GTAG®

GLOBAL TECHNOLOGY AUDIT GUIDE

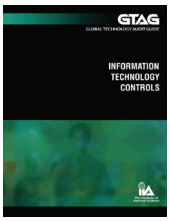
IPPF – Practice Guide

Fraud Prevention and Detection in an Automated World

The Institute of Internal Auditors

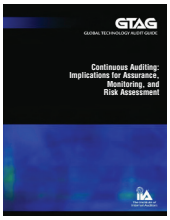
Global Technology Audit Guide (GTAG)

Written in straightforward business language to address a timely issue related to IT management, control, and security, the GTAG series serves as a ready resource for chief audit executives on different technology-associated risks and recommended practices.

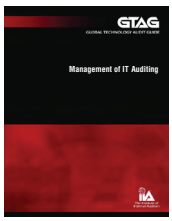


Information Technology Controls: Topics discussed include IT control concepts, the importance of IT controls, the organizational roles and responsibilities for ensuring effective IT controls, and risk analysis and monitoring techniques.

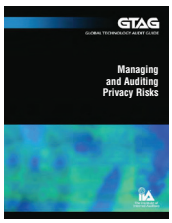
Change and Patch Management Controls: Describes sources of change and their likely impact on business objectives, as well as how change and patch management controls help manage IT risks and costs and what works and doesn't work in practice.



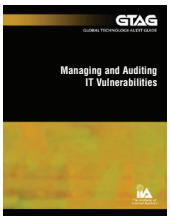
Continuous Auditing: Addresses the role of continuous auditing in today's internal audit environment; the relationship of continuous auditing, continuous monitoring, and continuous assurance; and the application and implementation of continuous auditing.



Management of IT Auditing: Discusses IT-related risks and defines the IT audit universe, as well as how to execute and manage the IT audit process.

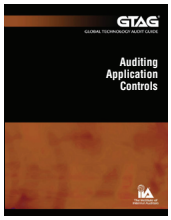


Managing and Auditing Privacy Risks: Discusses global privacy principles and frameworks, privacy risk models and controls, the role of internal auditors, top 10 privacy questions to ask during the course of the audit, and more.



Managing and Auditing IT Vulnerabilities: Among other topics, discusses the vulnerability management life cycle, the scope of a vulnerability management audit, and metrics to measure vulnerability management practices.

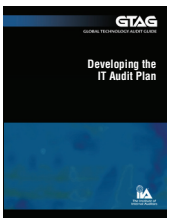
Information Technology Outsourcing: Discusses how to choose the right IT outsourcing vendor and key outsourcing control considerations from the client's and service provider's operation.



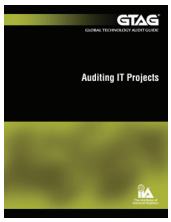
Auditing Application Controls: Addresses the concept of application control and its relationship with general controls, as well as how to scope a risk-based application control review.

Identity and Access Management: Covers key concepts surrounding identity and access management (IAM), risks associated with IAM process, detailed guidance on how to audit IAM processes, and a sample checklist for auditors.

Business Continuity Management: Defines business continuity management (BCM), discusses business risk, and includes a detailed discussion of BCM program requirements.



Developing the IT Audit Plan: Provides step-by-step guidance on how to develop an IT audit plan, from understanding the business, defining the IT audit universe, and performing a risk assessment, to formalizing the IT audit plan.



Auditing IT Projects: Provides an overview of techniques for effectively engaging with project teams and management to assess the risks related to IT projects.

Visit The IIA's Web site at www.theiia.org/technology to download the entire series.

Global Technology Audit Guide (GTAG®) 13

Fraud Prevention and Detection in an Automated World

December 2009

Table of Contents

Foreword

Thanks to unrelenting technological advancements, virtually everything we encounter is embedded with technology. Regardless of the industry or enterprise, IT is critical to maintaining a competitive edge, managing risks, and achieving business objectives; and organizations worldwide are allocating vast resources to vital technological projects.

As technology is advancing, so are schemes to commit fraud. The reliance on automated tools to help perpetuate these schemes provides new challenges in the detection and prevention of fraud.

Fraud, according to *Black's Law Directory*, consists of "all multifarious means that human ingenuity can devise which are resorted to by one individual to get an advantage over another by false suggestions or suppression of the truth." Fraud is costly to organizations and is bad for the economy. Technology enables fraudsters to commit and conceal traditional fraud schemes more easily. For example: Fraudsters can easily produce a fake document, such as an account statement, to deceive others.

Technology is also a tool that can help prevent and detect fraud. By using technology to implement real-time fraud prevention programs and advanced fraud detection tools, organizations can reduce the time it takes to detect fraud, thereby reducing the cost of fraud.

It is imperative that auditors stay ahead of fraudsters in their knowledge of technology and available tools. With readily available software, using computers to isolate accounting fraud clues not only makes sense, it is an absolute necessity if auditors are to help fulfill their duty of independent oversight.

For all of these reasons, I am especially pleased with the release of The IIA's new GTAG *13: Fraud Prevention and Detection in an Automated World*. This timely guidance provides an overview of techniques for effectively engaging with teams and management to assess the risks related to fraud, given the advancements in technology. This Practice Guide includes:

- An explanation of the various types of data analysis to use in detecting fraud.
- A variety of IT fraud risks.
- A technology fraud risk assessment template.

I encourage you to use this authoritative guidance to strengthen your knowledge of the integration of technology and fraud, for it surely will contribute to the success of your organization's fraud detection efforts!

Scott Grossfeld, CFE, CPA
Chief Executive Officer
Association of Certified Fraud Examiners

Executive Summary

Fraud is a business risk that executives, especially chief audit executives (CAEs), have had to deal with for a long time. Numerous headlines have highlighted corporate scandals and wrongdoing that demonstrate the need for organizations and governments to improve governance and oversight. How to address fraud risk within an organization effectively and efficiently is a major topic of concern for boards of directors, management, business owners, internal auditors, government leaders, legislators, regulators, and many other stakeholders. In many cases, new laws and regulations from around the world have forced organizations to take a fresh look at this longstanding problem.

Despite the fact that many internal audit organizations are faced with tight budgets, limited staffing, and extended workloads, today's audit professionals are expected to take a proactive role in helping organizations manage fraud risks by ensuring that appropriate controls are in place to help prevent and detect fraud. To meet the expectations of management, business owners, and boards of directors, CAEs are challenged to use their available resources effectively and efficiently. To this end, internal auditors require appropriate skills and should use available technological tools to help them maintain a successful fraud management program that covers prevention, detection, and investigation. As such, all audit professionals — not just IT audit specialists — are expected to be increasingly proficient in areas such as data analysis and the use of technology to help them meet the demands of the job.

In addition to evaluating the adequacy of internal controls, a challenge for internal auditors is to look beyond the controls and find loopholes in systems where fraud could occur. With an understanding of the relationships among different IT systems and applications, internal auditors can apply their critical thinking to identify high-risk areas and drill down to specific transactions.

The purpose of this GTAG is to supplement The IIA's Practice Guide, Internal Auditing and Fraud, and to inform and provide guidance to CAEs and internal auditors on how to use technology to help prevent, detect, and respond to fraud. The guide focuses on IT fraud risks, IT fraud risk assessments, and how the use of technology can help internal auditors and other key stakeholders within the organization address fraud and fraud risks.

1. Introduction

The objective of this chapter is to present the fraud-related standards published in The IIA's International Professional Practices Framework (IPPF). The chapter also defines fraud and provides an overview of the ways in which technology can be implemented to improve fraud prevention and detection.

