in the system? Do these users or stakeholders have a chance to bring attention to incorrect data or data that need to be updated?

Interaction with stakeholders can help make sure that the people most likely to have knowledge of the correct data can work to ensure its accuracy as it is captured in the system.

Management Reviews

Does the organization's management review data informally or systematically? Informal management reviews could include reviews of summary-level reports to look for outliers or the evaluation of period-to-period changes, looking for differences from historic trends. Outliers and unusual changes could (but do not necessarily) signal problematic data issues.

Do agency systematic management reviews include a random sample of cases that management reviews during each period? Does the computer system generate exception reports for unusual data being generated? Does management systematically review these exception reports?

System Changes

What are the organizational procedures regarding changes to the system? For example, are reporting requirements created by policy personnel correctly translated into programming requirements for system technicians?

Policy personnel might request reporting on the number of cases meeting specific criteria. Does the implemented programming generate accurate reporting of all cases in the system that meet those criteria? Are some cases meeting the criteria not reported because of programming logic that has errors? Are programming changes first conducted in a test environment before being implemented? What procedures define new data elements? What procedures are in place to change data elements?

System Controls

System controls that could affect the accuracy and completeness of data include, among others, edit checks, access controls, system assigned data, and case history.

Edit Checks

When personnel enter information in the system, do they receive error messages when they enter obviously incorrect data? For instance, edit checks could demand certain precision for dates that can be entered. If money is being obligated for a current fiscal year, does the system allow only dates from the current fiscal year?

The precision of data entry that edit checks demand can be important in determining the reliability of the data. Sometimes the edit checks are not precise enough to ensure data quality. Conversely, the precision of the edit checks could affect data quality negatively. For instance, if only some data entries are allowed by edit checks in the system, do personnel enter data that are allowed by the system but that are incorrect so they can avoid the edit checks?

Access Controls

Who can access the system? What controls limit access to only the appropriate people? What are the controls on who has “read” access versus “write” access to the system? Who is able to change programming in the system?

System-Assigned Data

Another system control could have the computer assign data instead of their being entered by agency personnel. For instance, does the computer generate a time and date stamp? This could ensure that dates are accurate and not susceptible to manipulation.

Case History

Does the system maintain historic data about the case? For instance, if a case moves from an old to a new status, is this history captured, or is the old status overwritten?

While auditors can learn about process and system controls through interview procedures, they should take additional steps to validate the effectiveness of process and system controls. The amount of validation needed is affected by the expected importance of the data to the final report. Validation could occur through inspecting case entry procedures as a case moves through a program. An auditor could examine personnel interactions with the data system at various stages in a process. To check for accuracy, auditors could choose a small sample of source documents and compare information in physical files with data in the system. Validation of programming requirements and access controls can be technically difficult and auditors might consult with information technology specialists if needed.

Appendix III: Sample Language for Reporting on Data Reliability

In a report's introductory paragraphs and section on objectives, scope, and methodology, include a statement about conformance to generally accepted government auditing standards. These standards include the appropriateness of the data being used.

You conform to GAGAS by discussing in the report what you did to assess the data, any data concerns, and your judgment about the reliability of the data for use in the product. When data are used to answer one or more of the researchable questions, summarize these points in the introductory section of the report.

General Examples

Here are four general examples.

Example 1:

We assessed the reliability of _____ data by (1) performing electronic testing of required data elements, (2) reviewing existing information about the data and the system that produced them, and (3) interviewing agency officials knowledgeable about the data. We determined that the data were sufficiently reliable for the purposes of this report.

Example 2:

We assessed the reliability of _____ data by (1) performing electronic testing of required data elements, (2) reviewing existing information about the data and the system that produced them, and (3) interviewing agency officials knowledgeable about the data. In addition, we traced a statistically random sample of data to source documents (see appendix x for details). We determined that the data were sufficiently reliable for the purposes of this report.

Example 3:

To assess the reliability of _____'s data, we (1) performed electronic testing for obvious errors in accuracy and completeness; (2) reviewed related documentation, including contractor audit reports on data verification; and (3) worked closely with agency officials to identify any

data problems. When we found discrepancies (such as nonpopulated fields or data entry errors), we brought them to _____'s attention and worked with _____ to correct the discrepancies before conducting our analyses. We determined that the data were sufficiently reliable for the purposes of our report.

