



G A O

Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

May 2001

HEADS OF DEPARTMENTS AND AGENCIES

Improper payments are a widespread and significant problem in the federal government and will continue to be of concern in the future. They include inadvertent errors, payments for unsupported or inadequately supported claims, payments for services not rendered, payments to ineligible beneficiaries, and payments resulting from outright fraud and abuse.

We are issuing this executive guide to provide federal agencies with information for their consideration when developing strategies and planning and implementing actions to reduce improper payments. The guide provides case illustrations and other information on actions that several federal agencies, states, foreign governments, and private sector companies found to be effective in addressing their improper payment problems. We categorize the actions into the areas outlined in our *Standards for Internal Control in the Federal Government*, since many of the causes of improper payments can be traced to the lack of or inadequate systems of internal control.

To facilitate review, the exposure draft is located on the Internet on GAO's Home Page (www.gao.gov) under "Other Publications." Additional copies can be obtained from the U.S. General Accounting Office, Room 1100, 700 4th Street, NW, Washington, DC 20548, or by calling (202) 512-6200, or TDD (202) 512-2537. This executive guide was prepared under the direction of Linda Calbom, Director, Financial Management and Assurance. Please send comments by August 15, 2001, to Linda Calbom or Tom Broderick, Assistant Director, Financial Management and Assurance, at the U.S. General Accounting Office, 441 G Street, NW, Room 5085, Washington, DC 20548.

Jeffrey C. Steinhoff
Managing Director
Financial Management and Assurance

May 2001

STRATEGIES TO MANAGE IMPROPER PAYMENTS

Learning From Public and Private Sector Organizations

EXPOSURE DRAFT



G A O

Accountability * Integrity * Reliability

Preface

The federal government of the United States—the largest and most complex organization in the world—expended approximately \$1.8 trillion dollars in fiscal year 2000. As the steward of taxpayer dollars, it is accountable for how its agencies and grantees spend those funds, and is responsible for safeguarding against improper payments—payments that should not have been made or that were made for incorrect amounts.

Despite the amount of funds involved and the impact improper payments can have on a program’s ability to achieve its intended outcome, most agencies have not yet estimated the magnitude of improper payments in their programs. Without a systematic measurement of the extent of the problem, agency management cannot determine (1) if the problem is significant enough to require corrective action, (2) how much to cost-effectively invest in internal control systems to correct the problem, or (3) the impact of the actions already taken to reduce improper payments or additional corrective actions needed.

This executive guide is intended to identify effective practices and provide case illustrations and other information for federal agencies’ consideration when developing strategies and planning and implementing actions to manage improper payments in their programs. It was prepared at the request of Senator Joseph I. Lieberman in his capacity as Ranking Member, Senate Committee on Governmental Affairs. This is one in a series of projects we are undertaking for the Senate Committee on Governmental Affairs and the House Committee on Government Reform concerning the issue of improper payments involving federal programs.

In producing this guide, we contacted a number of private and public sector organizations, which we identified primarily through extensive research on financial management practices, and obtained information on actions that they took and considered effective in reducing improper payments.¹ The participants were the Department of Health and Human Services’ Health Care Financing Administration; the Social Security Administration; the Department of Veterans Affairs; the states of Illinois, Texas, and Kentucky; the governments of Australia, New Zealand, and the United Kingdom; and three private sector corporations.² We thank them for their willingness to participate and for the valuable information and insights they provided.

This executive guide was prepared under the direction of Linda Calbom, Director, Financial Management and Assurance. Other GAO contacts and

¹For a more detailed discussion of our objectives, scope, and methodology, see appendix I.

²For a description of each of these entities, see appendix II.

key contributors are listed in appendix IV. Questions can be directed to Ms. Calbom at (202) 512-9508, calboml@gao.gov, or Tom Broderick, Assistant Director, by phone, e-mail, or regular mail at the following:

Phone: (202) 512-8705

E-mail: broderickt@gao.gov

Mail: Tom Broderick, Assistant Director
U.S. General Accounting Office
441 G Street, NW
Washington, DC 20548

A handwritten signature in black ink, appearing to read "Jeffrey C. Steinhoff". The signature is fluid and cursive, with the first name "Jeffrey" being the most prominent part.

Jeffrey C. Steinhoff
Managing Director
Financial Management and Assurance

Contents

Preface	1
Introduction	8
Control Environment: Instilling a Culture of Accountability	12
Case Illustration: Control Environment in the United Kingdom	15
Strategies to Consider—Control Environment	17
Risk Assessment: Determining the Nature and Extent of the Problem	18
Case Illustration: Risk Assessment at Centrelink	21
Strategies to Consider—Risk Assessment	23
Control Activities: Taking Action to Address Identified Risk Areas	24
Data Sharing	25
Data Mining	28
Neural Networking	30
Recovery Auditing	32
Contract Audits	33
Prepayment Investigations	34
Strategies to Consider—Control Activities	35
Information and Communications: Using and Sharing Knowledge to Manage Improper Payments	36
Case Illustration: Information and Communications in Illinois	40
Strategies to Consider—Information and Communications	41
Monitoring: Tracking the Success of Improvement Initiatives	42
Case Illustration: Monitoring at the Department of Work and Income New Zealand	44
Strategies to Consider—Monitoring	46
Observations	47

Appendixes

Appendix I:	Objectives, Scope, and Methodology	50
Appendix II:	Entity Descriptions	52
Appendix III:	Other Resources	58
Appendix IV:	GAO Contacts and Staff Acknowledgments	65

Figures

Figure 1: Trends in Certain Actual and Projected Federal Expenditures: Fiscal Years 1980 Through 2006	9
Figure 2: Managing Improper Payments Through Internal Controls	11

Abbreviations

AFFIRM	Association for Federal Information Resources Management
AGA	Association of Government Accountants
ANAO	Australian National Audit Office
BOI	Bureau of Investigations
CFO	chief financial officer
CIO	chief information officer
DI	Disability Insurance
DSS	Department of Social Security
FACS	Department of Family and Community Services
FAE	Fraud and Abuse Executive
FCW	<i>Federal Computer Week</i>
FITEC	Financial Implementation Team for Electronic Commerce
FPI	Fraud Prevention Investigations Program
FSC	Financial Services Center
FST	Fraud Science Team
GSA	General Services Administration
HCFA	Health Care Financing Administration
HHS	Department of Health and Human Services
HHSC	Health and Human Services Commission
HIC	Health Insurance Commission
HUD	Department of Housing and Urban Development
IDHS	Illinois Department of Human Services
IDPA	Illinois Department of Public Aid
IRD	Inland Revenue Department
ITRB	Information Technology Resources Board
KPI	key performance indicators
MFADS	Medicaid Fraud and Abuse Detection System
MMIS	Medicaid Management Information System
NAO	National Audit Office
NASIRE	National Association of State Information Resource Executives

NCMA	National Contract Management Association
OASI	Old Age and Survivors Insurance
OIG	Office of Inspector General
PSC	Private Sector Council
PWG	Procurement Working Group
SSA	Social Security Administration
SSI	Supplemental Security Income
TANF	Temporary Assistance for Needy Families
TDH	Texas Department of Health
TDHS	Texas Department of Human Services
VA	Department of Veterans Affairs
WINZ	Work and Income New Zealand

Introduction

Improper payments are a widespread and significant problem receiving increased attention not only in the federal government but also among states, foreign governments, and private sector companies. Improper payments include inadvertent errors, such as duplicate payments and miscalculations; payments for unsupported or inadequately supported claims; payments for services not rendered; payments to ineligible beneficiaries; and payments resulting from outright fraud and abuse by program participants and/or federal employees. In the federal government, for example, they occur in a variety of programs and activities, including those related to contractors and contract management; health care programs, such as Medicare and Medicaid; financial assistance benefits, such as Food Stamps and housing subsidies; and tax refunds.

While in the private sector improper payments most often present an internal problem that threatens profitability, in the public sector they can translate into serving fewer recipients or represent wasteful spending or a higher relative tax burden that prompts questions and criticism from the Congress, the media, and the taxpayers. For federal programs with legislative or regulatory eligibility criteria, improper payments indicate that agencies are spending more than necessary to meet program goals. Conversely, for programs with fixed funds, any waste of federal funds translates into serving fewer recipients or accomplishing less programmatically than could be expected.

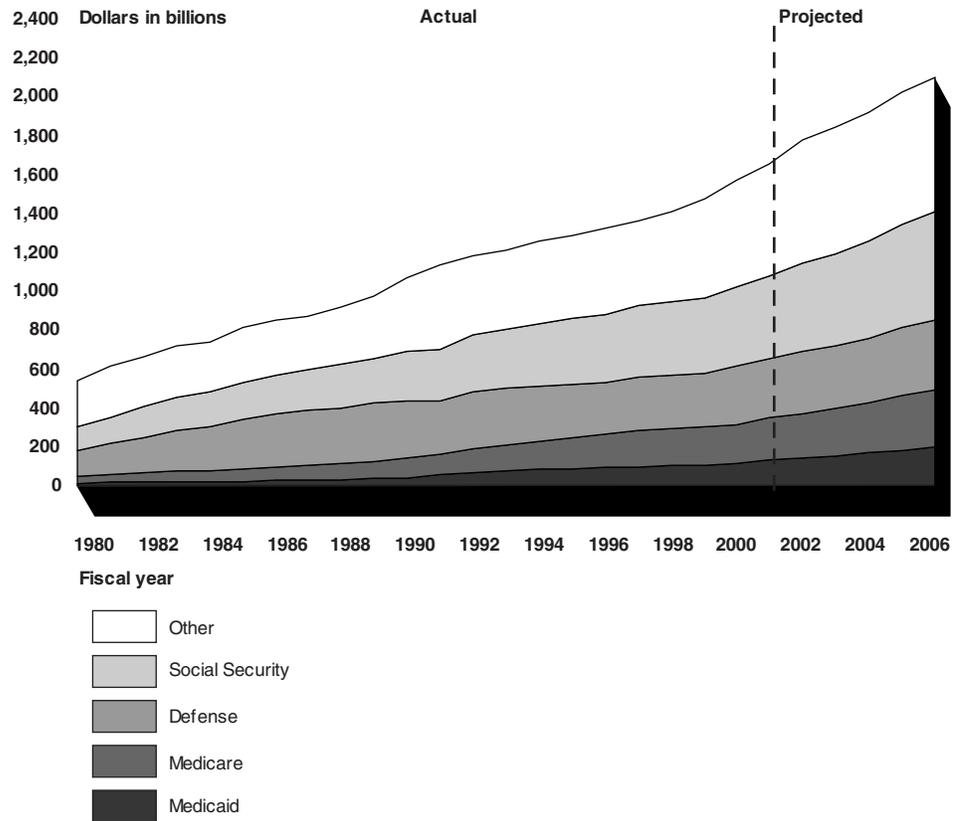
Despite a climate of increased scrutiny, most improper payments associated with federal programs continue to go unidentified as they drain taxpayer resources away from the missions and goals of our government. They occur for many reasons including insufficient oversight or monitoring, inadequate eligibility controls, and automated system deficiencies. However, one point is clear based on our study—the basic or root causes of improper payments can typically be traced to a lack of or breakdown in internal control. Collectively, internal controls are an integral component of an organization’s management that provides reasonable assurance that the organization achieves its objectives of (1) effective and efficient operations, (2) reliable financial reporting, and (3) compliance with laws and regulations. Internal controls are not one event, but a series of actions and activities that occur throughout an entity’s operations and on an ongoing basis. People make internal controls work, and responsibility for good internal controls rests with all managers.

The risk of improper payments increases in programs with (1) complex criteria for computing payments, (2) a significant volume of transactions, or (3) emphasis on expediting payments. Since these factors apply to a

number of government programs that collectively disburse billions of dollars, there is clearly a need for federal agencies to be ever more vigilant in the design, implementation, and maintenance of proper controls for safeguarding assets and preventing and detecting fraud and errors.

The risk of improper payments and the government's ability to prevent them will continue to be of concern in the future. Under current federal budget policies, as the baby boom generation leaves the workforce, spending pressures will grow rapidly due to increased costs of programs such as Medicare, Medicaid, and Social Security. Other federal expenditures are also likely to increase. The increased size of federal programs, spending pressures, implementation of new programs, and changes in existing programs all but guarantee that, absent improvements in internal controls and other proactive actions, the potential for additional or larger volumes of improper payments will be present. Figure 1 illustrates the reported and projected trends in certain federal expenditures, excluding interest on the public debt, for fiscal years 1980 through 2006.

Figure 1: Trends in Certain Actual and Projected Federal Expenditures: Fiscal Years 1980 Through 2006



Source: Actual and projected amounts are from the *Budget of the United States Government, Fiscal Year 2002, Historical Tables*.

Recognizing the increase in these expenditures and the related increase in the risk of improper payments, the administration's budget plan includes a policy issue to reduce erroneous payments to beneficiaries and other recipients of government funds.

Few would argue that the goal of reducing improper payments is not a worthy one. But attacking the problem requires a strategy appropriate to the organization involved and its particular risks, including a consideration of the legal requirements surrounding security and privacy issues. The organizations that participated in our study have taken actions that they consider to be effective in reducing potential as well as actual improper payments.

All of these actions shared a common focus of improving the internal control systems over the problem area. This focus on internal controls does not necessarily mean that the programs lacked controls but that the existing controls needed to be updated or policies and procedures added to strengthen the overall control system.

In this executive guide, we highlight many of the strategic actions taken by the study participants³ to reduce improper payments. We categorize these actions into the five general components of internal control—control environment, risk assessment, control activities, information and communications, and monitoring—outlined in the Comptroller General's *Standards for Internal Control in the Federal Government*.⁴ For purposes of this study, we define these components as follows.

- Control environment—creating a culture of accountability by establishing a positive and supportive attitude toward improvement and the achievement of established program outcomes.
- Risk assessment—performing comprehensive reviews and analyses of program operations to determine if risks exist and the nature and extent of the risks identified.
- Control activities—taking actions to address identified risk areas and help ensure that management's decisions and plans are carried out and program objectives are met.
- Information and communications—using and sharing relevant, reliable, and timely financial and nonfinancial information in managing improper payment related activities.
- Monitoring—tracking improvement initiatives, over time, and identifying additional actions needed to further improve program efficiency and effectiveness.