1.1 Definition of Fraud

Fraud encompasses a wide range of irregularities and illegal acts characterized by intentional deception or misrepresentation. The IIA's IPPF defines *fraud* as:

> *"… any illegal act characterized by deceit, concealment, or violation of trust. These acts are not dependent upon the threat of violence or physical force. Frauds are perpetrated by parties and organizations to obtain money, property, or services; to avoid payment or loss of services; or to secure personal or business advantage."*

This broad definition of fraud accommodates the fraud risks, exposures, and threats encountered within IT departments as well as frauds enabled by the use of technology.

1.2 The IIA's Fraud-related Standards

As noted in The IIA's Practice Guide, Internal Auditing and Fraud, The IIA has included standards that directly relate to fraud within the IPPF. The following standards cover internal auditors' roles and responsibilities pertaining to fraud within an organization.

1210.A2 — Internal auditors must have sufficient knowledge to evaluate the risk of fraud and the manner in which it is managed by the organization, but are not expected to have the expertise of a person whose primary responsibility is detecting and investigating fraud.

1220.A1 — Internal auditors must exercise due professional care by considering the:

- Extent of work needed to achieve the engagement's objectives.
- Relative complexity, materiality, or significance of matters to which assurance procedures are applied.
- Adequacy and effectiveness of governance, risk management, and control processes.
- Probability of significant errors, fraud, or noncompliance.
- Cost of assurance in relation to potential benefits.

2060—Reporting to Senior Management and the Board— The chief audit executive (CAE) must report periodically to senior management and the board on the internal audit activity's purpose, authority, responsibility, and performance relative to its plan. Reporting must also include significant risk exposures and control issues, including fraud risks, governance issues, and other matters needed or requested by senior management and the board.

2120.A2 — The internal audit activity must evaluate the potential for the occurrence of fraud and the manner in which the organization manages fraud risk.

2210.A2 — The internal auditors must consider the probability of significant errors, fraud, noncompliance, and other exposures when developing the engagement objectives.

1.3 Using Technology to Prevent and Detect Fraud

Advances in technology increasingly are allowing organizations to implement automated controls to help prevent and detect fraud. Technology also allows organizations to move from static or periodic fraud monitoring techniques, such as detective controls, to continuous, real-time fraud monitoring techniques that offer the benefit of actually preventing fraud from occurring. This GTAG describes both periodic and continuous monitoring techniques. Numerous advanced analytical software packages are now available to assist in data analysis. This GTAG addresses techniques in general, and does not endorse any specific platform.

Computer forensic technology and software packages are available to assist in the investigation of fraud — where computers are used to facilitate the fraud — or to identify red flags of potential fraud. Computer forensics is an investigative discipline that includes the preservation, identification, extraction, and documentation of computer hardware and data for evidentiary purposes and root cause analysis. Examples of computer forensic activities include:

- Recovering deleted e-mails.
- Monitoring e-mails for indicators of potential fraud.
- Performing investigations after terminations of employment.
- Recovering evidence after formatting a hard drive.

Computer forensic activities help establish and maintain a continuing chain of custody, which is critical in determining admissibility of evidence in courts. Although the CAE and internal auditors are not expected to be experts in this area, the CAE should have a general understanding of the benefits this technology provides so that he or she may engage appropriate experts, as necessary, for assistance with a fraud investigation.

2. IT Fraud Risks

The objective of this chapter is to provide information on various IT fraud scenarios that may take place within an organization. Although many audit executives, board directors, and management likely already have a working knowledge of specific IT fraud risks and exposures within their own organization, this chapter discusses the types of fraud in general terms. Therefore, it may not address situations unique to specific industries or organizations.

2.1 IT Fraud Risk Assessments

As stated in The IIA's Practice Guide, Internal Auditing and Fraud, all organizations are exposed to fraud risk in any process where human involvement is required. An organization's exposure to fraud is a function of the fraud risks inherent in the business; the extent to which effective internal controls to prevent or detect fraud are present; and the honesty and integrity of those involved in the process. These fraud risks and exposures apply to IT just as often as any other area of the organization.

The IPPF's risk management standard (2120.A2) indicates that the internal audit activity must evaluate the potential for the occurrence of fraud and the manner in which the organization manages fraud risk. Although there are various ways to meet this standard, it's important for internal auditors to validate that:

- Management has completed an enterprise fraud risk assessment.
- All significant areas of the organization were included in the assessment.
- Key elements such as fraud risks, controls, and gaps were documented.
- A process is in place for remediation efforts.

An IT fraud risk assessment is often a component of an organization's larger enterprise risk management program. As management is responsible for (ERM) programs, IT management should focus efforts on successfully completing the IT fraud risk assessment. In many organizations, internal auditors may be asked to participate in these assessments because of the unique skill sets they offer in identifying and assessing risks. The IT fraud risk assessment is a tool that assists IT management and internal auditors in systematically identifying where and how fraud may occur and who may be in a position to commit fraud. A review of potential fraud exposures represents an essential step in addressing IT management's concerns about IT fraud risks. Similar to an enterprise risk assessment, an IT fraud risk assessment concentrates on fraud schemes and scenarios to determine the presence of internal controls and whether the controls can be circumvented.

An IT fraud risk assessment usually includes the following key steps:

- Identifying relevant IT fraud risk factors.
- Identifying potential IT fraud schemes and prioritizing them based on likelihood and impact.
- Mapping existing controls to potential fraud schemes and identifying gaps.
- Testing operating effectiveness of fraud prevention and detection controls.
- Assessing the likelihood and business impact of a control failure and/or a fraud incident.

The following pages include an illustrative template of an IT fraud risk assessment:

Business Owner	Fraud Risks	Controls	Preventive or Detective	Monitoring	Likelihood	Impact
IT — CIO	Insufficient physical controls over IT hardware results in changes, destruction, or misappropriation for personal gain. (Physical Security)	• Critical computer hardware located in secured data centers. • Access to data centers restricted based on job responsibilities. • Various security schemes used, (e.g., key card access, closed. circuit camera surveillance, security guards). • Policies and procedures documented. • Visitor logs maintained. • Security cables used for laptop computers. • Inventory of workstations performed quarterly. • Formal provisioning procedures.	Both	• Data center management. • Loss prevention. • IT risk management. • IT operations. • Daily monitoring of visitor logs by management. • Periodic inventories completed by asset management. • Financial reconciliations of provisioning. • Internal auditing.	Low	High

IT — CIO	Access to systems or data for personal gain. (Logical Access)
	a) Access to customers' or employees' personal information (e.g., credit card information, payroll information). (Identity Theft)
	b) Access to confidential company information (e.g., financial reporting, supplier data, strategic plans).
	c) Copying and use of software or data for distribution.
	(continued)
		• Identity management:
		  ○ Individual user IDs assigned.
		  ○ Automated password complexity rules.
		  ○ Password rotation.
		• Access controls.
		• Authentication controls.
		• Authorization controls:
		  ○ Business owners approve access to data.
		  ○ Access control lists.
		• Documented policies and procedures
		• Segregation of duties.
		• Computer incident response team.
		• Network controls (e.g., firewalls, routers).
		• Secure remote access.
		• Anti-virus and patch management to control computer vulnerabilities.
		• System administrator IDs restricted.
		• Network penetration test completed.
		• Periodic software vulnerability assessments.
		• Procedures to delete terminated employees from access to network resources.
		(continued)
			Both	• Information security.
				• System administrators.
				• Business owners.
				• Internal auditing.
					Med	High