Example 4:

To assess the reliability of the data elements needed to answer the engagement objectives, we (1) performed electronic testing of required data elements, (2) reviewed related documentation, and (3) interviewed agency officials knowledgeable about the data. The results of our electronic testing showed that data elements key to our review contained high percentages of missing data. (See appendix x for further details.) Therefore, we determined that the data were not sufficiently reliable for the purposes of this report. To answer the research question, we . . .

Examples Adapted from
GAO Reports

Sufficiently Reliable

Here, adapted from GAO reports, are five examples of sufficiently reliable data, with no or few caveats.

Example 1:

To assess the reliability of the Federal Trade Commission's cost and fee collection data, we talked with agency officials about data quality control procedures and reviewed relevant documentation. We determined that the data were sufficiently reliable for the purposes of this report.

Source: GAO, *Telemarketing: Implementation of the National Do-Not-Call Registry*, [GAO-05-113](#) (Washington, D.C.: Jan. 28, 2005).

Example 2:

To assess the reliability of the FBI's October 2002 through May 2003 criminal fingerprint submission data, we (1) reviewed existing documentation related to the data sources, (2) electronically tested the data to identify obvious problems with completeness or accuracy, and (3) interviewed knowledgeable agency officials about the data. We determined that the data were sufficiently reliable for the purposes of this report.

Source: GAO, *Law Enforcement: Information on Timeliness of Criminal Fingerprint Submissions to the FBI*, [GAO-04-260](#) (Washington, D.C.: Jan. 27, 2004).

Involved some tracing to source documents and working with agency to resolve discrepancies

Discussion of use of background data

Example 3:

We obtained and analyzed data on the time associated with the grant award and distribution processes. We reviewed these data for obvious inconsistency errors and completeness and compared them for the five selected states with paper documents we obtained from these states. When we found discrepancies, we brought them to the attention of the Office for Domestic Preparedness and state and local officials and worked with them to correct the discrepancies before conducting our analyses. From these efforts, we determined that the time period data were sufficiently reliable for the purposes of this report.

. . . We also obtained and analyzed grant funding and expenditure data from selected states and local jurisdictions. Given that the grant funding and expenditure data are used for background purposes, we did not assess their reliability.

Source: GAO, *Homeland Security: Management of First Responder Grant Programs Has Improved but Challenges Remain*, [GAO-05-121](#) (Washington, D.C.: Feb. 2, 2005).

Example 4:

This documentation included information on staffing requirements and the number of bags per hour that can be screened by in-line explosives detection systems, compared with stand-alone explosives detection systems and explosives trace detection machines. We also interviewed officials from the Transportation Security Administration (TSA), air carriers, airports, explosives detection systems equipment manufacturers, and airport industry associations to obtain information on TSA's efforts to improve checked baggage screening operations using explosives detection system machines.

Use of corroborating evidence

Although we could not independently verify the reliability of all this information, we compared it with other available supporting documents to determine data consistency and reasonableness. From these efforts, we believe the information we obtained is sufficiently reliable for this report.

Further, we reviewed the results from unannounced, undercover, covert testing of checked baggage screening operations that TSA's Office of Internal Affairs and Program Review conducted, and we questioned TSA officials about the procedures used to ensure the reliability of the covert test data. From their answers, we believe that the covert test data are sufficiently reliable for the purposes of our review.

Source: GAO, *Aviation Security: Systematic Planning Needed to Optimize the Deployment of Checked Baggage Screening Systems*, [GAO-05-365](#) (Washington, D.C.: Mar. 15, 2005).

Reviewed various system
documentation and reports

Example 5:

We obtained online access to the DAISY, MIDAS, DODAAD, and FEDLOG programs, and we obtained copies of the SAMMS databases for fiscal years 2002 and 2003 and Government Liquidation LLC databases for June 2001 through December 2004. For each Department of Defense (DOD) system and database we used in our work, we (1) obtained information from the system owner or manager on its data reliability procedures; (2) reviewed systems documentation; (3) reviewed related DOD Inspector General reports, Defense Logistics Agency (DLA) comptroller budget data, and independent public accounting firm reports related to these data; and (4) performed electronic testing of commodity purchase and excess inventory databases to identify obvious errors in accuracy and completeness.

