

PERCEPTIONS OF THE ROLE OF THE INTERNAL AUDIT DEPARTMENT IN  
THE DEFINITION, DETERRENCE, PREVENTION, DETECTION,  
AND INVESTIGATION OF EMPLOYEE FRAUD IN THE  
CANADIAN INSURANCE INDUSTRY

by

Kenneth Bradley Schulz

B.A., Simon Fraser University, 1989

THESIS SUBMITTED IN PARTIAL FULFILLMENT OF  
THE REQUIREMENTS FOR THE DEGREE OF  
MASTER OF ARTS  
in the School  
of  
Criminology

© Kenneth Bradley Schulz 1994

SIMON FRASER UNIVERSITY

December 1994

All rights reserved. This work may not be reproduced in whole or in part, by photocopy or other means, without permission of the author.

## APPROVAL

**Name:** Kenneth Bradley Schulz  
**Degree:** Master of Arts  
**Title of Thesis:** Perceptions of the Role of the Internal Audit Department in the Definition, Deterrence, Prevention, Detection, and Investigation of Employee Fraud in the Canadian Insurance Industry

**Examining Committee:**

**Chairperson:** Robert Menzies, Ph.D.

---

John Lowman, Ph.D.  
Professor  
Senior Supervisor

---

F. Douglas Cousineau  
Associate Professor

---

David J. Cherrington, Ph.D.  
External Examiner  
Professor  
Brigham Young University

**Date Approved:** December 7, 1994

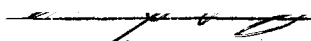
PARTIAL COPYRIGHT LICENSE

I hereby grant to Simon Fraser University the right to lend my thesis, project or extended essay (the title of which is shown below) to users of the Simon Fraser University Library, and to make partial or single copies only for such users or in response to a request from the library of any other university, or other educational institution, on its own behalf or for one of its users. I further agree that permission for multiple copying of this work for scholarly purposes may be granted by me or the Dean of Graduate Studies. It is understood that copying or publication of this work for financial gain shall not be allowed without my written permission.

Title of Thesis / ~~XXXXXXXXXXXXXXXXXXXX~~

Perceptions of the Role of the Internal Audit Department in the  
Definition, Deterrence, Prevention, Detection, and Investigation

of Employee Fraud in the Canadian Insurance Industry

Author:   
(signature)

Kenneth Bradley Schulz

(name)

December 14, 1994

(date)

## ABSTRACT

This thesis examines perceptions of employee-fraud-control policies and practices of internal audit departments of Canadian insurance companies. The research includes a literature review, the experience of six months of the researcher's employment in the internal audit department of a western Canadian insurance company, and the collection of questionnaire data. After analyzing the data in light of the extant literature on employee theft, employee fraud, embezzlement, and hidden workplace economies, an analysis of the policies and activities of internal audit departments is presented. Among other findings, the data indicate the following: (a) internal audit departments in the Canadian insurance industry undertake an active role in the deterrence, prevention, detection, and investigation of employee fraud; (b) the control measures used by internal audit departments focus on reducing the opportunities to defraud; and (c) the private security industry and employees play a role in employee-fraud control.

## ACKNOWLEDGMENTS

I would like to acknowledge the contributions of a few people who were instrumental in my achieving this degree. First, I would like to thank Dr. John Lowman for his helpful comments as well as his prompt reviews of my work. Second, I am appreciative of Pat Way who allowed me to conduct my research within his audit department. I wish to thank my wife, Sandra, who took over my share of family responsibilities when deadlines approached. In addition, I would like to thank my children, Erin, Megan, and Kaitlin, who were completely uninterested in my thesis, but who only cared that I took time to play, dance, and tell of the adventures of "Three Kitties and the Tickle Monster." I would like to thank my mom and dad for their constant reminders from time immemorial that a formal education is a good for me. And although it cannot be scientifically documented, I must acknowledge God's timely provision of various employment opportunities throughout my schooling. To each, I wish to say, "Thank-you."

## TABLE OF CONTENTS

Approval .....	ii
Abstract .....	iii
Acknowledgments .....	iv
List of Tables .....	x
List of Figures .....	xi
<b>Chapter 1: A Review of the Literature on Employee Fraud ...</b>	<b>1</b>
I. Introduction .....	1
A. Goal of Research .....	1
B. Importance of Studying Employee-Fraud Control ....	2
C. Importance of Studying Internal Audit Departments in the Canadian Insurance Industry .....	4
D. The Renewed Emphasis on Employee-Fraud Control by Internal Auditors Departments .....	4
II. Literature Review .....	6
A. Defining Employee Fraud .....	8
B. Incidence of Employee Theft and Employee Fraud ...	9
C. Correlates of Employee Theft and Employee Fraud .....	12
1. External Economic Pressure .....	13
2. Age of Worker .....	15
3. Opportunity to Offend .....	15
4. Job Dissatisfaction .....	17
5. Formal Policies and Informal Workplace Norms .....	18
D. Employee-Fraud-Control Measures .....	22
1. Issues Arising from the Relationship between the Correlates of Employee Fraud and Control Measures .....	23
2. Economic, Intra-, and Inter-Organizational Influences upon Employee-Fraud-Control Measures .....	25
a) Economic Influences .....	27
b) Intra-Organizational Influences .....	27
c) Inter-Organizational Influences .....	31