Table 1. IT Fraud Risk Assessment Illustrative Template

Business Owner	Fraud Risks	Controls	Preventive or Detective	Monitoring	Likelihood	Impact
IT — CIO	d) Access to audit logs or other monitoring devices used to detect problems for resolution. e) Abuse of telecommunications network.	• Account reconciliations and review. • Security violations logged and available for review. • Restricted access to software code. • Fictitious data used for system testing. • Dedicated and encrypted lines for transmitting personal information. • Secure Sockets Layer (SSL) encryption for online transactions.				
IT — CIO	Changes to system programs or data for personal gain. (Change Management)	• System development and project management procedures. • System change management procedures. • Segregation of duties. • Restricted access to production environment. • Management approval required for system changes. • Restricted access to software code. • Account reconciliations and review.	Both	• IT management. • System administrators. • Business owners. • Finance management. • Internal auditing.	Low	Med
IT — CIO	Fraudulent activity by an independent contractor or an off-shore programmer (e.g., fictitious billings; misappropriation of employee, customer, or company confidential data for personal gain).	• Terms of contract (e.g., confidential information, no disclosure, return of confidential information, right to audit). • Restricted access based on job responsibilities. • Access controls (e.g., authentication and authorization). • Security violations are logged and available for review. • Account reconciliations and review. • Monthly review of contractor charges. • Segregation of duties. • Management approval required.	Both	• IT management. • Information security. • Loss prevention. • Internal auditing.	Low	Med

Table 1. IT Fraud Risk Assessment Illustrative Template (continued)

Business Owner	Fraud Risks	Controls	Preventive or Detective	Monitoring	Likelihood	Impact
IT — CIO	Conflicts of interest with suppliers and third parties.	• Hotline number. • Segregation of duties. • Competitive bidding. • Annual communication to suppliers and employees (tone at top). • Business ethics statement. • Appropriation committee – capital expenditures. • Formal list of approved vendors. • Financial controls. • Background checks.	Both	• Ethics committee. • Human resources. • Loss prevention. • Procurement. • Finance. • Internal auditing.	Low	Med
IT — CIO	Copyright infringement (e.g., downloading or copying files illegally).	• Peer-to-peer connections blocked. • Software that identifies installed software on workstations and servers. • Documented policies and procedures. • Restricted access to physical media and software installation files.	Both	• IT operations. • Information security. • Internal auditing.	Med	Med
IT — CIO	Misappropriation of company data by third parties (e.g., employee and customer information, company confidential information).	• Terms of contract (e.g., confidential information, privacy language, no disclosure, return of confidential information, right to audit). • Seeding customer files.	Both	• Business owners. • Information security. • Internal auditing.	Low	Low

Table 1. IT Fraud Risk Assessment Illustrative Template (continued)

2.2 Assessing Fraud Schemes

The following are two approaches to assessing fraud schemes from the fraudster's perspective:[1]

- **The control weaknesses approach** — Looks at the potential for fraud by examining the key controls, determining who could take advantage of a control weakness, and determining how he or she could circumvent a control that may not be working properly.
- **The key fields approach** — Looks at the potential for fraud by considering the data being entered, which fields could be manipulated (and by whom), and what would be the effect.

Both approaches seek to determine who could be committing fraud, what the fraudster could be doing, and what the symptoms of fraud would look like in the data. Brainstorming with employees from key business areas is a good technique for assessing fraud and is useful with both of these approaches.

2.3 IT Fraud Schemes

As internal auditing assesses the organization's efforts to complete a comprehensive fraud risk assessment, it is important that potential fraud schemes related to IT be identified and included in the enterprisewide risk assessment. One of the first steps in accomplishing this mission is to identify those individuals within the organization who could complete the assessment effectively. Key participants to consider include

[1] Coderre, David G., *Computer Aided Fraud Prevention and Detection: A Step-by-Step Guide*, John Wiley & Sons, 2009.

IT management, information security managers, IT risk managers, loss prevention managers, compliance managers, and others with skills that add value to the process. If the organization does not have sufficient internal knowledge of fraud assessment, it may want to consider cultivating this talent through professional development of existing employees. In some cases, it may be necessary for the organization to go to an outside source for assistance to help complete a quality IT fraud risk assessment.

The following general fraud scenarios should be considered and addressed, if applicable to the organization.

Access to Systems or Data for Personal Gain

Some of the most valuable information desired by individuals perpetrating a fraud in the IT area resides in the form of digital assets maintained by the organization. Therefore, it is critical for organizations to include this area in their fraud risk assessment. Most organizations collect, create, use, store, disclose, and discard information that has market value to others outside the organization. This data can be in the form of employee or customer personal information, such as government issued identification numbers, social identification numbers, bank account numbers, credit card numbers, checking account numbers, bank routing numbers, and other personal information. Whether the perpetrator is an individual with authorized access to the data or a hacker, this information can be sold to others or used for personal gain for crimes such as identity theft, unauthorized purchases on stolen credit cards, counterfeiting of credit cards, or stealing or diverting money from a bank account.

Insiders, by virtue of having legitimate access to their organizations' information, systems, and networks, pose a significant risk to employers. Employees experiencing financial problems may be tempted to use the systems they access at work every day to commit fraud. Employees motivated by financial problems, greed, revenge, the desire to obtain a business advantage, or the wish to impress a new employer, may choose to steal confidential data, proprietary information, or intellectual property from their employers. Furthermore, technical employees can use their technical abilities to sabotage their employers' systems or networks in revenge for negative work-related events.[2]

The following examples illustrate how inappropriate access to systems or data resulted in personal gain or system destruction.

- *An employee of a telecommunications firm's payroll department moved to a new position within the department in which she no longer would be required to have privileged access to payroll accounts. Upon switching positions, the employee's access rights to the payroll accounts were left unchanged. An associate told her that he was starting up a financial services business and needed some contact information. Using the privileged access rights that she had retained, the employee provided her associate with confidential information for 1,500 of the firm's employees, including 401k account numbers, credit card account numbers, and social security numbers, which he then used to commit more than 100 cases of identity theft. The insider's actions caused more than US $1 million worth of damages to the company and its employees.*[3]
- *A database analyst for a major check authorization and credit card processing company exceeded his authorized computer access. The employee used his computer access to steal the consumer information of 8.4 million individuals. The stolen information included names and addresses, bank account information, and credit and debit card information. He sold the data to telemarketers over a five-year period. A U.S. district judge sentenced him to 57 months' imprisonment and US $3.2 million in restitution for conspiracy and computer fraud.*[4]
- *An IT consultant was working under contract for an offshore oil platform company. After the company declined to offer him permanent employment, he illegally accessed the company's computer systems and caused damage by impairing the integrity and availability of data. He was indicted on federal charges, which carry a maximum statutory penalty of 10 years in federal prison.*[5]

[2] "The, Big Picture, of Insider IT Sabotage Across U.S. Critical Infrastructures." Carnegie Mellon, May 2008.

[3] "Insider Threat Study: Illicit Cyber Activity in the Information Technology and Telecommunications Sector." U.S. Secret Service and CERT Coordination Center/SEI, January 2008.

[4] U.S. Department of Justice Web site, Computer Crime and Intellectual Property Section, http://usdoj.gov/criminal/cybercrime, 2009.

[5] U.S. Department of Justice Web site, Computer Crime and Intellectual Property Section, http://usdoj.gov/criminal/cybercrime, 2009.

Other potential IT fraud schemes in this category include copying and distributing proprietary software for personal gain and accessing and using confidential company information such as financial reports, vendor information, or strategic business plans for personal gain. For example, a disgruntled or fired employee may copy and illegally distribute or sell proprietary software. The perpetrator may then attempt to cover his or her tracks by altering or deleting audit logs and changing other monitoring devices used to detect problems.