³The examples we have included from these organizations are meant only to illustrate the range and variety of internal controls that may be useful to federal agency managers. They are not all-inclusive and may not include the specific controls that a particular agency may need.

⁴The Federal Managers' Financial Integrity Act of 1982 required that we issue standards for internal control in government.

Although these internal control components are applicable to the entirety of an organization's operations,⁵ this executive guide focuses on internal controls as they relate to reducing improper payments. The following graphic represents the interrelationship between the components and efforts to manage improper payments.

Figure 2: Managing Improper Payments Through Internal Controls



While this guide discusses each of these control areas separately, actions to manage improper payments would typically require a continual interaction between these areas. As depicted in the figure, the control environment surrounds and reinforces the other components, but all components work in concert toward a central objective, which, in this case, is managing improper payments.

We conclude our discussion of the actions taken to address improper payments with observations about key factors necessary for success. We have included descriptions of the entities we visited in appendix II. Also, appendix III identifies other sources of information that may be useful to federal agencies in their efforts to address improper payments in their programs.

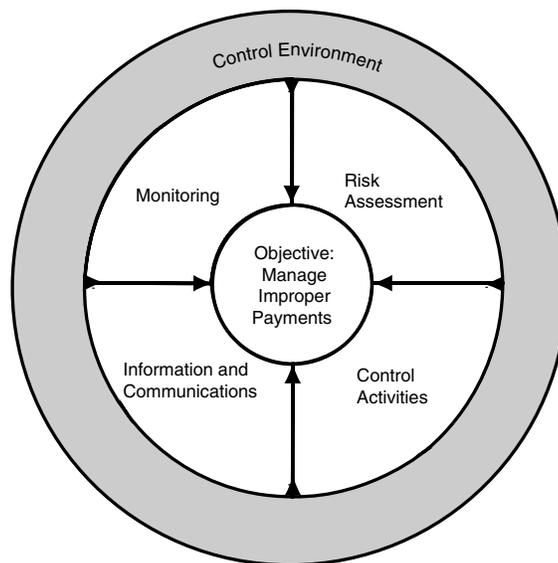
⁵See also *Internal Control Management and Evaluation Tool* (GAO-01-131G, February 2001), which has been issued as an exposure draft. The purpose of this tool is to assist agencies in maintaining or implementing effective internal control and, as needed, to help determine what, where, and how improvements can be implemented.

Control Environment: Instilling a Culture of Accountability

“Changes made in Texas might not have happened if the legislature hadn’t become involved. Regulations should not be seen as roadblocks, but as support or backing to achieve the agencies’ mission.”

Ken Holcomb,
Director of
Systems
Resources, Office
of Investigations
and Enforcement,
Texas Health and
Human Services
Commission

Of the elements that are critical to the identification, development, and implementation of activities to reduce improper payments, perhaps the most significant is the control environment. By focusing their attention on and communicating their intent to reduce improper payments throughout an organization and to all affected organizational units and individuals, top-level officials—whether in the government or within private sector companies—and legislative bodies set the stage for change. They instill a culture of accountability by adopting a positive and supportive attitude toward improvement and the achievement of established program outcomes. They also establish a transparent environment in which their expectations for program improvement are clearly defined and accountability for achieving these improvements is set. The actions of the entities in our study in areas including passing legislation, setting and maintaining the ethical tone, delegating roles and responsibilities, and implementing human capital initiatives clearly communicated the need for change.



We were told by many of the officials we met in the course of our work that, without the clearly established expectations and demands for improvement by top management and legislative officials, little would have happened to effectively reduce fraud and errors in their programs. However, it is important to note that, while top management sets the tone for cultural change, everyone from program managers to staff performing day-to-day operational activities must buy into this change and work to achieve its overall goals. The cultural change fostered by an effective control environment stresses the importance of improvement and efficient and effective program operations, while maintaining a balance with concerns raised regarding privacy and information security in a world where computers and electronic data are indispensable for making payments. In the legislative arena, it involved passing laws requiring certain actions by agency or program management, the use of various prevention and/or detection methodologies, and periodic agency reporting on the status of improvement efforts. At the agency or program level, it included management’s public commitment to reduce fraud and errors, as

well as annual performance reporting and follow-up actions based on performance results.

Top-level interest in the amount of improper payments at the organizations that participated in our study often resulted from program, audit, and/or media reports of misspent funds or fraudulent activities. As the magnitude of these improper payments became known, pressures increased on government officials and legislative bodies to reduce them.

In Texas, the legislature was instrumental in effecting changes to the state's benefit programs through provisions in several pieces of legislation. The legislature's involvement was precipitated in 1996 by the reported amounts of improper payments in Texas' Medicaid program (estimated to range from \$365 million to \$730 million, or 4 to 8 percent of total expenditures) and Temporary Assistance for Needy Families (TANF) and Food Stamp programs (estimated at a total of \$222.4 million, or about 8 percent of total expenditures for the two programs). Texas lawmakers sought to reduce improper payments by mandating specific actions by responsible agencies, including the use of computer technology to identify and deter fraud and abuse in the Texas Medicaid program. In addition, the lawmakers called for publicizing successful fraud prosecutions and fraud prevention programs to deter benefit fraud.

“There are two ways to stop fraud—one is to lock up everything around you, and the other is to surround yourself with ethical people.”

Chris Linton,
Certified Fraud
Examiner, National
Advisor, Fraud
Prevention and
Investigation, New
Zealand's Inland
Revenue
Department

Australia and New Zealand prepared and adopted a joint standard⁶ on “risk management,” to provide a cultural framework for managing risk. Risk management is the term applied to a logical and systematic method of managing risks associated with any activity, function, or process in a way that will enable organizations to minimize losses and maximize opportunities. The philosophy makes risk management a part of its organizational culture and integrates risk management into its day-to-day practices and business activities. When this is achieved, risk management becomes the business of everyone in the organization.

People are what make internal controls work, and the integrity and ethical values maintained and demonstrated by management play a key role in the entire organization's ethical tone. After the identification of significant internal fraud, New Zealand's Inland Revenue Department (IRD) created the position of National Advisor, Fraud Prevention and Investigation, and adopted a fraud control strategy. The primary aim of the strategy is to enable responsible conduct, where the need to obey the law and to behave ethically is part of the organization's ethos. Accordingly, IRD has adopted a code of conduct applicable to all employees that explains the standards of integrity and behavior expected.

In the experience of IRD's National Advisor, Fraud Prevention and Investigation, employees are often provided a copy of the code of conduct

⁶ *Joint Australian/New Zealand Standard 4360:1999* was prepared by the Joint Technical Committee OB/7—Risk Management. It was approved on behalf of the Council of Standards Australia on April 2, 1999, and on behalf of the Council of Standards New Zealand on March 22, 1999. It was published on April 12, 1999. Referenced material is from pages iii and 1 of the standard.

on their first day of work, along with a large volume of other paperwork, and never actually read the code unless the code is breached. To heighten employee awareness, IRD holds roundtable discussions with new and seasoned employees, which bring the code to life in terms of everyday business activity.

“Good customer service is accurate customer service. While timeliness is important, quality and accuracy are more important and will ultimately improve timeliness anyway.”

Sue Vardon, Chief Executive Officer, Centrelink

While many organizations have programs to deter and detect fraudulent payments, improper payments resulting from miscalculation and other errors often receive inadequate attention. Centrelink, a “one-stop shop” that pays a variety of Australian government benefits, has recently made it its business to improve payment accuracy. Centrelink was established in 1997 with a strong focus on customer service and the goal of paying beneficiaries promptly. However, in recent years, internal and external audit reports showed that Centrelink had, to some extent, traded quality for timeliness. Centrelink’s own internal review showed that up to 30 percent of all work was rework because it was not done correctly the first time. The organization’s management responded by implementing a “Getting it Right” strategy in 2000, which established a tone for change by setting out

- the roles and responsibilities of managers and team leaders, including setting clear and measurable goals in line with Centrelink’s strategic framework and meeting performance measures, and
- minimum standards to be applied by all staff in establishing proof of identity of customers, managing records, keeping technical knowledge and skills current, recording reasons for payment decisions, and checking work comprehensively.

Centrelink has distributed posters and mouse pads to reinforce the “Getting it Right” message and has provided resources to staff on how to reach minimum standards. Through implementation of the “Getting it Right” strategy, the Centrelink Chief Executive Officer has stated that she expects a reduction in improper payments as well as continued timeliness in payments to beneficiaries. Activities that must be undertaken for each program, to ensure the quality of assessment and services provided, are being developed. A number have already been released for implementation in Centrelink’s Customer Service Centre network.

Case Illustration: Control Environment in the United Kingdom

“We made the task of tackling fraud one of our early priorities. This is because public support is vital for welfare reform, and public support is eroded by the failure to stop people defrauding the benefit system.”

Tony Blair, Prime Minister, United Kingdom

By providing a clear and consistent message that benefit fraud would not be tolerated and taking initiatives to prevent or detect improper payments, the government has led the way in setting the stage for change in the United Kingdom. In 1993, the Comptroller and Auditor General in the United Kingdom, head of the National Audit Office, issued a report to Parliament stating that the government did not know enough about the level of fraud, organized or otherwise, in its benefit programs. As a result of the report, Parliament required the Department of Social Security (DSS) to improve measurement of the level of fraud within the country’s benefit programs. In 1994, DSS conducted a benefit review designed to identify the magnitude of fraud and error in Income Support followed by other major benefit programs, including Housing Benefit, Disability Living Allowance, and Retirement Pension. Based on the findings from these reviews, the government estimated that about \$3 billion⁷ per year was lost to known fraud, and noted that, if all suspicions of fraud were well founded, the figure could be as high as \$10 billion per year.

The level of improper payments captured the attention of all levels of government—including the Prime Minister. Top British officials judged that it was time to abandon business as usual, apply high standards of accountability, and use creative strategies to detect and prevent erroneous and fraudulent payments. Consequently, the British government created a control environment that mandated improvement by setting the tone at the top with the broad goal of reducing fraudulent and erroneous payments.

In 1998, DSS proposed a strategy to Parliament entitled *Beating Fraud is Everyone’s Business: Securing the Future* that explained the government’s commitment to reforming the welfare system and reducing improper payments within its programs. The proposal was widely endorsed and, the following year, DSS implemented the strategy entitled *A New Contract for Welfare: Safeguarding Social Security*. The strategy addressed efforts to be taken across four fronts:

- Getting it Right—ensuring that benefit payments are correct from day one,
- Keeping it Right—ensuring that payments are adjusted as circumstances change,
- Putting it Right—detecting when payments go wrong and taking prompt action to correct them with appropriate penalties to prevent recurrence, and

⁷Amounts included in this report have been converted to U.S. dollars using the following exchange rates, effective April 16, 2001, for one U.S. dollar: 0.697064 British pounds, 1.95665 Australian dollars, and 2.43533 New Zealand dollars.

- Making Sure Our Strategy Works—monitoring progress, evaluating the strength of controls, and making adjustments where needed.

DSS' strategy also established performance measures for the reduction of the amount of losses from fraud and error in the Income Support and Jobseeker's Allowance benefit programs.

To kick off its new program, DSS launched a publicity campaign against "benefit cheats" to shift public attitude and promote intolerance toward those who defraud the benefit system. Additionally, television commercials, billboards, newspaper articles, and an antifraud Web site (www.targetingfraud.gov.uk) communicated the government's message to the public that fraud and abuse of the benefits system would not be tolerated.

Parliament has also stayed actively involved in benefit payment reform and improper payment reductions. For example, it enacted legislation authorizing data sharing activities within and between government agencies and departments. Also the Treasury requires departments to disclose instances of irregular expenditures arising from erroneous benefit awards and fraud by claimants. Further, the Comptroller and Auditor General has qualified his opinion on DSS' fiscal year 1995 through fiscal year 2000 financial statements because of the level of fraud and error identified in the benefit programs. This served to reinforce the message that high levels of improper payments are unacceptable in the United Kingdom.

Among the organizations we studied, the pressures applied by oversight entities and top management were instrumental as change agents. They not only defined and communicated a need for improved program operations but, most important, they redefined the organizational culture. Further, by being transparent in redefining the culture, oversight entities and top management set expectations and obtained buy-in on the need for and importance of change from individuals throughout the organizations. This was critical for success since these individuals managed the day-to-day program activities. Further, a culture of accountability was essential to begin the critical next step in managing improper payments, the risk assessment process.

Strategies to Consider—Control Environment

To create a control environment that instills a culture of accountability over improper payments, the following strategies should be considered:

- provide leadership in setting and maintaining the agency's ethical code of conduct and in ensuring proper behavior under the code;
- provide a cultural framework for managing risk by engaging everyone in the organization in the risk management process;
- increase accountability by establishing goals for reducing improper payments for major programs; and
- foster an atmosphere that regards improper payments as unacceptable.

Risk Assessment: Determining the Nature and Extent of the Problem

“One of the worst problems an organization confronts is the problem of institutional denial. An organization should not simply say, ‘We know we have a problem, but we don’t want to know how big it is.’”