3.	Nature and Extent of Organizational Employee-Fraud-Control Measures .....	32
a)	Corporate Responsibility for Employee-Fraud Control .....	33
b)	Definition of Employee Fraud .....	37
c)	Deterrence and Prevention of Employee Fraud .....	38
d)	Detection of Employee Fraud .....	39
e)	Investigation .....	40
f)	Reporting .....	41
g)	Prosecution .....	42
III.	Theoretical Framework .....	43
<b>Chapter 2:</b>	<b>Methodology .....</b>	<b>46</b>
I.	Introduction .....	46
II.	Literature Searches .....	46
III.	Working in an Internal Audit Department .....	47
IV.	Data Collection .....	47
A.	Choice of Units of Analysis .....	47
B.	Company Goals and Operational Environments .....	49
C.	Preparation of Questionnaire .....	50
1.	Operational Definitions .....	50
2.	Structure of Questionnaire .....	51
3.	Focus of Questionnaire .....	51
4.	Pre-Testing the Questionnaire .....	52
D.	Delivery of the Questionnaire .....	52
<b>Chapter 3:</b>	<b>The Questionnaire: A Window on the World of the Internal Audit Department .....</b>	<b>53</b>
I.	Introduction .....	53
II.	Overview of Results .....	53
III.	Company Employment, Premiums, and Computer Environment .....	56
A.	Number of Employees .....	56
B.	Amount of Revenue, Premiums, and Deposits .....	56
C.	Nature of Companies' Computer Environment .....	57

IV.	Internal Audit Department's Structure .....	58
A.	Reporting Hierarchy for the Internal Audit Department .....	58
B.	Number of Managers, Staff, Support Staff, and Secretaries .....	58
C.	Staff Educational Background .....	59
V.	Organizational Responsibilities For Employee-Fraud Control .....	61
A.	Corporate Use of Investigation Units .....	61
B.	Central Responsibility for Employee-Fraud Control .....	61
C.	Responsibility for the Deterrence, Detection, and Investigation of Employee Fraud.....	62
1.	Deterrence and Detection .....	62
2.	Investigation .....	66
a)	Companies Without a Separate Investigation Unit .....	67
b)	Companies With a Separate Investigation Unit .....	68
c)	Companies Using a Committee to Oversee Employee-Fraud Investigations .....	69
d)	Role of Legal Counsel in Employee- Fraud Investigations .....	71
e)	Use of Police and Forensic Accountants in Employee-Fraud Investigations .....	72
VI.	Internal Audit Department Managers' Definition Of Employee Fraud .....	72
VII.	Deterring and Preventing Employee Fraud .....	76
A.	Corporate Measures Undertaken to Deter and Prevent Employee Fraud .....	76
B.	Internal Audit Department's Measures Undertaken to Deter Employee Fraud .....	78
C.	Employee Involvement in Deterring Employee Fraud .....	80



VIII.	Detecting Employee Fraud .....	81
A.	Incidence and Nature of Employee Fraud .....	81
B.	Focus of Employee-Fraud-Detection Measures .....	84
C.	Corporate Measures Undertaken to Detect Employee Fraud .....	86
D.	Internal Audit Department's Measures Used to Detect Employee Fraud .....	88
E.	Reporting of Employee-Fraud Allegations .....	93
1.	Receiver of Employee-Fraud Allegations .....	93
2.	Sources of Employee-Fraud Allegations .....	93
3.	Recording of Employee-Fraud Allegations ....	98
F.	Uniformity in the Skill Level of Internal Auditors in Employee-Fraud Detection .....	99
IX.	The Internal Audit Departments' Investigation of Employee Fraud and the Departments' Follow-Up Report .....	100
A.	Nature of the Internal Audit Department's Investigation .....	100
B.	Sources Used in an Investigation .....	102
C.	Procedure Following an Internal Audit Department's Investigation .....	103
D.	Responsibility for Issuing a Report Following an Investigation .....	103
X.	Prosecution and Adjudication of Employee-Fraud Cases..	105
	<b>Chapter 4: Explanations for the Internal Audit Departments' Employee-Fraud-Control Program .....</b>	<b>106</b>
I.	Introduction .....	106
II.	Internal Audit Managers' Definition of Employee Fraud .....	106
A.	Reasons for the Internal Audit Managers' Perception of Offense Seriousness .....	106
B.	Implications of Internal Audit Managers' Definition and Perceived Seriousness of Employee Fraud .....	108