Worked with agency to
resolve discrepancies and
disclosed limitations in report

We verified database control totals, where appropriate. We also received FEDLOG training from the Defense Logistics Information Service (DLIS) service provider. When we found obvious discrepancies, such as omitted national stock number data in the DLA commodity purchases databases and transaction condition coding errors in the Defense Reutilization and Marketing Service (DRMS) excess property systems data, we brought them to the attention of agency management for corrective action. We made appropriate adjustments to transaction data used in our analysis, and we disclosed data limitations with respect to condition coding errors and the omission of national stock number data that affected our analysis.

Performed statistical testing

Our data analysis covered commodity purchases and excess commodity turn-ins and disposal activity during fiscal years 2002 and 2003. In addition, we statistically tested the accuracy of excess inventory transactions at five Defense Reutilization and Marketing Offices (DRMO) and five DLA supply depots. We also reviewed summary data and selected reports on DRMS compliance reviews of 91 DRMOs during fiscal year 2004 to determine the extent to which DRMS had identified problems with adherence to DOD and DRMS policies, made recommendations for corrective actions, and monitored DRMO actions to address its recommendations. From these procedures, we are confident that that the DOD data were sufficiently reliable for the purposes of our analysis and findings.

Source: GAO, *DOD Excess Property: Management Control Breakdowns Result in Substantial Waste and Inefficiency*, [GAO-05-277](#) (Washington, D.C.: May 13, 2005).

Here, adapted from GAO reports, are four examples of sufficiently reliable data, with caveats and specific purpose stated.

Example 1:

To address the staffing effort for the Coalition Provisional Authority (CPA), we collected and analyzed information CPA, the United States Agency for International Development, the Department of State, and the Army Corps of Engineers provided. We interviewed officials of these organizations as well as from the departments of Justice and Treasury.

We relied primarily on staffing data from the CPA personnel office, as its data were the most comprehensive and it was responsible for processing and managing CPA personnel requirements. To assess the reliability of these data, we (1) interviewed the officials at CPA who are responsible for compiling these data and (2) performed some basic reasonableness checks of the data against other sources of information. According to CPA officials, the staffing data are only about 90 percent accurate because of difficulties in tracking personnel entering and exiting Iraq. We determined that the data from March 2004 onward were sufficiently reliable to make comparisons of the type of personnel directly supporting CPA.

Source: GAO, Rebuilding Iraq: Resource, Security, Governance, Essential Services, and Oversight Issues, [GAO-04-902R](#) (Washington, D.C.: June 28, 2004).

Limitations noted and
specific purpose for use of
data stated

Example 2:

To obtain fiscal year 2003 expenditure data for personal protection equipment (PPE), we asked the U.S. Coast Guard to survey all 188 stations and their oversight units. Each station and unit was asked to provide the total amount of fiscal year 2003 funds spent on PPE for personnel assigned to the station during the year. These totals included expenditures for station personnel at the group and district levels.

Tracing to source documents
with results reported

To verify the accuracy of these data, we reviewed original expenditure documentation for a judgmentally selected sample of 29 stations. From this documentation, we independently quantified PPE expenditures for each station. Our count of total PPE purchases at the 29 stations was 9 percent higher than the total the Coast Guard provided—our count was 4 percent less than the Coast Guard’s, after removing expenditures for one outlier station. Coast Guard officials attributed the difference to errors station personnel made when compiling the expenditure data.

Limitations noted and
specific purpose for use of
data stated

As a result of these differences, however, we refer to the total expenditure for fiscal year 2003 as an estimate. Because Coast Guard officials considered gathering expenditure data for fiscal year 2002 too labor intensive for station personnel, given their current workloads, we used the Coast Guard’s data on planned PPE expenditures for fiscal year 2002. After reviewing possible limitations in the PPE data provided us, we determined that the data were sufficiently reliable for the purpose of providing estimates of expenditures.