Aurora LeBrun,
Associate
Commissioner,
Office of
Investigations and
Enforcement,
Texas Health and
Human Services
Commission

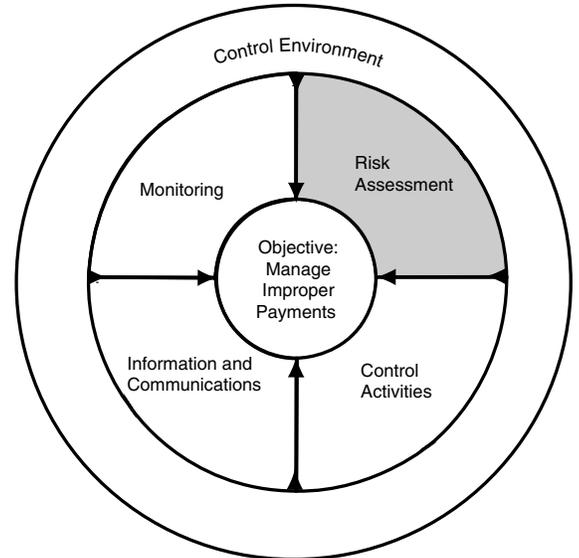
Strong systems of internal control provide reasonable assurance that programs are operating as intended and are achieving expected outcomes. A key step in the process of gaining this assurance is conducting a risk assessment, an activity that entails a comprehensive review and analysis of program operations to determine where risks exist and what those risks are, and then measuring the potential or actual impact of those risks on program operations. In performing a risk assessment, management should consider all significant interactions

between the entity and other parties, as well as all internal factors at both the organizationwide and program levels. Once risk areas are identified, their potential impact on programs and activities should be measured and additional controls should be considered. As risks are addressed and controls are changed, they should occasionally be revisited to determine where the risks have decreased and where new areas of risk may exist. As such, the risk assessment process should be iterative.

The information developed during a risk assessment forms the foundation or basis upon which management can determine the nature and type of corrective actions needed, and it gives management baseline information for measuring progress in reducing improper payments. The specific risk analysis methodology used can vary by organization because of differences in missions and the difficulty in qualitatively and quantitatively assigning risk levels. In addition, because governmental, economic, industry, regulatory, and operating conditions continually change, risk assessments should be periodically updated to identify and deal with any special risks prompted by such changes.

The organizations that participated in our study found that conducting risk assessments, to determine the nature and extent of their improper payments, was an essential step in helping them focus on the most significant problem areas and determine what needed to be done to address the identified risks in those areas.

Many federal agencies, even those with recognized weaknesses that result in improper payments, do not perform risk assessments to identify and estimate the magnitude of improper payments within their programs.



However, some agencies do perform risk assessments. For example, the Department of Health and Human Services (HHS) began reporting an annual estimate of improper payments in the Medicare Fee-for-Service program in 1996. In fiscal year 2000, it reported estimated improper Medicare Fee-for-Service payments of \$11.9 billion, or about 7 percent of such benefits. HHS' reporting and analysis of improper Medicare payments has helped lead to the implementation of several initiatives to identify and reduce such payments. These initiatives include working with providers to ensure that medical records support billed services.

A thorough risk assessment also allows entities to target high-risk areas and, therefore, to focus often limited resources where the greatest exposure exists. For example, the Illinois Department of Public Aid (IDPA) conducted a 1998 comparison of Medicaid payments made with information and documentation associated with the claims to determine if the payments were accurate. From this information, the IDPA calculated that the state's payment accuracy rate was about 95 percent. The review identified errors and their causes and provided IDPA with information that allowed it to focus attention on the 5 percent of inaccurate payments and target strategies to improve the accuracy of these payments. For example, of the \$37.2 million spent for non-emergency transportation services included in the study, \$11.55 million (31 percent) were estimated to be in error. The payment accuracy review and three other studies led to a series of actions that included assuring that transportation providers actually existed and were providing services, assuring that providers billed Medicaid correctly, and sending notices to let providers know what is expected of them.

Texas has performed two reviews of the accuracy of its health care payments—one in December 1998 and a second in January 2001. Both reviews of the Medicaid program were designed to measure the incidence of potential overpayments that could be due to fraud and abuse. The 2001 study used three different types of analyses—client telephone interviews, data analysis (identifying billing trends that are known to result in overpayments), and medical record review. Documentation errors, clerical errors, and potential fraud and abuse were identified. Texas used the results to improve its fraud and abuse detection process by considering certain high-risk areas in the development of data analysis techniques in its Medicaid Fraud and Abuse Detection System (MFADS). For example, it recommended an increase in analyses targeted at medical supplies and durable medical equipment and at providers who bill higher cost procedure codes to maximize their reimbursement.

Both Texas and Illinois found the first-time payment accuracy review to be expensive—\$250,000 and \$400,000 in direct costs, respectively. However, both states recognized that the cost of risk assessments would decrease after the baseline measurement had been determined, and found them to be cost-beneficial in light of the ability to focus on high-risk areas. Resources are maximized when strategically aimed at the areas that need the most improvement. Thus, they regarded the payment accuracy review as an effective and cost-beneficial way to combat improper payments.

Government agencies in other countries also use payment accuracy reviews to identify risk areas. For example, the Department of Social Security in the United Kingdom uses the results of a rolling program of reviews to determine the levels of fraud and error in its Income Support and Jobseeker's Allowance benefit programs. Specifically, these reviews quantify the amount of fraud, customer error, and official error (error by government employees) affecting benefit claims. The government uses the October 1997 through September 1998 review results as a baseline against which the results of subsequent reviews are measured. Further, DSS in the United Kingdom plans to use this information to target areas for prevention and detection in the benefit programs, to identify customers who are at risk for higher levels of error in their claims, and to facilitate case interventions.

Case Illustration: Risk Assessment at Centrelink

“Risk is not another thing to manage, but a way of managing.”

Dr. Helen McKenna, Deputy Chief Auditor and National Manager, Performance Assurance and Evaluation, Centrelink

Centrelink was established in 1997 as a “one-stop shop” for integrated access to Australian government services. In this role, Centrelink pays a variety of benefits on behalf of Australian government departments. Centrelink has 6.1 million customers, pays 9.2 million individual entitlements each year, and employs a staff of 22,000 in 1,000 service delivery locations across Australia.

On an annual basis, Centrelink enters into business partnership agreements with the government departments for which it administers benefits. These agreements include provisions that Centrelink perform risk assessments, noting that risk assessments and risk control strategies are integral to ensuring that compliance is effectively targeted. Centrelink’s risk assessments are performed based on information that already exists; its risk assessment process is a joint one between Centrelink and the responsible agency. A simplified version of Centrelink’s risk assessment of one of the means-tested type programs it administers might look like the following table:

	Exposure Rating		
	High	Medium	Low
Identified Risks for Improper Payments:			
Fictitious or Assumed Identity/Dual Payment	I	R	
Residential Qualification		I	R
Undeclared or Understated Income	I	R	
Payment After Death		I	R
Claiming While Imprisoned		I	R
Change in Domestic Circumstances			I/R
Undeclared or Understated Assets			I/R

I= Inherent risk

R= Residual risk

As displayed by the risk assessment table, Centrelink is identifying both

- inherent risk—the potential risk for impropriety that exists for a payment by its very nature, based on factors such as the number of beneficiaries receiving payment, complexity of legislation, use of discretion in decision-making, and political and public sensitivity, and
- residual risk—the risk that remains after considering the effectiveness of the controls put in place to address inherent risk.

To identify inherent risk for each area, Centrelink uses a variety of data sources, including prior review results, customer statistics, staff risk assessment workshops, and internal research papers. For example, to identify the inherent risk for one of its programs, Centrelink used results of reviews of 2,000 beneficiaries that identified undeclared or understated income as a major risk. In addition, a staff risk assessment workshop was held in which staff expressed concern that beneficiaries were not aware of, or did not remember, their obligation to notify Centrelink of all income they earn. This information, along with the sample results, contributed to Centrelink's assessment of the inherent risk of undeclared or understated income as high. Then, as portrayed in the table, existing controls over undeclared or understated income were considered, resulting in an assessment of residual risk at medium.

The risk assessment identifies "fictitious or assumed identity" and "undeclared or understated income" as the risk categories that pose the greatest exposure of improper payment after existing controls have been considered. Centrelink uses the risk assessment results to identify areas in which to implement strategies for decreasing the level of risk of improper payments.

"Control activities will not be fully effective until everyone, from the person on the counter through to the head of the agency, takes responsibility for managing risk from the perspective of their respective positions."

Ralph Watzlaff,
General Manager,
Professional
Review Division,
Australian Health
Insurance
Commission

In our study of activities to reduce improper payments, risk assessments identified problem areas and resulted in estimates of monetary values associated with the problems. Thus, the process of doing risk assessments was essential for evaluating the feasibility and cost-effectiveness of the various corrective actions considered. The organizations viewed risk assessments as opportunity, and identified risk areas were communicated throughout the organization.

Assessing its risks allows an organization to set goals and target its efforts to reduce improper payments. Having developed such a framework, an organization is well positioned to determine which control activities to implement to reduce risks and ultimately reduce fraud and errors.

Strategies to Consider—Risk Assessment

To assess risk by determining the nature and extent of improper payments, the following strategies should be considered:

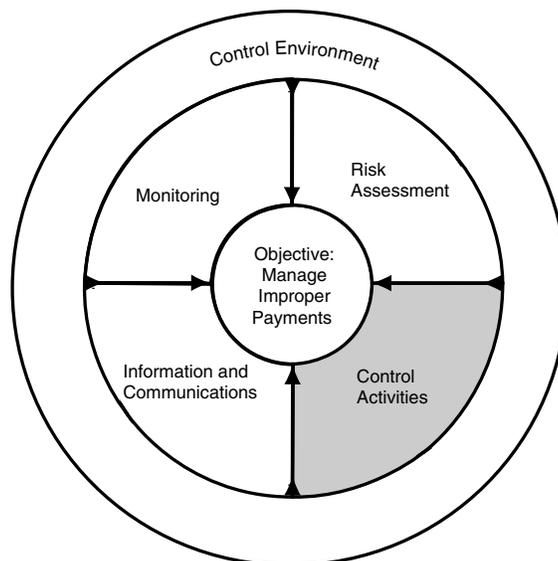
- institute a systematic process to estimate the level of improper payments being made by the organization;
- based on this process, determine where risks exist, what those risks are, and the potential or actual impact of those risks on program operations;
- use risk assessment results to target high-risk areas and focus resources where the greatest exposure exists; and
- reassess risks on a recurring basis to evaluate the impact of changing conditions, both external and internal, on program operations.

Control Activities: Taking Action to Address Identified Risk Areas

“There are no brownie points for just talking about the problem.”

Joan McQuay,
National Benefit
Control and Debt
Manager, Work and
Income New Zealand

Once an organization has identified areas of its operations that are at risk and quantified the possible extent of the risk, and its management and other key officials are committed to and have set a goal for reducing the risk, the organization must take action to achieve that goal. Control activities are the policies, procedures, techniques, and mechanisms that are designed to help ensure that management’s decisions and plans are carried out. They include activities designed to address risks that lead to fraud and error. They are an integral part of an organization’s actions in planning, implementing, reviewing, and achieving effective results.



The control activities used by an organization to address improper payments vary according to the specific threats faced and risks incurred; differences in objectives; managerial judgment; size and complexity of the organization; operational environment; sensitivity and value of data; and requirements for system reliability, availability, and performance. Additionally, they must comply with all relevant laws and help strike a balance between the sometimes competing goals of privacy and program integrity. Control activities can include both prepayment and postpayment mechanisms to manage improper payments. Given the large volume and complexity of federal payments and historically low recovery rates for certain programs, it is generally most efficient to pay bills and provide benefits properly in the first place. Aside from minimizing overpayments, proactively preventing improper payments increases public confidence in the administration of benefit programs and avoids the difficulties associated with the “pay and chase”⁸ aspects of recovering improper payments. However, recognizing that some overpayments are inevitable, agencies also need to adopt effective detection techniques to quickly identify and recover them. Detection activities play a significant role not only in identifying improper payments, but also in providing data

⁸“Pay and chase” refers to the labor-intensive and time-consuming practice of trying to recover overpayments once they have already been made rather than preventing improper payments in the first place.

on why these payments were made and, in turn, highlighting areas that need strengthened prevention controls.

The organizations in our study used many different prevention and detection control activities to manage improper payments. The nature of these activities ranged from sophisticated computer analyses of beneficiary and program participant data to postaward contract audits. The kinds of activities pursued were dictated by the types of payment activities each entity had identified as presenting the most significant risk of improper payments as well as the kind of data and other resources that were available to the entity in this effort. This guide discusses the following six kinds of control activities:

- data sharing,
- data mining,
- neural networking,
- recovery auditing,
- contract audits, and
- prepayment investigations.

The data sharing, data mining, and neural networking techniques discussed in this guide are powerful internal control tools that provide more useful and timely access to information. The use of these techniques can achieve potentially significant savings by identifying client-related reporting errors and misinformation during the eligibility determination process—before payments are made—or by detecting improper payments that have been made. However, the more extensive use of personal information in an evolving technological environment raises new questions about privacy and how it should be protected. In the federal arena, such activities must be implemented consistent with all protections of the Privacy Act of 1974, as amended by the Computer Matching and Privacy Protection Act of 1988, and other privacy statutes.

<input checked="" type="checkbox"/> Data Sharing
<input type="checkbox"/> Data Mining
<input type="checkbox"/> Neural Networking
<input type="checkbox"/> Recovery Auditing
<input type="checkbox"/> Contract Audits
<input type="checkbox"/> Prepayment Investigations

Data sharing allows entities that make payments—to contractors, vendors, or participants in benefit programs—to compare information from different sources to help ensure that payments are appropriate. For government agencies, data sharing can be particularly useful in confirming initial or

continuing eligibility of participants in benefit programs and in identifying improper payments that have already been made.⁹

A form of data sharing that Texas has found to be effective for determining the initial eligibility of individuals for Food Stamp benefits puts information from several state and local agencies in

⁹See also *Benefit and Loan Programs: Improved Data Sharing Could Enhance Program Integrity* (GAO/HEHS-00-119, September 13, 2000).

the hands of state caseworkers by means of a vendor-provided software program. The vendor maintains public information, such as that recorded by local department of motor vehicles or municipal courts, where it can be easily searched by caseworkers to evaluate information provided by individuals applying for benefits. Using the software, caseworkers can target questions to applicants when there are discrepancies between information provided by the clients and that recorded elsewhere. Caseworkers can search the database for data such as driver's license information, records showing the number of individuals or vehicles at the clients' reported addresses, telephone numbers, vehicle values, boat and motor files, criminal convictions, marriage/divorce records, and consumer credit reports. Then, for example, if the data search shows two cars at an applicant's address when the benefit applicant has reported only one, the caseworker can, at the time of the benefit application, question the applicant concerning this discrepancy. Generally, this query information is treated only as a "case clue" and must be verified. The database contains reporting options that allow supervisors to monitor employees' use of the system to ensure that all queries are appropriate—in addition, the state's internal auditor monitors the staff's use of the database.