III.	The Internal Audit Department's Deterrence and Prevention of Fraud .....	110
A.	Corporate Responsibility for Deterrence and Prevention .....	110
B.	Emphasis of Deterrence and Prevention Measures in Favour of Detection Measures .....	110
C.	The Emphasis on Situational Factors in Deterrence and Prevention Measures .....	113
D.	The Internal Audit Departments' Use of the Work Group Environment to Deter Employee Fraud .....	114
IV.	Detection of Employee Fraud .....	115
A.	Corporate Responsibility for Employee-Fraud Detection .....	115
B.	Role of Employees In Detecting Employee Fraud ..	119
C.	The Effectiveness of Internal Audit Departments' Detection Measures .....	121
V.	The Nature of the Employee-Fraud Investigation and Its Adjudication .....	127
VI.	Conclusion .....	129
A.	Perceptions of Internal Audit Departments' Employee-Fraud-Control Policy: A Review of Findings .....	129
1.	Reporting Hierarchy for the Internal Audit Department .....	129
2.	Internal Auditors' Knowledge of Employee Fraud .....	129
3.	Organizational Responsibilities for Employee-Fraud Control .....	130
4.	Internal Audit Managers' Definition of Employee Fraud .....	131
5.	Deterring and Preventing Employee Fraud ...	131
6.	Detecting Employee Fraud .....	132
7.	Internal Audit Departments' Investigation and Follow-up Procedures .....	133
8.	Role of Private Security Industry in the Control of Employee Fraud .....	134
9.	Distribution of Sanctions Across Companies .....	134
B.	Implications of the Research .....	135
	List of References .....	138
	Appendix 1: Searches of Printed Abstracts and Indexes ....	144
	Appendix 2: Questionnaire .....	146

## LIST OF TABLES

3.1	Internal Auditors' Education on Employee Fraud .....	60
3.2	The Responsibilities for Detection of Employee Fraud by the Internal Audit Department and Line Management .....	64
3.3	Responsibility For Employee-Fraud Investigations in the Thirteen Companies without a Separate Investigation Unit .....	68
3.4	Responsibility for Employee-Fraud Investigations in Companies with a Separate Investigation Unit .....	69
3.5	The Responsibilities of Committees to Oversee Employee-Fraud Investigations .....	71
3.6	Number of Companies That Would Fire or Dismiss an Employee for Selected Acts of Fraud, Theft, and Misconduct .....	73
3.7	Prevalence of Corporate Deterrence Methods .....	77
3.8	Measures Undertaken by the Internal Audit Department to Deter Employee Fraud.....	79
3.9	Measures Undertaken by Insurance Companies to Detect Employee Fraud .....	88
3.10	Measures Undertaken by Internal Audit Departments to Detect Employee Fraud .....	91
3.11	Receivers of Employee-Fraud Allegations .....	93
3.12	Employee Tips and Corporate Reporting Policy .....	96
3.13	External Tips and Corporate Reporting Policy .....	97
3.14	Nature of the Internal Audit Departments' Investigation into Employee Fraud .....	101
3.15	Sources of Information Used in the Internal Audit Departments' Investigation into Employee Fraud .....	102

**LIST OF FIGURES**

3.1 Corporate Responsibility for Deterrence, Detection,  
and Investigation of Employee Fraud ..... 63

3.2 Company Operations in Which Fraud Occurs Frequently  
as Perceived by Audit Managers ..... 83

3.3 Sources of Employee-Fraud Allegations as  
Identified by Internal Audit Managers ..... 95

## CHAPTER 1: A REVIEW OF THE LITERATURE ON EMPLOYEE FRAUD

### I. INTRODUCTION

#### A. Goal of Research

The purpose of this research is to describe internal audit managers' perceptions of employee-fraud policies undertaken by internal auditors in Canadian insurance companies. This will be accomplished by reviewing research on related topics, by the experience of my working alongside internal auditors in one company for a six-month period, and by distributing a self-administered questionnaire to a sample of insurance company internal audit departments.

The thesis describes the internal audit department's perceived organizational role in influencing employee-fraud policies and in developing measures to control employee fraud. In the process, this thesis examines the definition, deterrence, detection, investigation, and reporting of employee fraud; the incidence and frequency of employee fraud; the cause(s) of employee fraud; the effectiveness of formal and informal employee-fraud-control measures; and the conceptualization of employee fraud. My research does not attempt to describe the evolution of employee-fraud-control policies in Canadian insurance companies; rather, it describes them as they exist presently.