Changes to System Programs or Data for Personal Gain

If the organization has control breakdowns or weaknesses in the systems development life cycle, opportunities exist for fraud. The examples in Table 2 — Fraud in Systems Development[6] help demonstrate how fraud may occur in each of the system development phases.

[6] "Insider Threat Study: Illicit Cyber Activity in the Information Technology and Telecommunications Sector." U.S. Secret Service and CERT Coordination Center/SEI, January 2008.

Phase	Fraud	Oversights
Requirements Definition Phase	• 195 illegitimate drivers' licenses are created and sold by a police communications officer who accidentally discovers she can create them.	• Ill-defined authentication and role-based access control requirements. • Ill-defined security requirements for automated business processes. • Lack of segregation of duties.
System Design Phase	• A special function to expedite handling of cases allows two caseworkers to pocket US $32,000 in kickbacks. • An employee realizes there is no oversight in his company's system and business processes, so he works with organized crime to enter and profit from US $20 million in fake health insurance claims.	• Insufficient attention to security details in automated workflow processes. • Lack of consideration for security vulnerabilities posed by authorized system overrides.
System Implementation Phase	• An 18-year old former Web developer uses backdoors he inserted into his code to access his former company's network, spam its customers, alter its applications, and ultimately put the company out of business.	• Lack of code reviews.
System Deployment Phase	• A computer technician uses his unrestricted access to customers' systems to plant a virus on their networks that brings the customers' systems to a halt. • A software engineer deliberately creates no documentation or backups for his source code, and then deletes the only copy of the source code once the system is in production.	• Lack of enforcement of documentation practices and back-up procedures. • Unrestricted access to all customers' systems.
System Maintenance Phase	• A foreign currency trader covers up losses of US $691 million over a five-year period by making unauthorized changes to the source code. • A logic bomb sits undetected for six months before finally performing a mass deletion of data on a telecommunications firm.	• Lack of code reviews. • End-user access to source code. • Ineffective back-up processes, which amplified the impact of mass deletion of data.

Table 2. Fraud in Systems Development

Other IT fraud vulnerabilities that should be considered during the risk assessment include:

- Fictitious billings for services or misappropriation of employee, customer, or company confidential data for personal gain by an independent contractor or an onshore or offshore programmer.
- Copyright infringement and loss of intellectual property when employees or contractors copy or download files illegally.
- Misappropriation of company data by third-party service providers that process employee and/or customer information, or other company confidential information.

The following are some examples of best practices in addressing IT fraud risks.

- Completing periodic enterprise wide IT fraud risk assessments.
- Instituting periodic security and fraud awareness training for all employees.
- Enforcing segregation of duties.
- Restricting access to systems and data on a business need to know.
- Implementing strict password and identity management policies and practices.
- Logging, monitoring, and auditing employees' network actions.
- Using extra caution with system administrators and privileged users.
- Using layers of defense against network intrusions.
- Developing an effective incident response plan and assembling an incident response team.
- Deactivating computer access upon an employee's termination of employment.
- Collecting and saving forensic data for use in investigations.
- Allowing for secure back-up and recovery processe.
- Implementing good vulnerability management programs.

3. Fraud Detection Using Data Analysis

The objective of this chapter is to assist internal auditors in taking a proactive role in addressing fraud by using data analysis techniques. The chapter covers in detail why data analysis technology is important, specific analytical techniques that have proven to be highly effective, typical types of fraud tests, the importance of analyzing full data populations, fraud detection program strategies, and analyzing data using external and internal data sources.

3.1 Why Use Data Analysis for Fraud Detection?

Data analysis technology enables auditors and other fraud examiners to analyze transactional data to obtain insights into the operating effectiveness of internal controls and to identify indicators of fraud risk or actual fraudulent activities. Whether used to review payroll records for fictitious employees, or accounts payable transactions for duplicate invoices, data analysis technology can assist internal auditors in addressing fraud risks within an organization.

To test and monitor internal controls effectively, organizations should analyze all relevant transactions against control parameters, across all systems and all applications. Examining transactions at the source level helps assure the integrity and accuracy of the information.

Key factors that determine whether the auditor can rely on the data, or whether more data integrity testing is required include:

- The auditor's familiarity with the source data.
- The general and application controls.
- The reliance being placed on the data.
- The existence of corroborating evidence.

The first test of the data should be to verify its completeness and integrity. The completeness and integrity of the data is of paramount importance when dealing with potential fraud, because absent records or blank fields could falsely indicate fraud or cause potential frauds to go unnoticed. Then, additional tests should be performed to contribute to the auditor's understanding of the data and to search for symptoms of fraud in the data.[7]

3.2 Analytical Techniques for Fraud Detection

A number of specific analytical techniques have been proven highly effective in detecting fraud. Audit departments should consider these various techniques when evaluating the use of technology in fraud detection:

- Calculation of statistical parameters (e.g., averages, standard deviations, highest and lowest values) – to identify outlying transactions that could be indicative of fraudulent activity.
- Classification — to find patterns and associations among groups of data elements.
- Stratification of numeric values — to identify unusual (i.e., excessively high or low) values.
- Digital analysis using Benford's Law — to identify statistically unlikely occurrences of specific digits in randomly occurring data sets.
- Joining different data sources — to identify inappropriately matching values such as names, addresses, and account numbers in disparate systems.
- Duplicate testing — to identify simple and/or complex duplications of business transactions such as payments, payroll, claims, or expense report line items.
- Gap testing — to identify missing numbers in sequential data.
- Summing of numeric values — to check control totals that may have been falsified.
- Validating data entry dates — to identify postings or data entry times that are inappropriate or suspicious.

According to a 2008 white paper[8] by ACL Services Ltd., to maximize the effectiveness of data analysis in fraud detection, the technology employed should enable auditors to:

- Compare data and transactions from multiple IT systems (and address control gaps that often exist within and between systems).
- Work with a comprehensive set of fraud indicators.
- Analyze all transactions within the target area.
- Perform the fraud detection tests on a scheduled basis and provide timely notification of trends, patterns, and exceptions.

3.3 Typical Types of Fraud Tests

The data analysis techniques described above can be applied to a vast number of areas within an organization. The prioritization of where to look needs to be done in conjunction with a fraud risk assessment process. Table 3 — Fraud Detection Tests offers examples of some of the fraud detection tests that can be performed using data analysis.

[7] Coderre, David G. *Fraud Analysis Techniques Using ACL.* John Wiley & Sons, 2009.

[8] "Analyze Every Transaction in the Fight Against Fraud: Using Technology for Effective Fraud Detection." ACL Services Ltd., 2008.