Beyond determining initial eligibility of participants in benefit programs, data sharing can also be used to identify improper payments that have already been made. Data sharing allows a flow of information in two directions, which is particularly helpful to some organizations in managing improper payments. For example, the Social Security Administration (SSA) obtains death records from states to determine if deceased individuals are receiving benefit checks. At the same time, SSA provides data to states and other agencies. Among the data it shares is notification of whether there is a valid social security number to confirm the eligibility of applicants for various state or federal benefit programs. The exchange of information allows data matches to take place, a process in which information from one source is compared with information from another to identify any inconsistencies. Data matches of social security numbers and other data can help determine whether beneficiaries are receiving payments inappropriately or under more than one name or address.

SSA performs over 20 data matches with over 10 federal agencies and more than 3,500 state and local entities using incoming information. Additionally, SSA shares outgoing information with federal agencies through more than 15 matches. For example, SSA shares data with the Department of Housing and Urban Development (HUD) so it can perform a match to verify the identity of recipients of housing benefits and identify potentially fraudulent claims. SSA uses data matches to prevent and detect improper payments in its programs. It estimates that it saves \$350 million annually for Old Age and Survivors Insurance and Disability Insurance, and \$325 million annually for Supplemental Security Income through the use of data matching. Further, the savings are not limited to

SSA data matches save \$1.5 billion for other government agencies each year.

those realized by SSA. According to SSA, its matches save approximately \$1.5 billion each year for other agencies.¹⁰

Data matches to identify improper payments can be performed periodically (i.e., daily, monthly, or yearly) or on an ad hoc basis, using various sources of data to reconfirm eligibility of beneficiaries and accuracy of payments. Texas conducts both periodic and ad hoc matches using data including

- prisoner information obtained from the Texas Department of Criminal Justice and SSA's Prisoner Verification System (to determine whether prisoners are receiving benefits to which they are not entitled),
- deceased individuals lists obtained from the Texas Department of Health Bureau of Vital Statistics (to determine whether benefits are being paid to such individuals), and
- income information obtained from the Texas Employees Retirement System (to check retiree income for amounts that affect the level of benefit eligibility).

Texas also shares data with three of its bordering states to determine duplicity of benefits, which, for the four states, has resulted in an average of 337 potential duplicates per state per quarter. In fiscal year 2000, after researching potential duplicate payments, Texas denied or decreased benefits in 656 cases, resulting in approximately \$578,000 in benefits saved.

Kentucky performs data matches to determine eligibility for Food Stamps, TANF, and Medicaid benefits using an integrated automated system that lets caseworkers determine eligibility for the three programs simultaneously. At the time the application is entered into the system, the system performs several matches to obtain additional information on the applicant and prevent duplicate participation. These matches are made through its income eligibility and verification system using the applicant's social security number, name, date of birth, any previous disqualification record from assistance programs, and income. In addition, on a monthly basis, other matches are conducted. The state matches data with the National Crime Information Center to check for fleeing felons, with SSA to determine if any clients are in prison or have died, and with assistance programs in other states to check for client disqualification. In addition, matches with unemployment and state wages records are done monthly. When these matches result in information that could require changes in benefits, the matches appear on the daily case status reports, alerting caseworkers to potential changes in benefits.

The United Kingdom formalized data matching between government organizations in 1995, and it reported that, through March 2000, it had realized benefit savings of about \$450 million. From April 1999 through

¹⁰SSA calculates the annual savings based on a compilation of cost-benefit analyses performed by the matching agencies under the terms of their matching agreements with SSA.

March 2000, matches identified about 217,000 inconsistencies for further investigation, and resulted in an overall benefit saving of about \$53 million. Additionally, legislation has now been passed to enable the government to obtain financial information from the private sector in certain circumstances.

The prevalence of data sharing is evidence of the value provided to agencies when they can obtain and use data from sources external to an individual program's systems. Having the two streams of data allows for matches to occur and inconsistencies or anomalies to be flagged for further research. Federal entities contemplating data matching must do so in accordance with the provisions of the Computer Matching and Privacy Protection Act, which requires that (1) the privacy of data used in computer matches be protected, (2) agencies complete cost-benefit analyses on all computer matches and report annually on their findings, unless the matches are exempted by law, and (3) data integrity boards be established to approve and review the data matches.

<input type="checkbox"/> Data Sharing
<input checked="" type="checkbox"/> Data Mining
<input type="checkbox"/> Neural Networking
<input type="checkbox"/> Recovery Auditing
<input type="checkbox"/> Contract Audits
<input type="checkbox"/> Prepayment Investigations

While data sharing gives an organization the means to compare data from different sources, data mining offers a tool to review and analyze diverse data. Data mining analyzes data for relationships that have not previously been discovered. For example, the incidence of improper payments among Medicaid claims might, if sufficiently analyzed and related to other Medicaid data, reveal a correlation with a certain health care provider or providers.

The central repository of data commonly used to perform data mining is called a data warehouse. Data warehouses store historical and current data and consist of tables of information that are logically grouped together. The warehouse allows program and financial data from different nonintegrated systems throughout an organization to be captured and placed in a single database where users can query the system for information. The information can then be "mined" or searched according to specific criteria to identify associations, sequences, patterns, and clusters between different pieces of information—relationships that are often hidden in separated databases.

As a tool in managing improper payments, applying data mining to a data warehouse allows an organization to efficiently query the system to identify questionable activities, such as multiple payments for an individual invoice or to an individual recipient on a certain date. This technique allows personnel who are not computer specialists, but who may have useful program or financial expertise, to directly access data, target queries, and analyze results. Queries can also be made through data mining software, which includes prepared queries that can be used in the system on a regular basis.

IDPA began data mining in an effort to improve a system that was too slow to provide the timely information needed for a wide range of agency functions, including the prevention and detection of overpayments. As of December 2000, the state had spent \$29 million to create a data warehouse to supplement the Medicaid Management Information System (MMIS), which maintains data on Medicaid providers and beneficiaries as well as claims and payments. The data warehouse includes over 2,000 different fields/elements. The results of data queries are particularly useful because the data warehouse is able to store more current data than MMIS. At present, there is a 1-month lag in current information, compared to the 3 to 6 month lag that existed before IDPA began using data mining. In addition, the data warehouse can now store up to 5 years of data, and IDPA is currently weighing the costs and benefits of increasing this to 10 years of data.

IDPA officials noted that using data mining allows them to analyze large amounts of data. Because the large number of transactions in the system precludes manually examining each transaction for associations and patterns with other transactions, data mining is an effective and efficient alternative. The IDPA Office of Inspector General (OIG) also uses data mining to quickly respond to requests for information for ongoing investigations from the Federal Bureau of Investigation and the Illinois State Police.

The IDPA OIG created the Fraud Science Team (FST), an interdisciplinary team that includes an economist, program and policy experts, and information specialists. FST maximizes the value of the data warehouse by performing data mining activities and providing a research-based approach to fraud prevention and detection. FST has produced documentation on over 800 fraud schemes, which it has categorized into 19 different types, such as billing for services not rendered and kickback schemes. The information on these schemes is used in the development and implementation of targeted analyses that are run against the data warehouse information to identify data relationships and anomalies, which are often a sign of fraud. This information can also be used to implement specific controls in the system intended to prevent the identified types of fraud.

During our visit, the IDPA OIG staff ran several queries and analyses. For example, one risk area identified was health care providers that were billing for services provided in excess of 24 hours in a single day. With the capabilities of the data warehouse, OIG staff developed an analysis that identified 18 providers that had billed over 24 hours for at least 1 day during the 6 months ended December 31, 1999. A number of the identified providers were already under investigation for other program violations. As a result of this analysis, the OIG plans to refer serious cases to appropriate law enforcement agencies and take administrative action against the less serious violators.

Before the data warehouse was available, obtaining responses to queries of this kind would have required obtaining separate reports from different systems and could have taken up to 2 months. However, during our visit querying the warehouse took from several seconds to a few minutes per query.

New initiatives that Illinois expects will further improve data mining at IDPA are the development of a 3-day training course to help users properly structure queries and the use of data mining software. In an early effort using data mining software, IDPA OIG, as part of a partnership audit with HHS OIG, identified 232 hospital transfers that are believed to have been miscoded as discharges, creating a potential overpayment of \$1.7 million.

An early effort at using data mining software in Illinois has identified \$1.7 million in potential overpayments.

The large number of computerized claims processed by Medicare also lends itself to the application of data mining techniques. HHS' Health Care Financing Administration's (HCFA) claims administration contractors use data mining and statistical analysis as part of their postpayment review activities. Since 1993, HCFA also has contracted with a specialized statistical analysis contractor to perform large-scale analysis of durable medical equipment claims. Data mining can identify many potentially inappropriate payments, but determining which ones are actual overpayments takes additional investigation. Currently, the contractors only have the resources to investigate situations in which the data indicate potential large-scale abusive practices.

- Data Sharing
- Data Mining
- Neural Networking**
- Recovery Auditing
- Contract Audits
- Prepayment Investigations

Neural networking is a technique for extracting and analyzing data. In this case, the system analyzes associations and patterns among data elements, which allows it to find relationships that can result in new queries.

A neural network is intended to simulate the way in which a brain processes information, learns, and remembers. A neural network is initially "trained" or fed large amounts of data and rules about data relationships (for example, "a person's grandfather is older than that person's father"). Neural networks "learn" by comparing new data with historical data and can be used to detect patterns that are difficult, and sometimes impossible, to detect without computer intervention in large volumes of data. The more data a neural network processes the better it performs (i.e., the better it identifies the characteristics of potentially fraudulent payments). Based upon this knowledge, neural networks automatically alter their analytical processes to produce more accurate detection results.

In 1997, the Texas legislature mandated the use of neural networks in the Medicaid program. After examining the results of a pilot test

of neural networks conducted by the Comptroller's Office, Texas' Health and Human Services Commission (HHSC) responded to the legislation and implemented MFADS. The MFADS project was operational in January 1998 and combines both data mining and neural network capabilities.

In Texas, models used with the neural network technology identify fraudulent patterns from large volumes of medical claims and patient and provider history data. For example, they can help identify perpetrators of both known and unknown fraud schemes through the analysis of utilization trends, patterns, and complex interrelationships in the data. The state currently has models for physician and dental providers and plans to initiate a model for pharmaceutical providers.

HHSC awarded a contract for the development and operational support of MFADS. Annual contract costs range from \$2.6 million to \$3.1 million for contractor operations that include the development and ongoing support of the models. The Texas models are composed of 500 to 600 variables and generate an annual report that identifies the potential unscrupulous providers and ranks the providers according to how questionable their billing patterns appear to be. The models detail the variances through graphs that compare amounts billed and services rendered (among others items) by the identified provider with the average of the other providers. For example, one dental provider was ranked third on a dental model listing due to unusual activity in areas such as multi-surface restoration and root canal activities. An investigator, using MFADS, was able to run detailed reports on the provider's activity in the identified high-risk areas and determined that the combination of services provided, volume of services provided, and the recurring pattern of the services provided were indeed suspicious. Additionally, a dental consultant reviewed 100 of the provider's dental charts and determined that many of the services claimed were unnecessary. As a result, the provider agreed to a settlement and has repaid the identified overpayments of \$162,000 plus other penalties. Additionally, the provider was excluded from the Medicaid program for 15 years.

Texas' Medicaid Fraud and Abuse Detection System used neural networking to recover \$3.4 million in fiscal year 2000.

The results from both the data mining activities and the neural network reports are reviewed and possibly investigated to determine if the claims are fraudulent or the providers are unscrupulous. According to Texas officials, medical judgment is important when considering the accuracy of claims, and, as such, medical professionals assist in reviewing medical claims.

Texas' HHSC prepares quarterly reports for the legislature's review. *The Second Quarter Fiscal Year 2001 Contract Performance Report for the Medicaid Fraud and Abuse Detection System* reported that it had identified 2,567 cases (representing over \$6 million) for investigation in fiscal year 2000. As a result of

investigating these cases, approximately \$3.4 million has been recovered. These reports also show how HHSC is performing in relation to its performance measures. In fiscal year 2000, one of the performance measures was that total dollars identified for recoveries equal or exceed 139 percent (\$3.7 million) of the fiscal year contract cost amount. HHSC exceeded its goal by identifying \$6.1 million for recovery.

<input type="checkbox"/> Data Sharing
<input type="checkbox"/> Data Mining
<input type="checkbox"/> Neural Networking
<input checked="" type="checkbox"/> Recovery Auditing
<input type="checkbox"/> Contract Audits
<input type="checkbox"/> Prepayment Investigations

Recovery auditing is the practice of identifying and recovering overpayments that examines payment file information to identify possible duplicate or erroneous payments. For instance, vendors make pricing errors on their invoices, forget to include discounts that have been publicized to the general public, neglect to offer allowances and rebates, miscalculate freight charges, and so forth. In addition, the same invoices, or portions thereof, could be paid more than once. These mistakes, when not caught, result in overpayments. Recovery auditing can incorporate data mining techniques.

While traditionally used as a technique to identify improper payments already made, organizations have also experienced success in using recovery auditing to analyze records prior to payment. Because it helps to prevent improper payments before they occur, this use of recovery auditing eliminates the costs associated with obtaining reimbursements for the erroneous payments or taking other actions needed to offset future payments by the amount of the improper payment.

Recovery auditing started about 30 years ago, and it is used in several industries, including the automobile, retail store, and food service industries, and, to some extent, within the federal government. Some entities use their employees to analyze their payment records while others contract with recovery audit firms for the work. Contract firms often perform this work on a contingency fee basis, that is, they only receive compensation if they identify and recover amounts determined to be improper payments. As discussed below, recovery auditing, which has a long-standing track record in the private sector, offers an opportunity to identify improper payments before they occur and to identify and recover overpayments if they do occur.