Due to the scarcity of research on employee fraud control by internal audit departments, this research is exploratory in nature and limited to an examination of managers' perceptions.

Its main empirical contribution is provided by a questionnaire survey of internal audit departments. The internal audit department manager of 32 of the largest Canadian insurance companies received a self-administered questionnaire after it was pre-tested and revised. The questionnaire focused on the nature of corporate reporting on administrative matters; the structure of internal audit; the type of formal education for internal audit staff; the corporate responsibilities for employee-fraud deterrence, detection, investigation, and reporting; the priorities of internal audit departments when conducting audits; the number of criminal investigations for employee fraud; the methods used by the internal audit department to deter, detect, and investigate employee fraud; the characteristics of those individuals subject to control measures; and the nature and extent of the reporting of employee fraud allegations by departments to one another within the corporation.

#### B. Importance of Studying Employee-Fraud Control

There are several reasons for studying employee-fraud control. First, increased automation and increased participation in company decision-making by employees allow employees to exercise a greater degree of autonomy in carrying out their responsibilities. This increases the likelihood of employee fraud as well as the amount that can be taken.

Second, employee-fraud-control measures may contravene contemporary notions of privacy and trust. Employees value

trust in workplace relations because of the elevated social status associated with trust. Anything that attempts to circumvent that trust is viewed with suspicion. As is the case with other aspects of employees surveillance, the determination of the proper balance between trust and accountability is contested frequently at collective bargaining negotiations and arbitration hearings.

Third, as a consequence of an allegation of fraud, the employer or the offender may face serious legal action. A fraud investigation may result in an economic loss when an employer is sued in civil court for false imprisonment, defamation, malicious prosecution, or extortion. Even when the employer escapes court-ordered compensation, the act of going to civil court is costly in terms of time and expense. For an offender, a criminal conviction often prevents him or her from working in certain occupations.

Fourth, there is academic merit in studying employee fraud. The vast majority of research on crime in the workplace has focused on the theft of property and more minor rule violations (eg., time theft, unauthorized use of company equipment), and the primary foci have been the role of line management in its control of employee theft and fraud in the retail, manufacturing, and health industries (Ditton, 1979; Henry, 1978; Hollinger & Clark, 1983a). Although many similarities exist between employee theft and employee fraud, this thesis argues that employee fraud is different in many

important ways. Therefore, it is worthy of study as a separate issue.

### C. Importance of Studying Internal Audit Departments in the Canadian Insurance Industry

As a company grows in size and complexity, senior management may create a separate department to carry out the internal audit function. According to The Institute of Internal Auditors (IIA),

internal auditing is an independent appraisal function established within an organization to examine and evaluate its activities as a service to the organization. The objective of internal auditing is to assist members of the organization in the effective discharge of their responsibilities.... Internal auditors must be independent of the activities they audit (1985, p. 1).

Hence, the internal audit department serves the needs of management by functioning as a type of "business police." By evaluating internal financial and operational controls and by reporting on the manner in which these rules are adhered to by employees and managers, the internal audit department facilitates senior management's control over the corporation's operations.

### D. The Renewed Emphasis on Employee-Fraud Control by Internal Audit Departments

The renewed emphasis on the role of the Canadian internal audit department in employee-fraud control appears to have come by way of increasing pressure on the American independent auditor. Increasing pressure on independent auditors in the United States (a result of the fact that several public



institutions failed due to fraudulent financial reporting) led to the establishment of ,The Commission on Auditor's Responsibility (sponsored by the American Institute of Certified Public Accountants (AICPA) and commonly known as the Cohen Commission). In its report, the Commission found that "those who used financial statements [ie., shareholders] considered fraud detection a necessary and important objective of the financial audit" (The Internal Auditor and Fraud, 1990, p. 3).

By the 1980s, and with increasing demands by the public and politicians for greater accountability of publicly-owned companies, the publicly-funded National Commission on Fraudulent Financial Reporting (the Treadway Commission) was established. One objective of the Commission was to examine the role of independent public accountants in detecting fraud in publicly-owned companies (excluded in this study were employee embezzlements, violations of environmental or product safety regulations, and tax fraud) (1987, p. 2). One recommendation of the Commission was that each company should have "an effective internal audit function staffed with an adequate number of qualified personnel appropriate to the size and nature of the company" (1987, p. 37). The Commission also encouraged companies to adopt the IIA standards on fraud prevention and detection, which are "excellent guidance for effective internal auditing and reflect some of the most advanced thinking on fraud prevention and detection" (1987,

p. 38).<sup>1</sup> Since many Canadian internal audit managers belong to the IIA, the internal audit department has been forced to deal with employee-fraud control.