Source: GAO, *Coast Guard: Station Spending Requirements Met, but Better Processes Needed to Track Designated Funds*, [GAO-04-704](#) (Washington, D.C.: May 28, 2004).

Example 3:

To assess the reliability of the data on the pledges and disbursements international donors made, we (1) interviewed the official at the Department of State who is responsible for compiling these data, based on information provided by the government of Afghanistan, and (2) performed some basic reasonableness checks of the data against other sources of information. We determined that the data were sufficiently reliable for the purpose of making a broad comparison of U.S. contributions to those of other major donors and the combined total for all other donors.

However, we also noted several limitations in the data—notably that the data were largely self-reported by donor nations to the Afghan government and were affected by differences in exchange rates. In addition, donors both overreported and underreported, because of different definitions of disbursement. Furthermore, the data on larger donors are considered more reliable than the data on smaller donors, according to the Department of State.

Source: GAO, *Afghanistan Reconstruction: Deteriorating Security and Limited Resources Have Impeded Progress; Improvements in U.S. Strategy Needed*, [GAO-04-403](#) (Washington, D.C.: June 2, 2004).

Data used for broad comparisons rather than precise amounts, with limitations noted

Examined reliability of data
obtained through survey

Example 4:

To assess the reliability of cost data federal agencies provided on our questionnaire, we examined the cost information for obvious errors and inconsistencies, and we examined responses to the questionnaire items requesting information on the development of the cost data. When necessary, we contacted respondents to clarify responses, and we reviewed documentation about the cost data. Federal agencies generated their cost data from various sources such as their financial accounting systems, credit card logs, and security services contracts.

Detailed limitations and
specific purpose noted

This cost information is not precise and the costs are not likely to represent all additional costs for the Code Orange alert periods. In some cases, we have concerns about the reliability of the cost data source within particular agencies. For example, 6 of the 16 federal agencies reported that they extracted some of the Code Orange alert cost data from their financial accounting systems. As reported in the fiscal year 2005 President's Budget, 5 of these agencies' financial management performance reports had serious flaws as of December 31, 2003.

Despite these limitations, we believe the cost data are sufficiently reliable as indicators of general ranges of cost and overall trends. However, they should not be used to determine the cumulative costs for all federal agencies for Code Orange alert periods.

. . . We reported cost data that the Department of Homeland Security (DHS) collected from states and localities for the three Code Orange alert periods only to illustrate the range of costs that states reported to DHS for reimbursement. Cost information states submitted to DHS does not include all costs for states and localities during the Code Orange alert periods. In particular, not all states submitted costs to DHS for reimbursement, and it may be that not all state agencies and localities in states that submitted cost information reported costs to their states for submission to DHS.

In addition, the cost information states submitted does not include additional costs for training or equipment and material purchases during Code Orange alert periods, because these costs are not reimbursable

Detailed limitations and
specific purpose noted

through the critical infrastructure protection grant programs. Moreover, some states have not finished validating costs they plan to submit for reimbursement.

Despite these limitations, we believe the cost data are sufficiently reliable as indicators of general ranges of costs that states submitted for reimbursement to DHS and overall trends. However, because this cost information from states and localities is not complete, it should not be used to reach conclusions about the financial effect of Code Orange alerts on states and localities.

Source: GAO, *Homeland Security: Communication Protocols and Risk Communication Principles Can Assist in Refining the Advisory System*, [GAO-04-682](#) (Washington, D.C.: June 25, 2004).

Not Sufficiently Reliable

Here are two examples with reference to data of insufficient reliability for some purposes.

Example 1:

Staff of the Office of Records Services of the U.S. Citizenship and Immigration Service (USCIS) provided cost estimates for existing change of address processing costs and for an annual nonimmigrant alien address reporting requirement. We tried to obtain supporting explanations and documentation to verify these estimates but were not provided information on them all.

On the basis of our efforts to determine the reliability of the estimates for which supporting information was provided—which included verifying calculations and bringing any discrepancies we found to USCIS’s attention—we believe that they are sufficiently reliable for the purposes of this report. We did not use cost estimates for which supporting information was not provided.

Source: GAO, Alien Registration: Usefulness of a Nonimmigrant Alien Annual Address Reporting Requirement Is Questionable, [GAO-05-204](#) (Washington, D.C.: Jan. 28, 2005).