- One private sector company contracted, on a contingency fee basis, with a recovery audit firm for a review of its accounts payable files—files in which its systems’ controls had not found errors. The review resulted in the recovery of \$8 million in improper payments. The company recently began using recovery auditing techniques on accounts payable information to prevent improper payments before they occurred. It expected that this activity would identify possible duplicate payments, and the test verified the company’s expectations. For example, during our visit, it identified and avoided a duplicate payment of \$136,000 from the reports generated by the recovery audit

A private sector company recovered \$8 million in improper payments as a result of a recovery audit.

software. In addition, as a result of using recovery auditing before payments are made, the company identified and stopped the processing of \$41 million in wire payments that had already been processed. Another advantage of the recovery audit services used by the company is that the software identifies the employees who are making processing errors so that the company can take appropriate counseling and training action.

- Another private sector company contracted with a recovery audit firm, on a contingency fee basis, to perform two separate reviews of its disbursements—the first review was for disbursements made from 1992 through 1995, and the second for disbursements made from 1996 through 1998. Both reviews identified duplicate payments and resulted in recovery actions and in changes to the payment system to help reduce future overpayments. For example, from 1996 through 1998, the company processed about 9 million invoices. The recovery audit review of these invoices identified about \$5 million in potential overpayments and resulted in actions to recover these funds, where appropriate. Further, based on an analysis of the overpayments identified, the company has implemented procedures that have reduced its dollar error rate per million of dollars of transactions from a reported \$65 in 1992 through 1995 to a reported \$34 dollars in 1996 through 1998. In addition, the company is now preparing to enter an agreement with the recovery audit contractor under which the recovery auditing software will be installed in the company’s system, allowing its staff to perform the recovery audit function—even as part of the prepayment process.

Recovery auditing is also being used to some extent in the federal government. For example, the Department of Veterans Affairs’ (VA) Financial Services Center (FSC) in Austin, Texas, had contracted with recovery audit firms in the past, but now performs recovery auditing in-house using about three full-time employees to administer the program and one employee for software development. If a duplicate payment is identified, VA takes one of several actions, including canceling the transaction prior to payment, notifying Treasury to stop issuance of a check, or issuing a bill of collection. For example, FSC has identified over \$2 million in overpayments and has collected, by either offsetting future payments or cash collection, nearly \$300,000 for the first 6 months of fiscal year 2001. A FSC official noted that recovery auditing could be beneficial to almost any organization that makes payments.

- Data Sharing
- Data Mining
- Neural Networking
- Recovery Auditing
- Contract Audits**
- Prepayment Investigations

Postaward audits of contracts are another technique that can help to combat improper payments and are used, to some degree, within the federal government. These audits verify that

VA reported recoveries of \$119 million from contract audits.

payments are being made in accordance with contract terms and applicable regulations. They can detect improper payments that have been made, help avoid future payments of the same kind, and provide oversight of companies conducting business with the government. For example, in fiscal year 1993, the VA Office of Acquisition and Materiel Management partnered with the VA OIG and the VA Office of General Counsel to establish the VA Procurement Working Group (PWG). As a result, a Contract Review and Evaluation Division was established to provide audit and advisory services related to contracts awarded by contracting officers in VA's Office of Acquisition and Materiel Management. From 1993 through September 2000, PWG reported recoveries resulting from postaward audits of contracts totaling about \$119 million. This represents a reported return of \$18 for every dollar spent in support of these audits. PWG attributes its success to the establishment of a knowledgeable and professional group of contract auditors in the pharmaceutical and medical/surgical supply industries. As a result of the audits and PWG's efforts, many contractors have voluntarily elected to perform internal reviews and have submitted 65 voluntary disclosures and refund offers to VA. Prior to 1993, VA received almost no voluntary disclosures. Some contractors have also developed and implemented corporate responsibility plans to ensure compliance with acquisition regulations and statutes.

- Data Sharing
- Data Mining
- Neural Networking
- Recovery Auditing
- Contract Audits
- Prepayment Investigations

In 1996, IDPA established a Fraud Prevention Investigations Program (FPI) to prevent ineligible persons from receiving Food Stamps, TANF, and Medicaid. Under this program, case managers in the Illinois Department of Human Services

(IDHS) refer applications that contain suspicious or conflicting information to IDPA's Bureau of Investigations (BOI) for action before benefit payments begin. Case managers use certain referral criteria, such as applications that contain contradictory information about household composition or employment, to identify these applications. BOI submits referred cases to a private investigation firm, under contract with the IDPA OIG, which investigates the information on the application. This investigation may consist of interviews; contacts with employers, landlords, or neighbors; or a visit to the applicant's home. The results are reported to BOI within 8 business days (5 business days for food stamps) and then to the local IDHS office for appropriate action—approval, denial, or reduction of benefits.

Illinois reports saving \$12 for every dollar spent on fraud prevention investigations.

The program was piloted in 1995 and was implemented in 1996, with five Cook County (Chicago) IDHS offices participating. Currently, all 23 IDHS local offices in Cook County participate in the program. FPI reports total savings, since program inception, of about \$12 for every dollar spent.

Specifically, in fiscal year 2000, FPI prevented \$9.5 million in improper payments from being issued at a cost of \$823,000. Savings are calculated based on the administrative and contract costs of the program as a percentage of gross savings and cost avoidance for cases that resulted in denied or reduced benefits.

The preceding examples of control activities are meant to illustrate a sample of the type of activities that may be useful to agency managers. An agency's internal control activities should be flexible, weighing costs and benefits, to allow agencies to tailor control activities to fit their special needs. Once control activities are in place, the internal control cycle continues with the prompt communication of information that managers need to help them carry out these activities and run their operations efficiently and effectively.

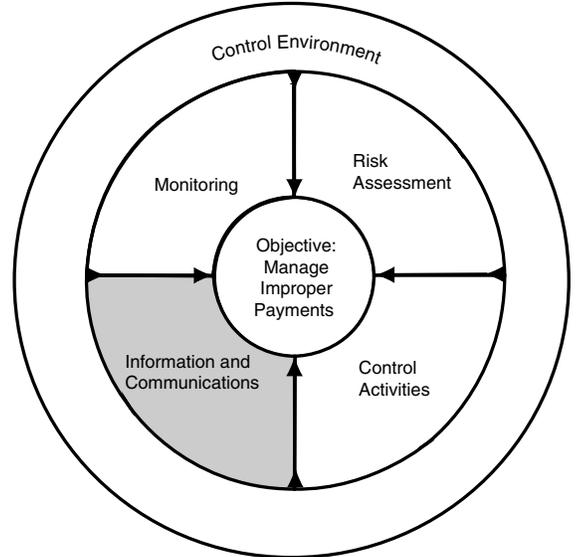
Strategies to Consider—Control Activities

In taking action to address identified risks, the following strategies should be considered:

- based on an analysis of the specific risks facing the organization, and taking into consideration the nature of the organization and the environment in which it operates, determine which types of control activities would be most effective in addressing the identified risks;
- where in-house expertise is not available, investigate the possibility of contracting activities out to firms that specialize in specific areas, such as recovery auditing and neural networking;
- perform cost-benefit analyses of potential control activities before implementation to help ensure that the cost of those activities to the organization is not greater than the potential benefit;
- ensure that personnel involved in developing, maintaining, and implementing control activities have the requisite skills and knowledge, recognizing that staff expertise needs to be frequently updated in evolving areas such as information technology and fraud investigation; and
- recognize and consider the importance of privacy and information security issues when developing and implementing control activities.

Information and Communications: Using and Sharing Knowledge to Manage Improper Payments

Top-level agency officials, program managers, and others responsible for managing and controlling program operations need relevant, reliable, and timely financial and nonfinancial information to make operating decisions, monitor performance, and allocate resources. This information can be obtained from a variety of sources using a wide range of data collection methodologies. The organizations that participated in our study used internal and external sources to obtain needed information. Further, these sources varied widely, from information contained in multiple computer databases to periodic meetings of individuals to share information on emerging issues and other areas relevant to effective program operations.



The need for information and communication extends beyond organizational boundaries. Many of the governmental programs with improper payments are benefit programs that involve recipients and providers of services. Organizations in our study developed educational programs to assist these participants in understanding eligibility and other requirements and, for service providers, information on issues including common claim filing errors.

Having information available to provide feedback to management on initiatives is necessary to adequately evaluate performance. At Centrelink in Australia, information showing achievement against key performance indicators (KPI) for compliance activity is provided to managers monthly, within 9 days of the end of the month. Information is provided about the number of compliance reviews (cases identified as high risk for incorrect payment) completed, savings, incorrect payments identified for recovery, and the level of incorrect payment. Information is also provided on prosecution activity. In addition, comparative information is made available so that the managers see how they are doing compared to other managers. While these reports are available within 9 days of the end of the reporting period, a database containing review information can be accessed within 48 hours. This enables managers to produce detailed, flexible, reports on-line. As a result

of having this timely information, managers can more effectively manage the resources available to them.

Minimizing improper payments often requires the exchange of relevant, reliable, and timely information between individuals and units within an organization and with external entities with oversight and monitoring responsibilities. This can be achieved by establishing working groups. For example, in 1997 Illinois established its Medicaid Fraud Prevention Executive Workgroup. The purpose of the workgroup is to develop reasonable and prudent measures consistent with the provision of quality health care to combat fraud and abuse in the Medical Assistance Program.

"We are always working to achieve balance between program integrity and access to health care for recipients."

Robb Miller,
Inspector General,
Illinois Department
of Public Aid

The workgroup has approximately 15 members from both the program and integrity sides of IDPA, including members from claims processing, technical support, budget and analysis, fraud research, investigations, information technology, and information systems. The cooperation between the program and the integrity divisions is the vehicle by which emerging issues are addressed. The group meets monthly to discuss the status of previously discussed and/or implemented initiatives and to propose and discuss current problems and potential initiatives. Topics discussed have resulted in ongoing changes to computer edits and policies, reflecting the dynamic nature of fraud.

While timely, accurate, and reliable information is necessary for internal use, the organizations we visited stressed that communication with the public, benefit providers, and beneficiaries was also necessary. Educating the parties involved in the transaction reduces the risk of potential errors and strengthens joint responsibility and accountability of those involved.

Texas considers the various forms of education to be cost-beneficial in its Medicaid program. For example, in 1997 it implemented several initiatives to educate new providers before they enroll in the Texas Medicaid program. First, each new Medicaid provider receives a "Success with Medicaid" package containing information on claim filing, including helpful tips, and instructions on how to use the automated phone system for inquiries. This "welcome" package is hand delivered during a site visit by one of Texas' 19 Medicaid field representatives. Three months after enrollment, the field representatives evaluate a sample of each new provider's claims to see if there are any issues that should be discussed. Then, the same representative who made the initial visit revisits the new provider to answer questions and discuss any problems noted in the claims sample. In addition, program personnel conduct various workshops for and make educational materials available to new providers.

In another example, Australia's Health Insurance Commission (HIC) implemented a feedback program to provide medical

practitioners with regular information about their own benefit authorization, age and gender patient demographics, and comparative statistical information showing the number of services rendered and dollar value of benefits paid. All 32,000 practitioners receive correspondence once a year from HIC. The program's educational feedback encourages compliance and can act as a deterrent to future wrongdoing, as practitioners are aware that HIC tracks what is claimed for reimbursement on an annual basis. While, at first, most practitioners did not realize that HIC was able to accumulate and analyze this information, the program has now become both an effective deterrent and a desired source of information for the practitioners. For example, some practitioners have asked for additional information or statistics prior to the annual feedback report. In October 1999, the HIC Internet Feedback Reporting Facility was established to provide on-line feedback and statistics to general practitioners. About 2,100 general practitioners accessed their feedback reports on-line during 1999, and HIC implemented further enhancements to include feedback to other medical practitioners.

Also in Australia, Centrelink has determined that 65 percent of its preventable incorrect payments¹¹ relate to incorrect declaration of income by the customer or beneficiary. Based on this risk assessment, Centrelink developed a range of specific prevention strategies aimed at educating beneficiaries and employers on income reporting requirements.

These include

- educating the beneficiaries on the correct way to declare earnings and reminding them of the consequences of failing to correctly declare earnings and
- outreaching employers in industries whose employees are traditionally more likely to receive improper payments, such as those with seasonal or part-time employees.

In the latter case, Centrelink provides these employers with materials to distribute to existing and new employees who are receiving benefits from Centrelink. For example, to encourage accurate income reporting, the employers distribute "payslips" envelopes to employees for their use in storing their wage records.

In addition to working groups, coordination and cooperation with local law enforcement and other sources external to an agency can establish an infrastructure conducive to preventing and detecting fraud. Our case illustration shows the value of such an

¹¹Centrelink defines all incorrect payments as preventable unless the payment is unavoidable, such as legislated advance payments. Furthermore, Centrelink categorizes preventable payments into three areas: preventable by the customer, preventable by staff, and preventable by the system. Centrelink reports \$410 million to \$460 million in incorrect payments a year, of which 70 percent is classified as preventable payments.

infrastructure in preventing a large-scale Medicaid fraud perpetrator from receiving payment for fraudulent claims.

Case Illustration: Information and Communication in Illinois

To coordinate fraud efforts, IDPA OIG established the position of Fraud and Abuse Executive (FAE) whose objective is to develop and maintain relationships with internal and external parties and be the conduit for all fraud issues. Earlier this year, the following events occurred, demonstrating the importance of direct and clear communication.

An Illinois bank teller, suspicious of a bank customer's attempt to cash an improperly endorsed Medicaid check, which was made out to a provider for \$123,000, phoned the State Treasurer's Office, which referred the teller to the FAE.

Based on the referral, the FAE queried the data warehouse and ascertained that checks totaling \$700,000 in payments had been issued to a provider within a 2-week period, based on 40,000 claims that had been filed for 43 recipients, 4 of whom were deceased. The FAE contacted the Illinois State Police Medicaid Fraud Control Unit and requested that they drive by the mailing address identified on the checks, and that they also investigate a sample of the recipients. The Illinois State Police Medicaid Fraud Control Unit immediately investigated and reported that the location was vacant and that periodically two people checked the mail. Based on this information, the FAE stopped payment on all checks to the potentially fraudulent provider and notified the Controller's Office that outgoing checks to the provider should be removed from the mailroom.