## II. LITERATURE REVIEW

To date, there has been no attempt to outline the activities and policies of the internal audit department concerning the definition, deterrence, prevention, detection, and investigation of employee fraud in the Canadian insurance industry. Other studies have covered a more restrictive terrain that includes the following: types of fraud committed (Albrecht, Romney, & Howe 1984; Hylas & Ashton, 1982), prevention measures (Allen, 1981; McKee & Bayes, 1987), and perceived responsibilities of internal auditors (Collier, Dixon, & Marston, 1991; Mautz, Tiessen, & Colson, 1984; McKenzie, 1989). Each of these studies have used the survey approach and have solicited the responses of internal audit department managers representing various industries. My research will address each of these issues and focus specifically on the insurance industry in Canada.

There has been significant research undertaken in the general area of employee theft. Henry's (1978) review suggests that it has only been since 1970 that there has been academic interest in "hidden economies in the workplace": Cressey (1953) studied embezzlement; Cameron (1964) studied

---

1. These standards are found in the 1985 statement by the IIA outlining the "Deterrence, Detection, Investigation, and Reporting of Fraud."

shoplifting; Henry (1976) studied the receiving of stolen goods; Ditton (1977a) studied computer fraud; Mars (1973) and Mars and Mitchell (1976) studied hotel and catering staff; Ditton (1977b) studied bread salesmen; Bigus (1972) studied milkmen; Robin (1965), Franklin (1975), and England (1976) studied shop workers; Horning (1970) studied factory workers; Quinney (1963) studied pharmacists; and Richstein (1965) studied lawyers.

Since Henry's published review, other researchers have studied employee deviance. Ditton (1979) studied "control waves" surrounding employee theft, and Hollinger and Clark (1983a) used the data from a self-report survey to evaluate theories about the cause of employee deviance. From a review of the literature, Albrecht, Romney, and Howe (1984) concluded that the interrelation between personal characteristics, situational pressures, and opportunities to commit fraud led to employee fraud.

Drawing on the aforementioned research, I do the following: (a) review past conceptualizations of employee deviance; (b) describe the present state of knowledge with regards to the incidence of employee theft and fraud; (c) outline the correlates of employee theft and fraud as identified in the literature; (d) discuss the manner in which economic, intra-, and inter-organizational factors influence an organization's employee-fraud-control policy; and (e) review the nature and the extent of formal control measures presently used and advocated. The literature review is used

to establish a context in which the role and practices of the internal audit department can be described and explained.

#### A. Defining Employee Fraud

The literature is not in agreement as to the appropriate criteria to be used to classify various types of employee deviance. There are several reasons why disagreement exists.

First, one view is that class structure affects rates of offending; therefore, data must be interpreted in light of this deterministic assumption. Terms such as "white collar crime," "corporate crime," "elite deviance," and "upper world crime" (Thio, 1988) reflect the assumption that there are qualitatively different structural, psychological, and sociological processes that differentiate acts of theft and fraud.

Second, there is debate over the extent to which various forms of employee deviance are related. Many theorists see all forms of property theft, norm violation, and hidden economy activity as being related theoretically. Henry (1978) used the term "hidden economy" to refer to a wide variety of acts undertaken in the course of employment. Hollinger and Clark (1983a) used the term "employee deviance" to refer to the varied forms of economic harm that can be experienced by the employer, including acts of theft, "wildcat strikes," and "time theft." Hollinger and Clark (1983a) identified two primary subcategories of employee deviance: "property deviance" are those acts against the property of the

organization, and "production deviance" are those acts that violate the norms regulating acceptable levels of production.

My research uses the concept of "employee fraud" because of the analytic and practical advantages it offers. First, it allows me to focus on fraudulent activity that occurs at all levels of the organization, whether the perpetrator is an employee or a supervisor. (Questions on the frauds committed by senior management were used to identify the internal audit departments' reaction towards all forms of fraud control within insurance companies.) Second, I believe that "time theft," "hidden economy," and "employee fraud" are not necessarily related theoretically; therefore, they should be treated separately (this issue will be elaborated upon later in this chapter). Finally, the concept of "employee fraud" is used frequently in the popular internal audit literature and thus provides the most uniform conceptualization for the purposes of this research. Following Gardiner and Lyman (1984, p. 3), employee fraud is defined as an illegal act that involves the "intentional misrepresentation of facts for purpose of receiving unauthorized benefits."

#### B. Incidence of Employee Theft and Employee Fraud

The disagreement over the proper way to conceptualize and to operationalize definitions of employee fraud as well as the secretive nature of the act have made the accurate quantification of this phenomenon extremely difficult. Usually, employee theft and employee fraud statistics are

based upon the methodologically questionable "guesstimates" of managers, auditors, and security officials. The typical method of collecting such statistics involves distributing questionnaires to these authorities and having them estimate the incidence of the behaviour in question (Baker & Westin, 1987; Chamber of Commerce of the United States, 1974). Often, these estimates are then added together to represent the total amount of crime or deviance. After reviewing the literature, several researchers have concluded that, in spite of renewed public interest, there are no reliable comparative measures that allow us to judge trends in employee deviance (Henry, 1978; Hollinger & Clark, 1983a; Raab, 1987; Shepard & Dustin, 1988).