Type of Fraud	Tests Used to Discover This Fraud
Fictitious vendors	• Run checks to uncover post office boxes used as addresses and to find any matches between vendor and employee addresses and/or phone numbers. • Be alert for vendors with similar sounding names or more than one vendor with the same address and phone number.
Altered invoices	• Search for duplicates. • Check for invoice amounts that do not match contracts or purchase order amounts.
Fixed bidding	• Summarize contract amount by vendor, and compare vendor summaries for several years to determine whether a single vendor is winning most bids. • Calculate days between close for bids and contract submission date by vendor to see whether the last bidder consistently wins the contract.
Goods not received	• Search for purchase quantities that do not agree with contract quantities. • Check whether inventory levels are changing in relation to supposed delivery of goods.
Duplicate invoices	• Review for duplicate invoice numbers, duplicate dates, and duplicate invoice amounts.
Inflated prices	• Compare prices across vendors to see whether prices from a particular vendor are unreasonably high.
Excess quantities purchased	• Review for unexplained increases in inventory. • Determine whether purchase quantities of raw materials are appropriate for production level. • Check to see whether increases in quantities ordered compare similarly to previous contracts or years or compare to other plants.
Duplicate payments	• Search for identical invoice numbers and payment amounts. • Check for recurring requests for refunds for invoices paid twice.
Carbon copies	• Search for duplicates within all company checks cashed. • Conduct a second search for gaps in check numbers.
Duplicate serial numbers	• Determine whether high-value equipment a company already owns is being repurchased by checking for duplicate serial numbers and for the involvement of the same personnel in both purchasing and shipping processes.
Payroll fraud	• Check whether a terminated employee is still on payroll by comparing the date of termination with the pay period covered by the paycheck, and extract all pay transactions for departure date less than the date of the current pay period.
Accounts payable	• Find transactions that do not match contract amounts by linking accounts payable files to contract and inventory files and examining contract date, price, ordered quantity, inventory receipt quantity, invoice quantity, and payment amount by contract.

Source: Computer *Aided Fraud Prevention and Detection: A Step-by-Step Guide*[9], by David Coderre.

Table 3. Fraud Detection Tests

[9] Coderre, David G. *Computer Aided Fraud Prevention and Detection: A Step-by-Step Guide*. John Wiley & Sons, 2009.

For analytical tests that rely on the access and use of personal and/or sensitive information, auditors must exercise due care in safeguarding that information. Organizations must also ensure that a privacy risk assessment is carried out for those instances where the use of personal information is restricted by local legislation. For additional information on this topic, refer to The IIA's *GTAG 5: Managing and Auditing Privacy Risks*.[10]

3.4 Analyzing Full Data Populations

For fraud detection programs to be effective, the fraud detection techniques listed in the previous section must be performed against full data populations. Although sampling data is a valid and effective audit approach, it is not necessarily appropriate for fraud detection purposes. When only partial data is tested, it is likely that a number of control breaches and suspicious transactions will be missed; the impact of control failures may not be quantified fully; and smaller anomalies may be missed. It is often these small anomalies that point to weaknesses that can be exploited, causing a material breach.

Analyzing the data against full data populations provides a more complete picture of potential anomalies. Random sampling is most effective for identifying problems that are relatively consistent throughout the data population; fraudulent transactions, by nature, do not occur randomly.

3.5 Fraud Prevention and Detection Program Strategies

Rather than take a reactive approach to fraud detection by relying solely on tips and whistleblower programs, organizations should take a proactive approach to fighting fraud. Their approach should include an evaluation by internal auditing of the operating effectiveness of internal controls, along with an analysis of transaction-level data for specific fraud indicators.

A fraud prevention and detection program should incorporate a spectrum of transactional data analysis — ranging from ad hoc, to repetitive, to continuous. Based on key risk indicators, ad hoc testing will pinpoint areas for further investigation. If initial testing reveals control weaknesses or suspected incidences of fraud, repetitive testing or continuous analysis should be considered. Transactional data analysis is one of the most powerful and effective ways of detecting fraud within an organization, and organizations can determine deployment along the analytics spectrum based on the their fraud risk areas.[11]

According to KPMG's *Fraud Risk Management* report, "unlike retrospective analyses, continuous transaction monitoring allows an organization to identify potentially fraudulent transactions on, for example, a daily, weekly, or monthly basis. Organizations frequently use continuous monitoring efforts to focus on narrow bands of transactions or areas that pose particularly strong risks."[12]

By applying data analysis technology on a continuous or repetitive basis — either as a continuous auditing or continuous monitoring initiative — organizations can detect fraud earlier and reduce the likelihood of greater loss. For additional information on the relationship between continuous auditing and continuous monitoring, refer to The IIA's *GTAG 3: Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment*.[13]

3.6 Analyzing Data Using Internal and External Data Sources

For data analysis to be effective in fraud detection, it's necessary to integrate data from various sources, including financial, nonfinancial, internal, and external. Using these diverse data sources provides a more comprehensive view of the organization from a fraud perspective. Table 4 — Diverse Data Sources illustrates this comprehensive view.

Organizations should use these and other data sources to conduct a fraud data analysis, which includes the four-step integrated process illustrated by Table 5 — Fraud Data Analysis.

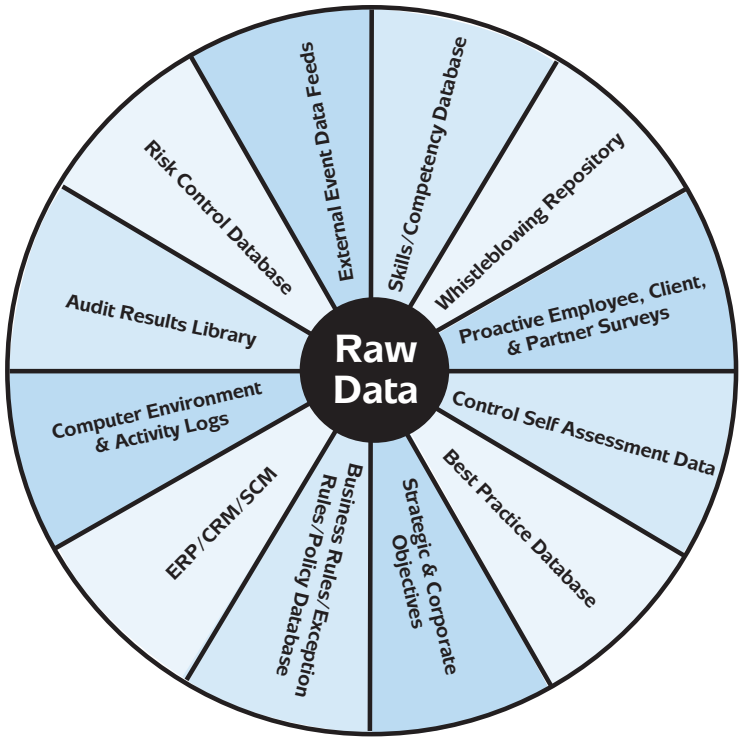
---

[10] *GTAG 5: Managing and Auditing Privacy Risks*. The Institute of Internal Auditors, 2006.

[11] "Analyze Every Transaction in the Fight Against Fraud: Using Technology for Effective Fraud Detection." ACL Services Ltd., 2008.

[12] "Fraud Risk Management: Developing a Strategy for Prevention, Detection, and Response." KPMG International, 2006.

[13] *GTAG 3: Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment*. The Institute of Internal Auditors, 2005.



Source: *The Buyer's Guide to Audit, Anti-Fraud, and Assurance Software*[14]

Table 4. Diverse Data Sources

[14] Lanza, Richard B. Brooks, Dean; and Goldman, Mort. *The Buyer's Guide to Audit, Anti-Fraud, and Assurance Software*. Ekaros Publishing, 2008.