A few days later, another bank customer attempted to cash one of the checks made to the provider in the amount of \$185,000. The corporate investigator at the bank contacted the FAE. The FAE called the Illinois State Police Medicaid Fraud Control Unit who then coordinated with the bank, the state investigator with the Medicaid Fraud Control Unit, the U.S. Attorney's Office, and the Attorney General's office for possible arrests.

A sting operation followed. The bank called its customer to come into the bank to pick up the money. Two suspects were subsequently arrested. While under arrest, one suspect received a cell-phone call from a person notorious for Medicaid fraud, who had previously been permanently excluded from the Medicaid program. The police were able to lure this suspect to the police station, where the person was promptly arrested. One suspect was recently sentenced to 4 years in state prison; the other suspect is awaiting trial.

The FAE continues to use the data warehouse to develop possible relationships between the suspects and other providers. The OIG attributes the speed and success of this investigation to the cooperation between investigative bodies throughout the state and to the data warehouse technology.

Effective communications should occur in a broad sense with information flowing down, across, and up the organization. In addition to internal communications, management should ensure there are adequate means of communicating with, and obtaining information from, external stakeholders that may have a significant impact on the agency achieving its goals. Moreover, effective information technology management is critical to achieving useful, reliable, and continual recording and communication of information. Program managers need operational and financial data to monitor whether they are meeting their agencies' strategic and annual performance plans and meeting their goals for accountability and effective use of resources. Monitoring strategies are discussed in the next section.

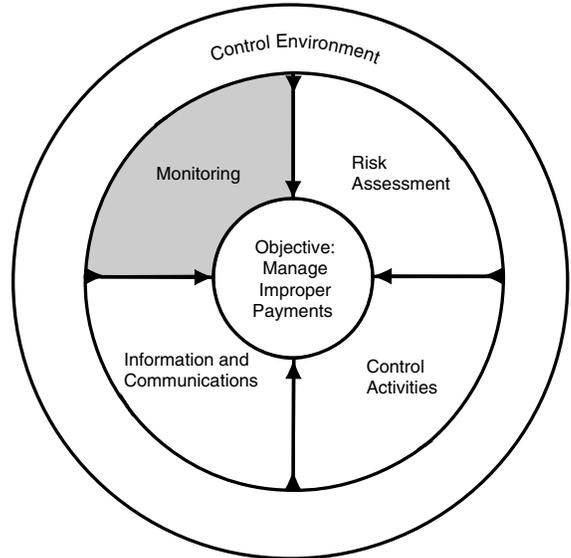
Strategies to Consider—Information and Communications

To effectively use and share knowledge to manage improper payments, the following strategies should be considered:

- determine what information is needed by managers to meet and support initiatives aimed at reducing improper payments;
- ensure that needed information is provided to managers in an accurate and timely manner;
- provide managers with timely feedback on applicable performance measures so they can use the information to effectively manage their programs;
- develop educational programs to assist program participants in understanding program requirements;
- ensure that there are adequate means of communicating with, and obtaining information from, external stakeholders that may have a significant impact on improper payment initiatives, such as periodic meetings with oversight bodies; and
- develop working relationships with other organizations to share information and pursue potential instances of fraud or other wrongdoing.

Monitoring: Tracking the Success of Improvement Initiatives

Monitoring performance, over time, is critical to program management and oversight. Evaluation of an organization's programs and its successes in meeting its established goals and in identifying additional actions is an integral element of performance measurement and continued improvement in operations. Monitoring focuses on the assessment of the quality of performance over time and on the prompt resolution of problems identified. Once an organization has identified its risks related to improper payments and undertaken activities to reduce such risks by upgrading its control activities, monitoring performance allows the organization to gauge how well its efforts are working.



“We will want to know what action is being taken and what more could be done to get a grip on the burgeoning levels of fraud and inaccuracy in benefit claims.”

David Davis,
Chairman of the
Parliamentary
Committee of Public
Accounts, United
Kingdom

In the United Kingdom, the Department of Social Security (DSS) annually reviews its Income Support and Jobseeker's Allowance programs to estimate the level of fraud and error in the programs, measure progress toward meeting established performance goals, and report performance results to Parliament. As a result of the program monitoring and evaluation activities these reviews permit, the government has set new, more challenging targets for future performance.

In addition, the National Audit Office (NAO) in the United Kingdom uses the review results in its annual audits of DSS' financial statements. NAO reviews DSS' sampling methodology and sample results, reviews some of the cases DSS examined, and selects its own sample to verify the accuracy of the reviews. The auditing standards issued by the United Kingdom's Audit Practices Board require NAO to plan and perform its audits to provide for reasonable assurance that the financial statements are “free from material misstatement, whether caused by error, or by fraud or other irregularity.” Further, Her Majesty's Treasury requires disclosure in the notes to the financial statements on a cash basis of all instances of significant irregular expenditures arising from erroneous benefit awards and fraud by claimants. After considering the results of DSS' review and its evaluation of those results, NAO qualified its fiscal year 1995 through fiscal year 2000 opinions on the DSS financial statements because of the amount of fraud and error in the benefit programs.

“The probability of review should never be zero. Not for any provider, no matter how reputable; nor for any claim, no matter how small.”

Malcolm K. Sparrow, *License to Steal; Why Fraud Plagues America's Health Care System*, 1996

Illinois assessed the risk of improper payments in its Medicaid program, and, based on the results, implemented initiatives designed to improve payment accuracy. To monitor the effects of the new initiatives, Illinois will use random claims sampling to test the accuracy of the payments by reviewing 150 randomly selected claims per month, or 1,800 per year. The goal of this project is to ensure that every paid claim faces an equal, random chance of review. The judgment of field staff, auditors, nurses, and policy experts will be used to determine if they are paid correctly. This approach not only provides periodic estimates of payment and service accuracy rates to help measure the results of existing enforcement and detection efforts, but also helps deter future erroneous and fraudulent billings.

Performance measures are key to monitoring progress in addressing improper payments. New Zealand requires entities from which the government purchases a significant quantity of goods and services to include audited statements of objectives and statements of service performance with their financial statements. These statements include, where appropriate, performance measures related to improper payments. For example, performance measures relating to entitlement accuracy, services to reduce benefit crime, and debt management have been established for Work and Income New Zealand (WINZ), a government agency that provides income support and/or employment assistance to eligible people. WINZ's financial statements are the main accountability reports used by Parliament to monitor the agency's performance. In addition, Parliament uses the audited information to make informed decisions on resource allocation, and, through a Public Service Monitoring Body (the State Services Commission), to hold the entity's Chief Executive Officer responsible if performance standards are not met. For example, the government, in its role as purchaser, can offer rewards and apply sanctions to a Chief Executive Officer to ensure performance. In addition, the government may seek to purchase goods and services from more than one source.

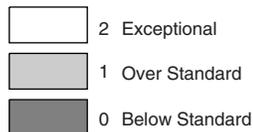
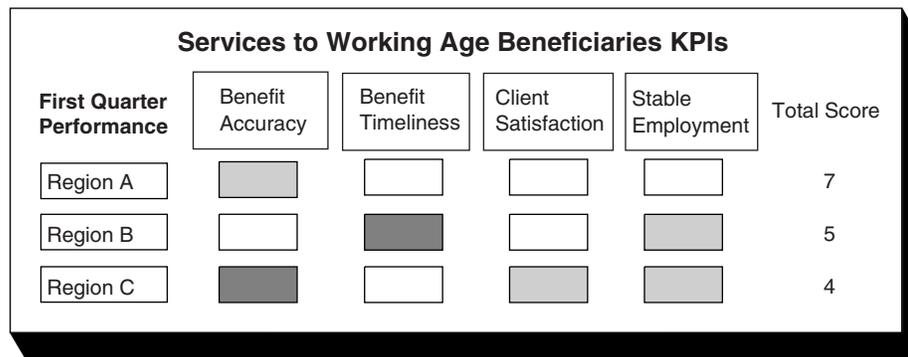
WINZ's monitoring of its payment accuracy is discussed further in the case illustration on the following page.

Case Illustration: Monitoring at the Department of Work and Income New Zealand

WINZ is one of the largest government departments in New Zealand. It administers over \$5 billion of transfer payments on behalf of the government, and is expected to affect the lives of at least one-third of the people in New Zealand at any one time. The primary purpose of WINZ is to help eligible people participate in employment, education, training, and community life through income support and/or employment assistance.

The purchase agreements between WINZ and the government include performance measures related to the accuracy of entitlement benefit decisions and the timeliness in which the decisions are made. WINZ established an Accuracy Reporting Program to help ensure that its contractual performance goals would be met. Through a monthly sampling process, cases are reviewed for accuracy and timeliness—that the right person was paid the right benefit in the right amount at the right time. Results of the accuracy reporting reviews are incorporated into the monthly service delivery KPI reports provided to regional operations managers for monthly monitoring. Performance reports are also provided quarterly to Responsible Ministers of Parliament.

WINZ officials stated that payment accuracy was just over 70 percent when it began the program in 1996. When the first KPI reports came out, staff were surprised by the areas that were below standard and wanted to know how they could improve. Some regional managers wondered why and how certain regions were doing better than their own. To monitor performance, WINZ utilized performance summaries, which include information about each region’s standing in relation to the performance goals. An example of such a performance summary is depicted below.



Several years ago, the performance summaries reflected numerous areas of below standard achievement. Over time, staff found it rewarding to track their progress. An official told us that comparing performance between regions fostered an atmosphere of healthy competition and a focus on ongoing improvement. In addition to this summary level performance reporting, WINZ implemented a team coaching program to monitor individual employee performance and provide individual feedback and support to case managers. The team coach reviews each case manager's work based on his/her level of experience. For example, a trainee has five cases per month selected for review of timeliness and accuracy. WINZ attributes team coaching, in part, to its recently reported increase in accuracy. For the period from June 30, 1999 through June 30, 2000, WINZ reported that the accuracy rate improved from 88 to 94 percent for Services to Seniors and from 89 to 90 percent for Services to Working Age Beneficiaries.

Monitoring the activities used by an organization to address improper payments should be performed continually and should be ingrained in the entity's operations. Ongoing monitoring enables an organization to measure how well it is doing, track performance measures, and adjust control activities based on the results of monitoring activities. The monitoring process should also include policies and procedures for ensuring that the results of the reviews are communicated to the appropriate individuals within the organization so that they can be promptly resolved.

Strategies to Consider—Monitoring

To track the success of improvement initiatives, the following strategies should be considered:

- establish agency-specific goals and measures for reducing improper payments;
- using baseline information for comparison, periodically monitor the progress in achieving the established performance measures;
- make the results of performance reviews widely available to permit independent evaluations of the success of efforts to reduce improper payments;
- ensure timely resolution of problems identified by audits and other reviews; and
- adjust control activities, as necessary, based on the results of monitoring activities.

Observations

Our study identified many techniques and approaches that organizations have used and found effective in reducing their levels of improper payments that could be used by federal agencies to help reduce improper payments in their programs. The techniques and approaches shared a common focus of improving the internal control systems over the problem areas and generally included actions in five areas—control environment, risk assessment, control activities, information and communications, and monitoring. Our observations on the key factors for successful actions in each of these areas follow.

In the area of control environment, we found that, for improper payment initiatives to be successful, setting the tone at the top is critical. The pressures applied by top management and oversight entities are instrumental in clearly defining and communicating the need for improved program operations and, most important, in redefining the organizational culture. The goals and objectives of the initiatives being implemented must be transparent to all in the organization. Without the ongoing strong support, both in spirit and in action, of top-level program officials and legislative bodies, the chances for success in implementing the changes needed to address improper payments are slim. This top-level support is especially critical given that an investment of time and money is often needed in these types of efforts.

One of the biggest hurdles that many entities face in the process of managing improper payments is overcoming the propensity toward denial of the problem. It is easy to rationalize avoiding or deferring taking action to address a problem if you do not know how big the problem is. The nature and magnitude of the problem—determined through a systematic risk assessment process—needs to be determined and openly communicated to all relevant parties. When this occurs, especially in a strong control environment, denial is no longer an option, and managers have the information, as well as the incentive, to begin addressing improper payments. This risk assessment is used to determine where risks exist, what those risks are, and the potential or actual impact of those risks on program operations. As such, it helps identify the areas most in need of corrective action and helps form a basis for determining how to allocate resources, human and monetary, to the problem areas. By performing risk assessments on a recurring basis, organizations also obtain information on the status of their efforts to reduce improper payments and on areas needing further attention.

In the area of control activities, we found that organizations need to tailor their actions to fit their particular needs. There is a wide range of activities that can be used to effectively address improper payments. These include the use of computer-assisted activities ranging from simple

comparative analyses (e.g., comparing beneficiaries with mortality rolls) to the use of sophisticated computer models for interactive analysis of large amounts of information (e.g., using neural networking to identify suspicious patterns of payments). Regardless of the level of sophistication involved, the key to success is having the right people perform the right jobs. While these technology-based solutions can be expensive, such investments usually more than pay for themselves in terms of dollars saved. They also can be a significant deterrent and provide for a level of program integrity that could not otherwise be achieved.

When obtaining, storing, and using computer-generated information, an organization must always be mindful of privacy and security issues. In the federal arena, including federal programs managed by state organizations, computer-assisted activities must be implemented consistent with all protections of the Privacy Act of 1974, as amended by the Computer Matching and Privacy Protection Act of 1988, and other privacy statutes.

We also found that organizations use both computer-generated information and nontechnical methods to obtain, summarize, and communicate information needed to evaluate program performance. Whatever method is used, the flow of relevant, reliable, and timely information regarding performance should lead to improved performance, particularly if an atmosphere of healthy competition is introduced into the process.

Educational activities for both beneficiaries and other program participants also serve as an effective communication approach to help reduce improper payments and strengthen program operations. The better educated agency employees, contractors, and beneficiaries are about what is expected of them and the consequences of not meeting those expectations, the greater the chances for reducing fraud and errors in the payment process.