In light of the preponderance of statistics collected in this manner, Gardiner and Lyman argued that the achievement of a credible approximation of the incidence and the severity of fraud using organizational information is best accomplished by using a sophisticated measurement procedure. This involves "systematic data collection, the classification or labeling of those data, and the extrapolation or projection from those data to some assumed universe (1984, p. 4)." "Systematic data collection" involves a deliberate attempt to count purposefully secretive behaviour. The "classification" of fraud requires the accurate assessment of intent behind each act and a clear understanding of an organization's procedural rules. "Projections" are to be based on a representative sample of the population, and by carefully controlling for

potentially confounding variables that may affect data collection. In order for a compilation of fraud statistics to be reliable, each requirement needs to be adequately incorporated into a research project -- something not yet accomplished in the area of employee fraud.

A second method that may produce accurate statistics on employee fraud is the use of a self-report questionnaire. Using this method, Hollinger and Clark concluded that employee theft "exhibits a bimodal distribution where a few people take large amounts while the vast majority of those involved take relatively small amounts" (1983a, p. 40). Hollinger and Clark found that more than 65% of employees in the retail sector, 69% in the hospital sector, and 82% in the manufacturing sector were involved in production deviance (eg., time thefts such as taking long lunch breaks or leaving work early) in the preceding 12 months (1983a, pp. 44-45). When it came to property theft, Hollinger and Clark found that 6% to 15% of employees in all three industries stole "production supplies, company tools, or merchandise, and 3 percent of retail employees reported taking money" (1983a, pp. 41-43). Also, they found that the majority of cases involved only a single perpetrator, that management does not perceive the problem as having reached a crisis point, and that more company property is stolen by employees than by outsiders (1983a, p. 41).

Since my research does not attempt to collect statistics either in the manner suggested by Gardiner and Lyman or

through a self-report questionnaire, only a secondary analysis of employee-fraud statistics, will be incorporated into my work. The Hollinger and Clark (1983a) study is important to my endeavors because of its methodological improvement in quantifying the nature and the extent of various forms of employee deviance. However, their study describes the relatively minor property deviance undertaken by retail, hospital, and manufacturing employees in the United States. My study focuses on the Canadian insurance industry. It uses the conclusions of Hollinger and Clark and others to contextualize the efforts of internal auditors. The results of studies conducted on other samples are cautiously extrapolated to the sample under investigation in this research.

### C. Correlates of Employee Theft and Employee Fraud

In spite of the sparcity of credible statistics on the incidence of employee theft and fraud, researchers have attempted to outline correlates of the same. Since the purpose of this research is to analyze the actions of those attempting to control the extent of employee theft and fraud, a brief review of the more commonly mentioned correlates of employee theft and fraud is sufficient. This review outlines how the controllers' perceive the causes of employee fraud and how these perceptions, in turn, determine the measures undertaken to control employee fraud. This review



incorporates much of Hollinger and Clark's (1983a) review and evaluation of employee deviance correlates.

Hollinger and Clark's (1983a) literature search yielded five separate, but interrelated, sets of hypotheses explaining employee theft. These include external economic pressure, age of worker, opportunity to offend, job dissatisfaction, and formal policies and informal workplace norms.<sup>2</sup> Hollinger and Clark used a statistical analysis of their questionnaire data to test these five hypotheses. Although they focused on production deviance and on minor forms of theft, their conclusions are useful for a preliminary discussion of the possible cause(s) of employee fraud. Hollinger and Clark admitted that their conclusions do not account for all forms of property deviance, such as major embezzlements.

#### **1. External Economic Pressure**

The external economic pressure hypothesis suggests that the offender is motivated to steal in order to meet a perceived financial need. Cressey's (1953) work on embezzlers best represents this line of thinking. His conclusion was that

trusted persons become trust violators when they conceive of themselves as having a financial problem which is non-shareable, are aware that this problem can be secretly resolved by violation of the

- 
2. Apart from "age of offender," these categories deal with situational as opposed to dispositional factors. According to Litton, criminologists historically have focused on searching for dispositions in individuals or groups to explain criminal behaviour. This predominant focus, however, appears to be misguided since situational factors appear to influence fraud rates (Litton, 1990).

position of financial trust, and are able to apply to their own conduct in that situation verbalizations which enable them to adjust their conceptions of themselves as trusted persons with their conceptions of themselves as users of the entrusted funds or property (p. 30).