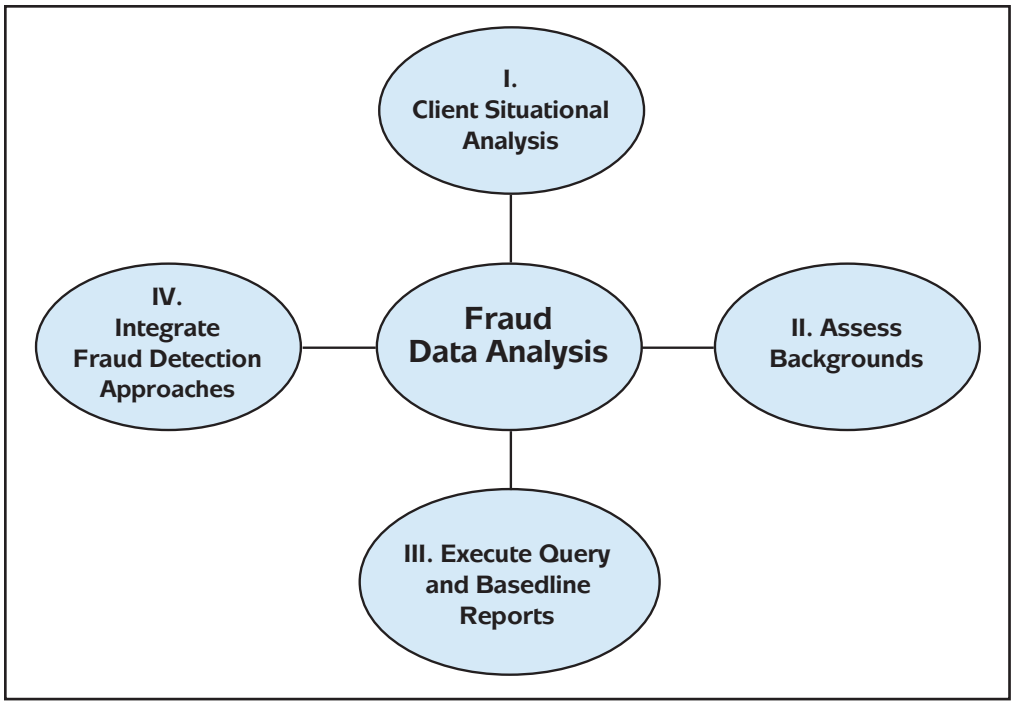


Table 5. Fraud Data Analysis

I. Complete a Situational Analysis

Identify top fraud risks from an impact and likelihood perspective for a particular organization. Internal controls used to minimize fraud risks should be taken into account, as well as plans to research results of a fraud risk assessment. Refer to Chapter 2 for more information about conducting a risk assessment to search for fraud.

II. Assess Backgrounds of Key Parties Associated with Transactions

Typically, background searches are only completed on employees or candidates for employment. Organizations should also consider using Internet databases to complete background searches on vendors, customers, and business partners associated with the transactions in areas with a high risk of fraud. For example, the procurement process may be seen as a high risk for fraudulent activity in an organization. With this in mind, the organization may elect to review vendors that are large (in terms of material dollars), those that have increased in size over the last few years, or those that are showing up on a variety of potential fraud activity reports.

Most countries have a number of government and industry data sources and lists available that can help organizations identify barred, sanctioned, or watch-listed companies. The United States, the Excluded Parties List System (www.epls.gov) provides information on parties that are excluded from receiving federal contracts and certain federal financial assistance and benefits. Company information databases such as Dun & Bradstreet and Equifax can also be used to identify business issues affecting companies such as pending legal action and financial hardship. These are useful external data sources to consider, provided the organization has identified clear objectives and outcomes for their use in fraud detection. The following list offers examples of the type of information that can be gathered from these sources and used to help assess the potential fraudulent nature of a business.

- Invalid company address and/or phone number.
- Conflicts of interest with current employees.
- Invalid tax identification number.
- Inability to find evidence of the company's existence in any of the external data sources.
- Employees posing as suppliers.
- Three-way relationships among employees, their next-of-kin, and suppliers.
- Risky type of company (e.g., sole proprietorship may be more risky).
- Newly started company.
- Past legal issues or other special issues.

The use of external databases helps organizations gain a clearer picture of business partners from the perspective of their potential to commit fraud.

III. Execute a Variety of Queries and Calculate Baseline Statistics

Based on the company's identified fraud risks, queries may be executed by internal auditors and the results combined to identify business partners, vendors, company departments, employees, and even specific transactions that appear to be fraudulent. Baseline statistics can then be calculated for business partners, company departments, employees, time, and other categories. Then, any additional activity would be related to the baseline to identify potential exceptions or red flags that would necessitate additional analysis.

One useful tool for generating report ideas is The IIA Research Foundation's study, *Proactively Detecting Fraud Using Computer Assisted Audit Reports*.[15]

An example from this publication related to billing schemes is noted below.

[15] Lanza, Richard B., "Proactively Detecting Fraud Using Computer Assisted Audit Reports," The IIA Research Foundation, 2003.

BILLING SCHEMES

Billing schemes occur when a fraudster submits invoices for fictitious goods or services, inflated invoices, or invoices for personal purchases, prompting the victim organization to issue a payment. There are three subcategories of billing schemes:

- *Shell Company* —A phony organization is created on the company's books for use in paying fictitious invoices.
- *Non-accomplice Vendor* — A vendor payment is intentionally mishandled in order to make a fictitious payment to the employee.
- *Personal Purchases* — Personal purchases are made using company accounts such as a company procurement card.

Testing Procedure	Testing Detail and Analysis	Data File(s)
Identify duplicate payments based on various means.	Duplicate payment tests can be enacted on the vendor, invoice number, and amount. More complicated tests can identify cases in which the same invoice and amount are paid, yet the payment is made to two different vendors.	• Invoice Payment
Summarize debit memos by vendor, issuer, and type.	Debit memo trends that appear unusual should be investigated, as they may indicate attempts to cover unauthorized payments.	• Invoice Payment
Identify manual checks and summarize by vendor and issuer.	Manual checks are more prone to abuse and therefore should be scrutinized, especially if a particular employee is drafting the majority of manual checks.	• Check Register
Find all purchases with no purchase orders and summarize by vendor and issuer.	Purchases with no purchase orders are more prone to abuse and therefore should be scrutinized, especially if invoices are without corresponding purchase orders.	• Invoice Payment
Match vendor master file to the accounts payable invoice file.	Identify payments to a potentially unapproved vendor by joining the vendor file to the invoice file or vendor number. This should be done on an "unmatched" basis — so that only those vendor numbers in the invoice file *not* appearing in the vendor file are shown.	• Vendor Master • Invoice Payment
Extract vendors with no telephone or tax ID number.	Vendors without this information are more prone to abuse and should be scrutinized.	• Vendor Master

When producing query and baseline statistics, auditors should use the classic "Five W" questions: who, what, why, where, and when. Many professionals use such an approach to capture a holistic picture of the complete situation and circumstances. Using the "Five W" approach to review journal entries, as illustrated below, elicits a higher probability of detecting unusual or fraudulent general ledger entries.[16]

Who made the journal entry?

- Identify journal entries that are entered by unauthorized personnel or restricted users.

What was the nature of the journal entry?

- Identify nonstandard or manual journal entries (versus standard or automated entries, such as those from an accounts payable ledger posting).
- Identify journal entries by general ledger account to identify repetitive and unique account sequences (based on the first 10 debit and credit account postings).

When was the journal entry entered?

- Identify journal entries posted on weekends and holidays.
- Classify journal entry credits and debits processing by day, month, and year.
- Summarize journal entry credits and debits processing by day, month, and year.

Why is there unusual activity related to the journal entry?

- Filter general ledger transactions (debit or credit) that exceed the average amounts for that account by a specified percentage. (Five times the average is a good starting point.)
- Identify journal entries that contain questionable language in their descriptions, such as the terms "plug," "balance," and "net to zero."
- Identify journal entries that fail to net to zero (debits less credits).

[16] Lanza, Richard B. and Gilbet, Scott. "Maximizing Journal Entry Testing Through Automation." ITAudit, 2007.