Another key point is that just putting control activities in place is not the end of the process—monitoring progress and results is essential and must include the involvement of top-level officials. In addition to monitoring day-to-day performance, it is important for an organization to track performance over time and measure it against established performance goals or indicators. This monitoring activity provides information on the effectiveness of the control activities implemented and helps oversight and top-level management officials identify areas needing further attention or a shift in focus.

High levels of improper payments need not and should not be an accepted cost of running federal programs. The organizations that participated in our study found they could effectively and efficiently manage improper payments by (1) changing their organizations' control environments or cultures, (2) performing risk assessments, (3) implementing activities to reduce fraud and errors, (4) providing relevant, reliable, and timely information and communication of results to management, and (5) monitoring performance over time.

In the federal government, implementation of this process will likely not be easy or quick. It will require strong support, not just in words but in actions, from the President, the Congress, top-level administration appointees, and agency management officials. Once committed to a plan of action, they must remain steadfast supporters of the end goals and their support must be transparent to all.

Further, there must be a willingness to dedicate the human capital and monetary resources needed to implement the changes. In the human capital area, this could involve performing needs assessments and taking the actions necessary to obtain individuals with the skills and knowledge necessary to turn the planned actions into reality. Regarding funding, many actions that proved successful to the organizations in our study involved computer-assisted analyses of data. Effectively and efficiently implementing some of these practices could require funding for computer software and hardware, additional staff, and/or training.

In addition, it is important that the results of the actions taken be openly communicated or available not only to the Congress and agency management, but also to the general public. This transparency demonstrates the importance that the government places on the need for change and openly communicates performance results. It also acts as an incentive for agencies to be ever vigilant in their efforts to address the wasteful spending that results from lapses in controls that lead to improper payments.

Objectives, Scope, and Methodology

The objectives of this study were to identify effective practices and provide case illustrations and other information for federal agencies' consideration when developing strategies and planning and implementing actions to manage improper payments. In performing this study, we conducted extensive research and identified three federal agencies, three state governments, three foreign countries, and three private sector companies that took aggressive actions that they considered effective in reducing improper payments in their programs.

In general, for the organizations that participated in this study, we (1) conducted extensive Internet and literature searches to identify actions that each had taken to reduce improper payments, (2) made site visits to interview representatives involved in identifying and taking actions to reduce improper payments, and (3) obtained and reviewed organization reports and other documentation describing the actions taken, the results of those actions, and future plans in the area.

As outlined below, we used several techniques to identify the study participants.

Federal Agencies

We formed a focus group within GAO that was composed of program and financial analysts familiar with each federal agency. This group identified agencies that had implemented practices to reduce improper payments. Additionally, we contacted the inspectors general of the 24 Chief Financial Officers (CFO) Act agencies to obtain their views on agency activities, if any, designed to reduce improper payments. Once we identified potential participants, we conducted extensive Internet searches of their Web sites and reviewed entity and GAO audit reports and other documents to obtain background and other information for potential best practice efforts. We then contacted three agencies, discussed our study objectives and planned approach, and asked each if it had any programs in which actions to reduce improper payments were effective. Representatives at the three agencies (the Department of Veterans Affairs, the Social Security Administration, and the Department of Health and Human Services' Health Care Financing Administration) identified programs in which their organizations had taken actions considered effective and agreed to participate.

State Governments

We conducted extensive Internet searches for all 50 states to identify reports and other studies that identified states that had taken actions that appeared to identify and reduce improper payments. We also coordinated

with other GAO representatives to identify states that had taken actions to reduce improper payments in federal programs in which program management is a state responsibility, such as the Food Stamp program. Based on the information obtained, we asked representatives in the states of Illinois, Kentucky, and Texas if they had any activities that they believed were effective in reducing improper payments. Each identified some actions and agreed to participate in the study.

Private Sector Organizations

We contacted the Private Sector Council, a public service organization that assists in the sharing of knowledge between the private and public sectors. Through this organization, three companies volunteered to participate in our study and supplied us with information on the techniques they used and considered effective in reducing improper payments.

Foreign Governments

Our External Liaison Office contacted our counterparts in 12 countries and two world organizations to explain our study objective and ask for input on activities, if any, each had taken to reduce improper payments in its programs. We also conducted extensive Internet searches to identify programs in each of these entities in which actions had been taken to reduce improper payments. Based on the responses from our initial requests for information from the countries and organizations and our Internet search results, we selected three countries (Australia, New Zealand, and the United Kingdom) as possible study participants. We contacted representatives for each, and they agreed to participate.

In the course of identifying actions that possible participants in our study had taken to reduce improper payments, we identified numerous Web sites that might provide organizations with useful information that they can consider when attempting to address improper payment or other problems in their programs. Appendix III lists these resources.

We conducted our fieldwork from May 2000 through March 2001. We asked officials of the various organizations highlighted in the case illustrations and throughout the report to verify the accuracy of the information presented on their activities and incorporated their comments as appropriate. We did not independently verify the accuracy of that information.

Entity Descriptions

This appendix provides descriptions of the foreign governments' agencies and U.S. federal agencies, state governments, and private sector organizations that participated in this study. For our study, we contacted and visited various people from the listed organizations who spent many hours planning and hosting our visits, coordinating meetings, and preparing and presenting information. We thank them for their willingness to participate in our study, for the valuable information and insights they provided, and for their hospitality.

Foreign Governments

Several agencies responsible for delivering a variety of government services in Australia, New Zealand, and the United Kingdom participated in our study. The government services provided by the agencies range from providing audit oversight and tax collection activities to benefit administration and benefit payments.

Australia

The Australian Federation has a three-tier system of government, under the provisions of a written constitution that includes the legislative, executive, and judicial branches of government at both the national and state levels. The division of powers between the federal and state parliaments broadly follows the American model—states and territories are responsible for matters not assigned to the federal government. Australia is an independent nation and retains constitutional links with Queen Elizabeth II of Great Britain who is Queen of Australia. A Minister of State is accountable to Parliament for each department's functions and activities. Under the Minister is the head of a department, usually referred to as the Secretary.

Centrelink

Centrelink is a "one-stop shop" that pays a variety of Australian government benefits. Centrelink is an agency not individually funded by the Treasury, but rather through business partnership agreements with government departments. The agency has agreements with 11 government departments, including the Department of Family and Community Services (FACS); the Department of Employment, Workplace Relations and Small Business; the Department of Veterans' Affairs; and the Department of Education, Training and Youth Affairs. The one-stop shop was formed by merging functions and staff from the social security and employment departments with strong support from the Department of Finance. It is in the top one hundred of Australian companies in terms of size and turnover. Its budget is \$818 million, and it distributes \$22.4 billion social

security payments on behalf of FACS.¹² Centrelink has 6.1 million customers, pays 9.2 million individual entitlements each year, and employs a staff of 22,000 in 1,000 service delivery locations across Australia.

Health Insurance Commission

The Health Insurance Commission (HIC) is a government agency that administers Australian health programs such as Medicare and the Pharmaceutical Benefits Scheme. In addition to administering these programs, HIC is charged with preventing and detecting fraud and abuse. Medicare is a universal health insurance scheme available to all Australian citizens. From 1999 through 2000, HIC paid over \$3.5 billion in benefits, processing over 209 million claims to 11 million active enrollees in Medicare. Through the Pharmaceutical Benefits Scheme during the same year, HIC processed over 149 million claims totaling over \$1.8 billion in benefits.

New Zealand

New Zealand is an independent nation within the British Commonwealth. Queen Elizabeth II of Great Britain is represented in New Zealand by the Governor-General. New Zealand has no written constitution but rather it has two documents of importance—the Treaty of Waitangi and the Bill of Rights Act. Much of the business of government is performed by ministries, government departments, and other government agencies, which are collectively known as the public sector.

Inland Revenue Department

The Inland Revenue Department (IRD) provides tax services as well as social policy services, including the administration of child support and family assistance programs and the collection of student loan repayments. IRD revenues include \$7 billion in individual taxes, \$3.76 billion in Goods and Services Tax revenue, and \$1.85 billion in company tax. Total tax revenue in 1999 was \$13.5 billion. During the 1999/2000 year, IRD processed 7.2 million tax returns. Additionally, IRD processed 7.3 million payments during the same year.

Work and Income New Zealand

The Department of Work and Income New Zealand (WINZ) is a government agency that aids job seekers, pays income support, and administers superannuation (retirement) payments and student loans and allowances. WINZ was established in 1998 by combining the income support function from the Department of Social Welfare and the employment services and local employment coordination functions from

¹²Amounts included in this report have been converted to U.S. dollars using the following exchange rates, effective April 16, 2001, for one U.S. dollar: 0.697064 British pounds, 1.95665 Australian dollars, and 2.43533 New Zealand dollars.

the Department of Labor. Total benefits exceed \$5.34 billion in transfer payments to

- over 460,000 seniors for superannuation and transitional retirement benefits payments,
- over 404,000 people for income support payments,
- approximately 56,000 students for student allowances, and
- approximately 143,000 students for student loans.

United Kingdom

The United Kingdom is a constitutional monarchy and parliamentary democracy under Queen Elizabeth II and two houses of Parliament—the House of Lords and the House of Commons. The executive power rests with the Cabinet, headed by the Prime Minister.

National Audit Office

The National Audit Office (NAO) scrutinizes public spending on behalf of Parliament. It is an independent body that audits the accounts of all government departments and agencies, as well as a wide range of other public bodies, and reports to Parliament on the economy, efficiency, and effectiveness of government agencies.

NAO is headed by the Comptroller and Auditor General, who is also an officer of the House of Commons. NAO employs 750 people in offices throughout the United Kingdom.

Department of Social Security

The Department of Social Security administers the United Kingdom's welfare programs through four agencies—the Benefits Agency, Child Support Agency, War Pensions Agency, and Appeals Service Agency. The Benefits Agency administers programs such as Income Support and Jobseeker's Allowance Benefits. The Benefits Agency employs about 71,000 people and delivers more than 20 social security benefits, making payments in excess of \$156 billion each year.

Federal Agencies

Department of Health and Human Services—Health Care Financing Administration

The Department of Health and Human Services (HHS) is the U.S. government's principal agency for protecting the health of all Americans and providing essential human services. In addition to the Medicare and Medicaid programs, the department includes more than 300 hundred programs, covering a wide spectrum of activity from medical research, financial assistance to low-income families, to substance abuse treatment and prevention programs.

The Health Care Financing Administration (HCFA), one of HHS operating divisions, administers both the Medicare and Medicaid programs, which provide health care to about one in every four Americans.

Medicaid

Medicaid, established in 1965 by Title XIX of the Social Security Act, is a federal-state matching entitlement program that pays for medical assistance for certain vulnerable and needy individuals and families with low incomes and resources. In fiscal year 2000, it provided health care assistance to an estimated 33 million persons, at a cost of about \$118.6 billion to the federal government. HCFA is responsible for the overall management of Medicaid; however, each state is responsible for managing its own program. Within broad federal statutory and regulatory guidelines, each state (1) establishes its own eligibility standards, (2) determines the types and ranges of services, (3) sets the rate of payment for services, and (4) administers its own program.

Medicare Fee-for-Service

Authorized by Title XVIII of the Social Security Act in 1965, Medicare is the nation's largest health insurance program handling more than 900 million claims per year on behalf of elderly and disabled individuals at a cost of about \$214.6 billion in fiscal year 2000. Fee-for-service payments account for about \$173.6 billion of Medicare payments. HCFA contracts with over 50 insurance companies to process fee-for-service claims; however, HCFA is responsible for overseeing these contractors and for ensuring that claims are paid accurately and efficiently.

Social Security Administration

In 1935, the Social Security Act established a program to help protect aged Americans against the loss of income due to retirement. Since that time, various amendments were added, creating the programs that the Social Security Administration (SSA) administers today. Established in 1994 as an independent agency within the U.S. government, SSA is responsible for administering the Old Age and Survivors Insurance (OASI) and Disability Insurance (DI) programs as well as the Supplemental Security Income (SSI) program. SSA's organization features centralized management of the programs and a decentralized nationwide network of 10 regional offices overseeing 1,340 field offices, 138 hearings offices, 36 teleservice centers, 7 processing centers, and 1 data operations center. OASI provides for the protection of loss of income for aged Americans as well as survivors of deceased workers. OASI had fiscal year 2000 outlays of about \$347.9 billion, with about 39 million beneficiaries. DI protects disabled workers and their dependents from loss of income, and had fiscal year 2000 outlays of \$54.2 billion, serving about 6.6 million beneficiaries. Workers are considered disabled if they have severe physical or mental conditions that prevent them from engaging in substantial gainful activity. SSI had outlays of \$30.8 billion in fiscal year 2000, providing cash

assistance to about 6.6 million financially needy individuals who are elderly, blind, or disabled.

Department of Veterans Affairs

In 1930, the Congress consolidated and coordinated various veterans' programs with the establishment of the Veterans Administration. It became a cabinet-level position in March 1989—the Department of Veterans Affairs (VA). VA administers the laws providing benefits and other services to veterans and their dependents and beneficiaries. Through 21 organizations, including the Veterans Health Administration and the Veterans Benefits Administration, VA ensures that veterans receive medical care, benefits, and social support. Major programs of VA include medical care, education, research, compensation, pension, education, and burial. In fiscal year 2000, more than 3.8 million patients used VA health care, over 2.6 million veterans and family members received monthly VA disability compensation payments, and nearly 2.4 million graves were maintained at national cemeteries.

State Governments

The state agencies that participated in our study are responsible for administering a variety of benefit programs in Illinois, Kentucky, and Texas.

State of Illinois

The Illinois Department of Human Services (IDHS) was created in 1997 by consolidating three human services agencies, one of which was the Illinois Department of Public Aid (IDPA), and parts of three others. IDHS assumed the responsibility for administering cash assistance, food stamps, and Medicaid eligibility programs. However, IDPA retains most of the responsibility for administering Medicaid. IDPA has an Office of Inspector General (OIG) that helps enforce policies and investigates misconduct in the Medicaid, food stamp, and welfare programs administered by IDPA and IDHS. IDPA OIG includes a staff of 311 employees, and, in fiscal year 2000, it operated under a budget of \$19.6 million and collected or avoided costs totaling \$38.3 million. According to preliminary fiscal year 2000 data, Illinois' Food Stamp program provided approximately \$777 million in benefits to over 779,000 recipients. In fiscal year 1999, Illinois spent approximately \$390 million of its Temporary Assistance for Needy Families (TANF) funds. In fiscal year 1998, Illinois spent approximately \$6.2 billion for Medicaid covering over 1.3 million recipients.