Some data not used for lack of supporting information

Example 2:

Although we did not independently verify the accuracy of the self-reported information these agencies provided, we took a series of steps—from survey design through data analysis and interpretation—to minimize potential errors and problems. To identify potential questions, we spoke with numerous transportation experts, agency officials, and officials at organizations relevant to transportation planning and decision making, including the American Association of State Highway and Transportation Officials, the American Public Transportation Association, and the Association of Metropolitan Planning Organizations (AMPO).

Examined reliability of data obtained through survey

To verify the clarity, length of time of administration, and understandability of the questions, we pretested the questionnaire with 12 transit agencies, state departments of transportation, and metropolitan planning organizations. We also had the questionnaire reviewed by a survey expert and AMPO staff. In addition, we examined survey responses for missing data and irregularities. We analyzed the survey data by calculating descriptive statistics of state transportation and transit agency responses.^a

^aWe also surveyed state transportation departments about the analysis of benefits and costs of transit projects and the importance of different factors in decision making, for capacity-adding transit projects in their states. However, from the inconsistencies and irregularities of the survey responses, low response rate, and telephone conversations with survey respondents, we concluded that the information from this survey was not sufficiently reliable for our purposes. Therefore, we did not use the information from this survey in our analysis or include it in the report.

Some data not used because of problems found; explicit statement that did not use

Source: GAO, *Highway and Transit Investments: Options for Improving Information on Projects' Benefits and Costs and Increasing Accountability for Results*, [GAO-05-172](#) (Washington, D.C.: Jan. 24, 2005).

Here are three examples of data of insufficient reliability leading to agency changes or recommendations.

Example 1:

To assess the reliability of [early and late] release data, we reviewed the process by which the District of Columbia Department of Corrections tracks these data and the extent to which each relevant data element is complete and accurate. To do this, we interviewed department staff about the processes used to capture early and late release errors, the controls over those processes, and the data elements involved. For late release errors, we also traced data to their corresponding source documents.

We identified inconsistencies in the information, prompting the department to review its methodology for identifying late releases. This review led it and us to conclude that its methodology had been incomplete and had produced an undercount of the true number of late releases. The department modified its methodology in April 2004 to be more comprehensive.

Because the department did not have complete data on early and late inmate releases, it does not know the full extent to which they occurred and may not discover an early release error until long after an inmate has been released. With respect to late releases, the department used an incomplete methodology and, therefore, may have understated the actual number of late releases. During our review, the department modified the methodology to more accurately identify the number of late releases.

Source: GAO, *District of Columbia Jail: Management Challenges Exist in Improving Facility Conditions*, [GAO-04-742](#) (Washington, D.C.: Aug. 27, 2004).

Data problems found during review led to a statement of possible effect and modification by agency

Because of the quality of the data, database reliability became a reporting objective

Example 2:

From Results in Brief: Our review of prospective ruling request cases showed that the Legal Case Inventory System (LCIS), the Office of Regulation and Rulings' (OR&R) automated database, continued to face data reliability challenges potentially hindering its effectiveness as a tool for tracking and monitoring the progress and history of cases and measuring timeliness. For example, our comparison of LCIS data to case files showed that 88 of the 325 cases we reviewed were inaccurately coded as rulings in LCIS.

In response to recommendations we made in our September 2000 report, and to data errors we found in this review, OR&R has taken corrective actions to improve the accuracy and reliability of LCIS data, such as developing uniform procedures for recording cases in LCIS. However, they may not resolve the LCIS data reliability challenges. Although the corrective actions include goals such as correctly coding cases and entering timely and accurate information into the database, some of the actions lack specific procedures for effective implementation. For example, OR&R did not provide specific guidance as to how, when, and by whom information letters are to be coded. This report contains a recommendation to the OR&R Assistant Commissioner regarding continued assessment of LCIS data reliability to determine whether the corrective actions are sufficient.