Because of the need to meet a financial need, one might expect that a person with such a motivation would not only steal cash but also steal anything that would provide an economic benefit (Hollinger & Clark, 1983a). In support of the conclusion that the lure of money motivates fraud, research conducted by the American Institute of Certified Public Accountants (AICPA) on 119 cases of banking and insurance electronic data processing (EDP) fraud cases as reported by 5127 banks and 854 insurance companies found that

most perpetrators were motivated by the money, some tried to create a better record of their own performance, and only a few for a sense of "self-satisfaction" (1984, pp. 14-15).

As mentioned earlier, Hollinger and Clark designed their questionnaire to detect and explain small-scale thefts of money; therefore, their data cannot test Cressey's "non-shareable problem" hypothesis. However, they argue that their data can be used to make valid conclusions about the causes of employee theft. They compared personal income, income adequacy, financial concern, and community pressures against the self-reported incidence of theft and found "little evidence to support the hypothesis that employees become involved in theft because of greater economic pressure" (1983a, p. 61).

## **2. Age of Worker**

Research repeatedly concludes that younger workers are over represented in employee theft statistics, a correlation that is also found for most index crimes. In addition to confirming this fact, Hollinger and Clark's (1983a) data indicate that younger employees are less likely to have tenure, are more concerned about their education and future career than about their present job, anticipate leaving their present job for another, and are unmarried. Hollinger and Clark concluded that the over-representation of younger workers in employee theft statistics is a function of their marginal position within the company rather than a function of their age. This marginalized status of youths may also account for their high rate of involvement in index crimes. Their low social status not only provides the motivation to commit crime, but also makes it more difficult to escape prosecution and conviction.

## **3. Opportunity to Offend**

Fraud-control experts in industrial security and in internal audit departments frequently advocate directing the organization's attention and resources to the reduction of opportunities to commit fraud and theft. The primary assumption underlying this tactic is that every employee is greedy and dishonest by nature and will steal if a sufficiently tempting opportunity exists. A greater number of opportunities results in a greater number of employee thefts.

The key to controlling this behaviour is to understand and to reduce the "relative levels of opportunity that the employee has to steal" (Hollinger & Clark, 1983a, p. 8).

This assumption can be criticized on three grounds: First, the approach that emphasizes removing all opportunities to steal implies an overly negative view of human nature and of the worker's propensity to steal. Second, by emphasizing the effectiveness of formal control measures, attention and resources are diverted away from apparently more effective informal control measures (Hollinger & Clark, 1983a). Third, by emphasizing formal control measures, there is little attention given to the dynamic nature of rule negotiation within the work environment.

For Albrecht, Howe, and Romney (1984), the opportunity to commit fraud is a significant factor in the explanation of employee fraud. They argued that embezzlement is determined, to varying degrees, by "personal characteristics," "situational influences," and "opportunity factors." From their review of the literature on criminal records, legal documents, and a computer fraud file, they concluded that fraud is a consequence of an interaction among these sets of variables. By manipulating these variables, controllers can increase or decrease the incidence of employee fraud.

Also, Hollinger and Clark (1983a) found a relationship between opportunity and reported employee theft, subject to some qualifications. Those employees having regular access to some products are more likely to steal those products than are

other employees with irregular access. Also, merchandise with intrinsic value is more likely to be stolen if the opportunity to steal is available. However, increased access to raw products (ie., those that become valuable only after the manufacturing process is complete) does not bring about greater theft rates of those products. Finally, although hospital employees perceive the victimization of a hospital as acceptable, the victimization of hospital patients is unacceptable. In sum, Hollinger and Clark concluded that the opportunity to offend is an important, albeit secondary, factor in causing employee theft; informal social controls deter employee theft most effectively.

#### **4. Job Dissatisfaction**

Some theorists have argued that "conditions in the work place may exacerbate or even be the primary cause of theft" (Hollinger & Clark, 1983a, p. 8). Instead of being a passive victim, the organization plays an active role in determining the level of theft by employees by "influencing their perceived level of dissatisfaction with their jobs" (Hollinger & Clark, 1983a, p. 8). Consequently, organizations desiring to control employee theft need to evaluate and to make appropriate changes to their internal operations if they are to decrease theft rates.

Hollinger and Clark (1983a) found support for the hypothesis that employees who are more dissatisfied with their job and who expect to search for work elsewhere in the near

future report higher theft rates. It is a relationship that exists for all age groups. Hollinger and Clark concluded that social conditions internal to, and not external to, the work environment affect employee theft rates.

#### **5. Formal Policies and Informal Workplace Norms**

The final explanatory theme<sup>4</sup> discussed by Hollinger and Clark (1983a) concerns how informal and formal organizational policies influence the amount of employee theft. Again, the explanatory variables are intrinsic to the work place; theft patterns are influenced simultaneously by informal social structure (ie., workplace norms and relationship between supervisors and employees) and by formal ones (ie., policies, hiring, inventory control, security and punishment).