Commonwealth of Kentucky

Kentucky's Cabinet for Families and Children protects and promotes the well being of Kentuckians by delivering quality human services. It administers the state's human services programs, such as food stamps, foster care, disability, and cash assistance. Meanwhile, the state's Cabinet for Health Services administers programs to promote mental and physical

health, emphasizing education and prevention. It administers Medicaid through the Department of Medicaid Services. According to preliminary fiscal year 2000 data, Kentucky's Food Stamp program provided approximately \$337 million in benefits to over 403,000 recipients. In fiscal year 1999, Kentucky spent approximately \$82 million of its TANF funds. In fiscal year 1998, Kentucky spent approximately \$2.4 billion for Medicaid covering over 644,000 recipients.

State of Texas

Texas has a number of departments involved in the administration of its medical and general assistance programs. Its Health and Human Services Commission (HHSC), which provides overall leadership and strategic direction to the health and human services system in Texas, oversees the work of 13 state agencies, including the Texas Department of Health (TDH) and the Texas Department of Human Services (TDHS). TDH administers more than 200 separate programs and operational units, including Medicaid. This department has more than 5,500 employees and an annual appropriation of approximately \$6.5 billion. TDHS administers state and federal human services programs, including TANF and the Food Stamp program, to more than 2 million needy, elderly, or disabled Texans each month. As one of the largest human services agencies in the country, TDHS employs more than 15,000 and has an annual budget of \$3.5 billion. According to fiscal year 2000 data, Texas' Food Stamp program provided approximately \$1.2 billion in benefits to over 1.3 million recipients. In addition, Texas spent approximately \$228 million of its TANF funds in serving more than 300,000 recipients. In fiscal year 1998, Texas spent approximately \$7.1 billion for Medicaid covering over 2.3 million recipients.

Private Sector Companies

Private Sector Council

The Private Sector Council (PSC) is a nonprofit, nonpartisan public service organization committed to assisting the federal government in improving its efficiency, management, and productivity. Since its founding in 1983, PSC has continued to promote and further the notion that private sector "know-how" can, and should, be utilized to assist in solving public sector challenges by supplying federal managers with modern ideas, methodologies, and applications through over 300 projects. Member companies consist of prominent Fortune 500 companies from across North America, including telecommunications, defense, finance, and energy businesses. PSC assembled three volunteer companies to participate in our study. These companies included a telecommunications company with \$33.6 billion in fiscal year 2000 sales, a document management company with \$18.6 billion in fiscal year 2000 sales, and a consulting firm with \$1.95 billion in revenues.

Other Resources

We identified the following Web sites during the course of our work, which may be useful to organizations as sources of additional information.

Best Practice Web Sites

Best Practices in the Federal Government

<http://hydra.gsa.gov/fitec/bestprac.htm>

The CFO Electronic Commerce Task Force has created an interagency team, the Financial Implementation Team for Electronic Commerce (FITEC), to help create integrated strategies, execution plans, and schedules for achieving the federal CFO financial community's electronic commerce goals. This site, created by FITEC, provides agencies with a resource for locating financial and/or electronic commerce practices that can be used throughout the federal government.

The Cabinet Office

www.cabinet-office.gov.uk/servicefirst/index/guidhome.htm

The United Kingdom's Cabinet Office works in partnership with other parts of the central government, local government, and other bodies in the public and private sectors to modernize and coordinate government in order to secure excellence in policymaking and responsive, high-quality public services. The Cabinet Office's best practices site includes a best practice database, best practice guides, best practice links, and different forums organizations can use to share information on their various initiatives.

National Association of State Procurement Officials

www.naspo.org

The National Association of State Procurement Officials is a nonprofit association dedicated to strengthening the procurement community through education, research, and communication. Under its "Whitepapers" section, this site includes a "Best Practices Compendium" that lists innovative procurement practices in state government.

Organisation for Economic Co-operation and Development

www.oecd.org/puma/focus/compend/matrixframe.htm

The Organisation for Economic Co-operation and Development provides a setting in which 30 member countries can discuss, develop, and perfect economic and social policy. Countries can compare experiences, seek answers to common problems, and work to coordinate domestic and international policies. This site provides examples of public management

initiatives in a variety of areas, including ethics, performance management, and regulatory reform.

Award Winners

Government Technology Leadership Awards

www.govexec.com/tech/award

Government Executive magazine annually presents Government Technology Leadership Awards to recognize federal agencies and state governments for their excellent performance with information technology programs. This site includes a list of all award winners and a searchable database of *Government Executive* articles.

National Association of State Information Resource Executives

www.nasire.org/awards/index.cfm

The National Association of State Information Resource Executives (NASIRE) represents state chief information officers (CIO) and information resource executives who share a mission to shape national information technology policy through collaborative partnerships, information sharing, and knowledge transfer. Each year, NASIRE presents Recognition Awards for Outstanding Achievement in the Field of Information Technology to those programs and systems that have created cost-effective, innovative solutions in the operation of state government. This site provides a list of award winners.

Publications

CIO Magazine

www.cio.com

CIO magazine aims to provide actionable insight and decision support for information technology and business executives so that they may use information technology to obtain a competitive advantage. This Web site includes discussion forums, research centers on topics such as leadership and management and data warehouses, and a searchable database.

Federal Computer Week

www.fcw.com

Federal Computer Week (FCW) is directed toward users and buyers of federal information technology. It focuses on desktop, client/server, and enterprisewide computing. This site can be used to access previous FCW articles, which can be searched by topic or by keyword.

Government Executive Magazine

www.govexec.com

Government Executive magazine provides daily news for federal managers and executives. This site provides information about the Government

Performance and Results Act, as well as links to research reports and organizations. In addition, articles from past issues can be searched by keyword.

Government Technology Magazine
www.govtech.net

Government Technology magazine is dedicated to providing government executives with key information they need to succeed in running modern government. This site provides a solution center containing best practices and case studies in state and local government.

Other Bookmarks

Australian National Audit Office
www.anao.gov.au

The Australian National Audit Office (ANAO) is a specialist public sector entity providing a full range of audit services to Parliament and Commonwealth public sector agencies and statutory bodies. ANAO's site includes links to its various publications, including its audit reports and better practice guides. These publications can be searched by title, theme, or date.

C.A. MacDonald & Associates
www.camacdonald.com

C.A. MacDonald & Associates, a health and human services consulting company, was established in 1993 to assist policy developers and decisionmakers in government in achieving their program and service goals. This site allows users to read the company's public reports that relate to various fraud and error programs in both the United States and Canada.

Center for Technology in Government
www.ctg.albany.edu

The Center for Technology in Government is an applied research center devoted to improving government and public services through policy, management, and technology innovation. The center's Web site includes information about its projects, research, and publications. Among the center's publications are a best practices starter kit, a report on data warehousing, and information on the center's project to find best practices in state and local information systems. This site also includes links to other related resources.

Chief Information Officers Council
www.cio.gov

The CIO Council was established in 1996. The CIO Council serves as the principal interagency forum for improving practices in the design,

modernization, use, sharing, and performance of federal agency information resources. This site contains a library of documents, a searchable database, and a discussion area.

The Data Warehousing Institute
www.dw-institute.com

The Data Warehousing Institute provides education and training in the data warehousing and business intelligence industry. The institute is dedicated to educating business and information technology professionals about the strategies, techniques, and tools required to successfully design, build, and maintain data warehouses. This site lists winners of its Best Practices and Leadership in Data Warehousing Awards. In addition, it provides case studies, lessons from experts, and a forum allowing users to share information or to ask questions.

Government Performance Project
www.maxwell.syr.edu/gpp/index.htm

The Government Performance Project is the joint effort of the Maxwell School of Citizenship and Public Affairs at Syracuse University and *Governing* magazine, which are working to rate the management capacity of local and state governments and selected federal agencies in the United States. This site includes reports on those rankings in addition to highlighted innovative practices.

Illinois Department of Public Aid's Office of Inspector General
www.state.il.us/agency/oig/index.htm

IDPA's Office of Inspector General's (OIG) mission is to prevent, detect, and eliminate fraud, waste, abuse, and misconduct in various payment programs. This site contains research reports conducted by the OIG, including the first ever payment accuracy review performed on Medicaid. This site also contains a searchable database of sanctioned providers and barred individuals within the state of Illinois.

National Medicaid Fraud and Abuse Initiative
www.hcfa.gov/medicaid/fraud/default.htm

HCFA began its National Medicaid Fraud and Abuse Initiative in June 1997. This initiative works to facilitate communication, information sharing, and a national forum for Medicaid fraud and abuse issues for the states. This Web site contains guidance and reports, including information about executive seminars conducted by Dr. Malcolm Sparrow, a leading authority in the area of health care fraud, and state Medicaid contacts.

Related Organizations

Association of Certified Fraud Examiners
www.cfenet.com

The Association of Certified Fraud Examiners consists of approximately 25,000 certified fraud examiners and associated members in 70 different countries. The association's mission is to reduce the incidence of fraud and white-collar crime through prevention and education. This site provides information about membership, events, and products and services offered by the association.

Association for Federal Information Resources Management
www.affirm.org

The Association for Federal Information Resources Management (AFFIRM) is a nonprofit, professional organization whose overall purpose is to improve the management of information, and related systems and resources, within the federal government. Founded in 1979, AFFIRM's members include information resource management professionals within the federal, academic, and industry sectors. This site contains information on membership, a calendar of events, and links to AFFIRM's publications.

Association of Government Accountants
www.agacgfm.org

The Association of Government Accountants (AGA) serves the professional interests of financial managers from local, state, and federal governments, as well as public accounting firms responsible for effectively using billions of dollars and other monetary resources every day. AGA is recognized as a leading advocate for improving the quality and effectiveness of government fiscal administration. Its Web site includes information on membership, conferences, and its publications.

Council for Excellence in Government
www.excelgov.org

The Council for Excellence in Government, whose members include former leaders in both government and the private sector, works toward practical public sector reform. This Web site provides information on the council's programs and publications.

Highway 1
www.highway1.org

Highway 1 is a nonprofit organization, made up of companies such as IBM and Microsoft, whose goal is to educate the government on the potential of information technology by being a source for information and by demonstrating technologies that are shaping our society, economy, and public policy. This Web site includes a list of Highway 1's programs and an information center.

Information Technology Resources Board
www.itrb.gov

The Information Technology Resources Board (ITRB) is a group of information technology, acquisition, and program managers and practitioners with significant experience in developing, acquiring, and managing information systems in the federal government. The primary focus of ITRB is to provide a review of major system initiatives at the joint request of the Office of Management and Budget and an agency and to publicize lessons learned and promising practices. This site includes a list of ITRB's members, events, publications, and related links.

The Institute of Internal Auditors
www.theiia.org

Established in 1941, the Institute of Internal Auditors serves as the profession's watchdog and resource on significant auditing issues around the globe. This site provides standards, guidance, and information on internal auditing best practices for its members.

National Contract Management Association
www.ncmahq.org

The mission of the National Contract Management Association (NCMA) is to help contract managers best achieve their objectives to manage customer and supplier expectations and relationships, control risk and cost, and contribute to organizational profitability and success. This site contains information about NCMA's member services, event calendar, publications, and professional resources.

National Health Care Anti-Fraud Association
www.nhcaa.org

Founded in 1985 by several private health insurers and federal/state law enforcement officials, the National Health Care Anti-Fraud Association is a unique, issue-based organization comprising private and public sector organizations and individuals responsible for the detection, investigation, prosecution, and prevention of health care fraud. This site includes information on upcoming education and training events.

Private Sector Council
www.privatesectorcouncil.org

The Private Sector Council (PSC) is a nonprofit, nonpartisan public service organization committed to helping the federal government improve its efficiency, management, and productivity. This site provides information about PSC's upcoming events.

Standards Australia
www.standards.com.au

Standards Australia International Limited is an organization with principal activities focused on business-to-business services based on the creation, distribution, sharing, and application of knowledge using a variety of technologies. One of the major activities of the organization is the development of technical and business standards. This site provides a means of acquiring the Australian/New Zealand Standard 4360: *Risk Management*.

GAO Contacts and Staff Acknowledgments

GAO Contacts

Tom Broderick, (202) 512-8705

Marie Novak, (202) 512-4079

Staff Acknowledgments

In addition to those named above, the following individuals made important contributions to this report: Cheryl Driscoll, Valerie A. Freeman, Sharon Loftin, Elizabeth Martinez, Mary Merrill, Debra Sebastian, Ruth Sessions, Brooke Whittaker, and Maria Zacharias.

(916360)

Ordering Information

The first copy of each GAO report is free. Additional copies of reports are \$2 each. A check or money order should be made out to the Superintendent of Documents. VISA and MasterCard credit cards are accepted, also.

Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:
U.S. General Accounting Office
P.O. Box 37050
Washington, DC 20013

Orders by visiting:
Room 1100
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders by phone:
(202) 512-6000
fax: (202) 512-6061
TDD (202) 512-2537

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

Orders by Internet:
For information on how to access GAO reports on the Internet, send an e-mail message with "info" in the body to:

info@www.gao.gov

or visit GAO's World Wide Web home page at:

<http://www.gao.gov>

To Report Fraud, Waste, or Abuse in Federal Programs

Contact one:

- Web site: <http://www.gao.gov/fraudnet/fraudnet.htm>
- e-mail: fraudnet@gao.gov
- 1-800-424-5454 (automated answering system)

**United States
General Accounting Office
Washington, D.C. 20548-0001**

**Presorted Standard
Postage & Fees Paid
GAO
Permit No. GI00**

**Official Business
Penalty for Private Use \$300**

Address Correction Requested