IV. Integrate the Above Approaches into a Consolidated Analysis

By combining the results of the procedures described in Step III, above, and using scoring methodology, organizations can develop a targeted list at the business partner, department, employee, and/or transaction level. When developing the list, the level of specificity desired by the company, in addition to the company's plans to research any unusual activity, should be considered.

One way to score activity is to assign a point to each result that contains a business partner/transaction, and then assign a weight to that score based on the amount of processing associated with the particular business partner/transaction. This can be explained best by using the general ledger example above and scoring the activity accordingly, as follows:

Step 1 — A numeric score of one (1) was given to each journal entry that appeared on each of the following audit tests.

1. Nonstandard or manual journal entries.
2. Journal entries made to suspense accounts, grouped by the person who did the entering, and grouped by corresponding account numbers.
3. General ledger transaction amounts that exceed the average amounts for that account by a specified percentage.
4. Journal entries that contain questionable language in their descriptions.
5. Journal entries that do not net to zero.

Step 2 — Scores from step 1 were added together to create a total numeric score. For example, a journal entry that met the conditions for audit tests 1, 3, and 6 in Step 1 was given a numeric score of three.

Step 3 — The total numeric score for each journal entry from Step 2 was then multiplied by the amount of the corresponding journal entry debits to create a weighted score. For example, a journal entry with a numeric score of three from Step 2 with account debits totaling US $100,000 has a weighted score of US $300,000 (3x $100,000).

Step 4 — The journal entries were sorted by the total numeric score, per Step 2 above, and the top 20 total numeric scored journal entries were itemized on a report. The journal entries were then sorted on the weighted score, per Step 3 above, and the top 20 weighted scored journal entries were extracted to a report.

Although each journal entry report could be reviewed in isolation, it is more effective to review them in combination so that the internal auditor can focus on the most probable or unusual journal entries. Thus, if a given journal entry appeared on many suspicious reports, it is more likely to be unusual or associated with inappropriate management override.

4. The CAE's Role in Addressing IT Fraud

The objective of this chapter is to provide the CAE with guidance on communicating with the audit committee about IT fraud risks, and regularly asking questions to help gain a better understanding of the organization's IT fraud risks and internal auditing's role. Specific ideas are included on the types of IT fraud-related information that should be considered for sharing with the audit committee. The chapter also includes twenty questions about IT fraud, and tips on what to include in a fraud investigation policy to help internal auditors gain a better understanding on how the organization addresses fraud risks.

4.1 The Audit Committee

The relationship between the CAE and the audit committee should be one that includes reporting on internal auditing activities relating to IT fraud risks and IT fraud risk assessments. Maintaining awareness of what is happening within the organization and its specific industry enhances the CAE's ability to address IT fraud risks with the audit committee.

What exactly do CAEs discuss with their audit committees when it comes to IT fraud or frauds enabled by technology? In most cases, it is nothing different from the usual updates on fraud to senior management and the audit committee. The IIA's Practice Guide, Internal Auditing and Fraud, provides insight into communicating with the board. On the other hand, the audit committee may require a more detailed explanation of the technology or IT area affected to better understand the impact and risk to the organization. Therefore, the CAE must be familiar with — and be able to articulate to the audit committee — how the organization manages and controls critical IT resources and the role internal auditing plays in this area.

The CAE may discuss the following IT fraud topics with the audit committee:

- Role of internal auditing in IT fraud investigations.
- All fraud audits performed in the IT area.
- The IT fraud risk assessment process performed.
- IT fraud or conflicts of interest and results of monitoring programs concerning compliance with law, code of conduct, and/or ethics.
- The internal audit activity's organizational structure as it pertains to addressing IT fraud.
- Coordination of IT fraud audit activity with external auditors.
- Overall assessment of the organization's fraud control environment in IT.
- Productivity and budgetary measures of internal auditing's IT fraud activities.
- Benchmarking comparisons of internal auditing's IT fraud activities with other companies.

4.2 Twenty Questions the CAE Should Ask About Fraud

The CAE should never be reluctant to ask questions about fraud. Conducting timely and appropriate discussions about fraud with all levels of the organization, including the audit committee, demonstrates that the internal audit activity is taking a proactive role in this area. Some of the many questions that the CAE should be asking about IT fraud on a regular basis include:

1. Does the organization have a fraud governance structure in place that assigns responsibilities for IT fraud investigations?
2. Does the organization have an IT fraud incident response policy in place? (Refer to What to Include in a Fraud Investigation Policy, below, for more information.)
3. Has the organization identified laws and regulations relating to IT fraud in jurisdictions where it does business?
4. Does the organization's IT fraud management program include coordination with internal auditing?
5. Does the organization have a fraud hotline that notifies appropriate individuals of fraud concerns involving IT resources?
6. Does the audit charter mention internal auditors' roles and responsibilities relating to IT fraud?
7. Has responsibility for IT fraud detection, prevention, response, and awareness been assigned within the organization?
8. Do management and the CAE update the audit committee on IT fraud?
9. Does management promote IT fraud awareness and training within the organization?
10. Does management lead IT fraud risk assessments and include internal auditing it the assessment process?
11. Are the results of IT fraud risk assessments implemented into the audit planning process?
12. Are periodic IT fraud awareness and training programs provided to internal auditors?
13. Are automated tools available to those responsible for preventing, detecting, and investigating IT fraud?
14. Has management identified the types of potential IT fraud risks in its areas of responsibility?
15. Do management and the CAE know where to obtain guidance on IT fraud from professional organizations?
16. Do management and internal auditors know their professional responsibilities relating to IT fraud?
17. Has management incorporated appropriate controls to prevent, detect, and investigate IT fraud?

18. Does management have the appropriate skill sets in place to perform IT fraud investigations?
19. Do management and internal auditing periodically assess the effectiveness and efficiency of IT fraud controls?
20. Are IT fraud investigation working papers and supporting documents appropriately secured and retained?

What to Include in a Fraud Investigation Policy

1. How and when to start a fraud investigation.
2. Documentation requirements for the fraud investigation.
3. How to select the investigation team.
4. The process for adding experts to the team.
5. How to assess, evaluate, and mitigate internal controls.
6. How and when to elevate investigations.
7. Consistency and uniformity to be sure all offenses are treated the same.
8. Guidance on how far the organization is willing to pursue an investigation.
9. Communication channels to use before, during, and after the investigation.
10. Guidelines on the extent of recovery efforts to be conducted.

References and Resources

Institutes and Associations:

American Institute of Certified Public Accountants (AICPA) — www.aicpa.org

Association of Certified Fraud Examiners (ACFE) — www.acfe.org

The Institute of Internal Auditors (IIA) — www.theiia.org

International Laws and Regulations Relating to Fraud:

Australia — Corporate Law Economic Reform Program Act 2004

Canada — Criminal Code

European Union — Financial Services Action Plan

United Kingdom — Companies Act of 2004

United States — USA PATRIOT Act, Foreign Corrupt Practices Act, U.S. Sarbanes-Oxley Act of 2002

Other References:

"2008 Report to the Nation on Occupational Fraud & Abuse," Association of Certified Fraud Examiners, 2008.

"Analyze Every Transaction in the Fight Against Fraud: Using Technology for Effective Fraud Detection," ACL Services Ltd., 2008.

"The 'Big Picture' of Insider IT Sabotage Across U.S. Critical Infrastructures." Carnegie Mellon, May 2008.

Cappelli, Dawn; Trzeciak, Randal; Moore, Andrew, "Insider Threats in the SDLC," CERT, 2006.

Cline, Jay, "530M Records Exposed, and Counting," *Computerworld Security*, Sept. 9, 2008.

Coderre, David G., *Computer Aided Fraud Prevention and Detection: A Step-by-Step Guide*, John Wiley & Sons, 2009.