Data collection included a file review of randomly selected cases, with comparison to the database and review of documents such as standard operating procedures

From Objectives, Scope, and Methodology: To determine whether OR&R resolved the data reliability challenges it faced with LCIS, we interviewed OR&R management officials, reviewed case file information for our sample of 325 OR&R headquarters cases categorized in LCIS as prospective rulings, and collected and reviewed other available information. This information included the July 2002 Standard Operating Procedure, intended to ensure a consistent process for receiving, acknowledging, assigning, recording, tracking, updating, signing, and closing ruling cases in LCIS.

In reviewing OR&R's case files for our sample of cases and noting discrepancies with LCIS data for "type of case code," "case category code," "date assigned," and "date closed," we did not discuss each case with OR&R officials to determine the reasons that case file data did not

match LCIS data or data were missing from case files. To do so would have been time consuming and complex, for us as well as OR&R, with little likelihood of determining the reason for each discrepancy. In carrying out the work for our September 2000 report on OR&R headquarters rulings, we asked OR&R officials to explain the reasons for discrepancies. However, we reported that we could not always identify the reasons why LCIS data were inaccurate for the cases we reviewed.

From Recommendations: To help ensure that LCIS data are accurate and that OR&R can reliably use the database as a management tool to record and monitor prospective rulings and measure timeliness, we recommend that the OR&R Assistant Commissioner take steps to continue to assess LCIS data reliability to determine whether recent improvements sufficiently correct past problems.

Source: GAO, *U.S. Customs Service: Prospective Rulings More Timely, but Database Reliability Questions Remain*, [GAO-03-828](#) (Washington, D.C.: Aug. 6, 2003).

Example 3:

In our effort to examine General Services Administration’s (GSA) FAIRS systems, we reviewed the extent and quality of controls over federal aircraft data. In doing so, we sought to determine whether (1) GSA had management controls in place to provide reasonable assurance that the FAIRS data included in its report were valid and reliable and (2) FAIRS data were sufficiently reliable for our intended use.

We identified and evaluated GSA’s management controls over the processes to collect, analyze, and report costs, use, and numbers of government aircraft. We did not audit the data that agencies submit to FAIRS, and we did not audit the data produced by FAIRS or the information GSA included in its annual reports. We conducted background research and site visits, interviewed GSA officials, and collected and reviewed documentation on GSA and FAIRS to gain an understanding of GSA’s operations and FAIRS processes, its inherent and control risk factors, and existing management controls. We documented our understanding of the processing of aircraft inventory, cost, and use data in FAIRS, and the identified internal controls in a process flow chart. For each relevant process identified, we assessed the overall effectiveness of existing controls by conducting a walk-through of the system and performing control testing— physical observation of how controls actually operated.

Engagement involved review of internal controls for system, as well as reliability of information in the database

Further, we evaluated the results of our analyses and testing to conclude whether GSA management controls provide reasonable assurance that the FAIRS data included in GSA’s annual report are valid and reliable. We found that information in the database was not sufficiently reliable to accurately determine the composition and cost of federal aircraft programs. However, we used the information to provide descriptive and summary statistics (in app. II). As a result, we developed recommendations for improving or establishing management controls to help ensure FAIRS data quality.

From Recommendations: To improve the completeness and accuracy of the FAIRS database so that it captures all aircraft program costs and is useful for conducting detailed analyses of the condition and

performance of the federal aircraft fleet, we are making the following three recommendations to the Administrator of GSA:

- Clarify existing FAIRS guidance to agencies to identify the cost elements that all aircraft programs should report to the FAIRS system, make the reporting of those elements mandatory, and develop a mechanism to ensure that agencies comply with reporting requirements.
- Expand existing FAIRS guidance to require that programs report additional aviation costs associated with acquiring aircraft, not currently required; this would provide more complete and accurate data on the composition and cost of the federal aircraft fleet and, thus, enhance GSA's annual report on federal aircraft operations. At a minimum, agencies should be required to report acquisition, financing, and self-insurance costs.
- Test the FAIRS database periodically to ensure that existing systems controls are working as designed and work with the Interagency Committee for Aviation Policy to identify, develop, and implement additional controls as necessary.

Source: GAO, *Federal Aircraft: Inaccurate Cost Data and Weaknesses on Fleet Management Planning Hamper Cost Effective Operations*, [GAO-04-645](#) (Washington, D.C.: June 18, 2004).

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, <http://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