Coderre, David G., *Fraud Analysis Techniques Using ACL*, John Wiley & Sons, 2009.

"Data Breaches Surpass 2007 Level, But Businesses Are Rarely Penalized," *The Wall Street Journal*, Sept. 9, 2008.

"Fraud Risk Management: Developing a Strategy for Prevention, Detection, and Response," KPMG International, 2006.

Global Technology Audit Guide 3: Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment; The IIA; 2005.

Global Technology Audit Guide 5: Managing and Auditing Privacy Risks, The IIA, 2006.

"How Fraud Hurts You and Your Government Organization," Association of Certified Fraud Examiners' Web site: http://www.acfe.com/resources/fraud-tools.asp?copy=video.

"Insider Threat Study: Illicit Cyber Activity in the Information Technology and Telecommunications Sector," U.S. Secret Service and CERT Coordination Center/SEI, January 2008.

Internal Audit 2012: A Study Examining the Future of Internal Auditing and the Potential Decline of a Controls-centric Approach, PricewaterhouseCoopers, 2007.

International Professional Practices Framework. Practice Guide, Internal Auditing and Fraud. The IIA 2009

Lanza, Richard B.; Brooks, Dean; and Goldman, Mort; *The Buyer's Guide to Audit, Anti-Fraud, and Assurance Software*; Ekaros Publishing; 2008.

Lanza, Richard B. and Gilbet, Scott, "Maximizing Journal Entry Testing Through Automation," *ITAudit*, Feb.10, 2007.

Lanza, Richard B., "Proactive Control Monitoring," *ITAudit*, Nov.15, 2003.

Lanza, Richard B., "Proactively Detecting Fraud Using Computer Assisted Audit Reports," The IIA Research Foundation, 2003.

Management Anti-fraud Programs and Controls: Guidance to Help Prevent, Deter, and Detect Fraud; AICPA, The IIA, Association of Certified Fraud Examiners (ACFE), Information System Accountability and Control Auditors, Financial Executives Institute, Institute of Management Accountants, and Society of Human Resource Professionals; 2002.

Managing the Business Risk of Fraud: A Practical Guide; The IIA, ACFE, and AICPA; 2008.

"Sample Fraud Policy," ACFE Web site, http://www.acfe.com/documents/sample_fraud_policy.pdf.

SOX Section 404: A Guide for Management by Internal Controls Practitioners, Second Edition, The IIA, 2008.

U.S. Department of Justice Web site, Computer Crime and Intellectual Property Section, http://usdoj.gov/criminal/cybercrime, 2009.

About the Authors

- **Ken Askelson**
  CIA, CPA, CITP, retired from JC Penney Co. Inc.

- **Rich Lanza**
  CPA, CFE, PMP, President of Cash Recovery Partners, LLC

- **Peter Millar**
  Director, Technology Application, ACL Services Ltd

- **Marilyn Prosch**
  Ph.D. W.P Carey School of Business, Associate Professor, Department of Information Systems Management Arizona State University

- **Donald E Sparks**
  CIA, CISA, ARM, Vice President, Audimation Services, Inc.

Reviewers and Contributors

The IIA thanks the following organizations and individuals who provided valuable comments and added great value to this guide:

- Association of Certified Fraud Examiners
- Professional Practices Advisory Council:
  - Advanced Technology Committee
  - Board of Regents
  - Committee on Quality
  - Ethics Committee
  - Internal Auditing Standards Board
  - Professional Issues Committee
- The Institute of Internal Auditors — UK & Ireland
- Douglas J. Anderson, The Dow Chemical Company, USA
- David Bentley, independent consultant, UK
- Denny K. Beran, JC Penney Co. Inc., USA
- Lily Bi, The Institute of Internal Auditors, USA
- David Coderre, Office of the Comptroller General of Canada
- John D. Gill, Association of Certified Fraud Examiners
- Larry Harrington, Raytheon Company, USA
- Steve Hunt, Crowe Horwath LLP, USA
- David Lione, independent consultant, USA
- Susan Lione, The Institute of Internal Auditors, USA
- Jay R. Taylor, General Motors, USA
- Karine Wegrzynowicz, Lafarge SA, Francev

About IPPF

The International Professional Practices Framework (IPPF) is the conceptual framework that organizes authoritative guidance promulgated by The Institute of Internal Auditors. IPPF guidance includes:

Mandatory Guidance

Conformance with the principles set forth in mandatory guidance is required and essential for the professional practice of internal auditing. Mandatory guidance is developed following an established due diligence process, which includes a period of public exposure for stakeholder input. The three mandatory elements of the IPPF are the Definition of Internal Auditing, the Code of Ethics, and the *International Standards for the Professional Practice of Internal Auditing (Standards)*.

Element	Definition
Definition	The Definition of Internal Auditing states the fundamental purpose, nature, and scope of internal auditing.
Code of Ethics	The Code of Ethics states the principles and expectations governing behavior of individuals and organizations in the conduct of internal auditing. It describes the minimum requirements for conduct, and behavioral expectations rather than specific activities.
International Standards	*Standards* are principle-focused and provide a framework for performing and promoting internal auditing. The *Standards* are mandatory requirements consisting of: • Statements of basic requirements for the professional practice of internal auditing and for evaluating the effectiveness of its performance. The requirements are internationally applicable at organizational and individual levels. • Interpretations, which clarify terms or concepts within the statements. It is necessary to consider both the statements and their interpretations to understand and apply the *Standards* correctly. The *Standards* employ terms that have been given specific meanings that are included in the Glossary.

Strongly Recommended Guidance

Strongly recommended guidance is endorsed by The IIA through a formal approval processes. It describes practices for effective implementation of The IIA's Definition of Internal Auditing, Code of Ethics, and *Standards*. The three strongly recommended elements of the IPPF are Position Papers, Practice Advisories, and Practice Guides.

Element	Definition
Position Papers	Position Papers assist a wide range of interested parties, including those not in the internal audit profession, in understanding significant governance, risk, or control issues and delineating related roles and responsibilities of internal auditing.
Practice Advisories	Practice Advisories assist internal auditors in applying the Definition of Internal Auditing, the Code of Ethics, and the *Standards* and promoting good practices. Practice Advisories address internal auditing's approach, methodologies, and consideration, but not detail processes or procedures. They include practices relating to: international, country, or industry-specific issues; specific types of engagements; and legal or regulatory issues.
Practice Guides	Practice Guides provide detailed guidance for conducting internal audit activities. They include detailed processes and procedures, such as tools and techniques, programs, and step-by-step approaches, as well as examples of deliverables.

This GTAG is a Practice Guide under IPPF.

For other authoritative guidance materials, please visit www.theiia.org/guidance/.

GTAG®

Fraud Prevention and Detection in an Automated World

As technology advances, so do schemes to commit fraud. Technology can not only be used to perpetrate fraud, but also to prevent and detect it. Using technology to implement real-time fraud prevention and detection programs will enable organizations to reduce the cost of fraud by lessening the time from which a fraud is committed to the time it is detected.

Through a step-by-step process for auditing a fraud prevention program, an explanation of the various types of data analysis to use in detecting fraud, and a technology fraud risk assessment template, the GTAG aims to inform and provide guidance to chief audit executives and internal auditors on how to use technology to help prevent, detect, and respond to fraud.

We'd like your feedback! Visit the GTAG page under www.theiia.org/gtags to rate it and submit your comments.

The Institute of Internal Auditors

www.theiia.org

Order Number: 1069
ISBN: 978-0-89413-680-1
IIA Member Free
Nonmember US $25