Several researchers have concluded that the informally established normative consensus of the work group regulates employee deviance (Cressey, 1953; Hollinger & Clark, 1983a; Horning, 1970; Tittle, 1980; Sieh, 1987). These work group norms, which regulate employee theft, are malleable. This malleability is related to several possible conditions in the workplace: an applicable norm may be non-existent; an inconsistency between two or more applicable norms may exist; a consensus on the appropriate definition of a norm within a particular work group is absent; or a discrepancy exists among departments on which norm is applicable. Hollinger and Clark (1983a) defined this concept as "normative incongruity" where an entire span of behaviours can be placed upon a continuum,

with perfect normative clarity at one end and normative confusion at the other. For those "gray" issues, employees analyze the actions of supervisors and of co-workers to determine an act's acceptability. Hollinger and Clark found employees' perceptions of informal co-worker sanctions to more strongly influence their behaviour than their perceptions of management's more formalized sanctions.

Hollinger and Clark (1983a) found that lower rates of employee theft are consistently related to formal measures, such as corporate-theft policy, checks on previous work performance, inventory vulnerability, satisfaction with inventory controls, security size, security sophistication, and apprehensions and terminations for theft. However, the impact of these organizational controls is neither uniform nor very strong.

Hollinger and Clark concluded that informal controls are more effective than formal controls in minimizing the amount stolen. In their self-report survey, Hollinger and Clark (1983a) found that

employee perceptions of informal co-worker sanctions consistently demonstrated stronger negative coefficients than the threat of more-formalized sanctions promulgated by management.... [This is] consistent with previous studies conducted in different social settings; employee behavior seems to be constrained more by the anticipated reaction to deviance by one's fellow co-workers than the threatened formal reaction on the part of management.... [This] relationship between formal- and informal-sanction threat and employee deviance persists independent of the employee's age, gender, and marital status (pp. 123-124).

From this, Hollinger and Clark concluded that employee deviance and theft can be viewed as a "dynamic process involving both structural and interpretive factors" (1983a, p. 133). Workplace rules are manipulated by workers to meet the work group's needs. The environment becomes an arena for negotiation between the supervisors and the work group over which acts are punishable and which acts are acceptable.

An issue relevant to my research, but not specifically addressed in the literature, concerns questions about the extent to which workplace norms affect the stealing of larger sums of money from an organization. In light of Hollinger and Clark's (1983a) admission that their conclusions fail to account for large scale thefts, it is possible to conceive of an offender stealing money, particularly sums exceeding petty cash, for monetary gain. Indeed, the offender's external situation may better predict money theft than the quality of informal controls (cf. Cressey, 1953). Conversely, a person's self-perception may prevent him or her from defrauding the company even when there exist few informal controls to inhibit such behaviour. Consequently, a wide variety of causes of employee fraud necessitates a wide variety of deterrence and detection measures. Unfortunately, until research attempts to address the causes of employee fraud in greater detail, the explanations of employee fraud are speculative.

In sum, the factors associated with employee fraud can be inferred from research on employee theft. First, the opportunity to commit a fraud appears to facilitate, but not



determine, the occurrence of employee fraud. However, an attractive opportunity to defraud is only one factor that is considered by the offender.

Second, a cognitive adjustment in the offender's thinking is required before engaging in employee fraud. Such adjustments appear to be shaped by one's "verbalizations" (Cressey, 1953), by "work-group norms" (Henry, 1978), or by utilizing "techniques of neutralization" (Hollinger, 1991).

Third, a person must be sufficiently motivated to steal money. The question of whether this motivation to defraud is internal or external to the organization is unclear. Hollinger and Clark (1983a) concluded that the motivation to defraud is related to some variable found within the work environment. As mentioned earlier, Hollinger and Clark's research does not directly evaluate either the "non-shareable problem" hypothesis (Cressey, 1953) or the hypothesis that people steal goods chiefly for the purpose of exchanging merchandise with friends and family (Henry, 1978). As a result of this uncertainty, my research discusses fraud-control measures that focus on both internal and external motivations, in light of the possibility that the motivations for employee fraud and theft differ.

It appears that a concise delineation of the cause(s) of employee theft and fraud is impossible given the present level of knowledge of the subject. Although academics have the luxury of pondering these causes over long periods, this uncertainty fails to provide employers with clear ideas on how

to respond to employee fraud. Employers would probably agree with Shepard and Dustin's (1988) conclusion that,

to be practical, employers cannot wait until psychologists and sociologists resolve their debate over whether people have a propensity to steal or whether theft is caused by their workplace environment. Corporate policies to reduce employee theft must rely on several approaches, even if the theoretical assumptions underlying them differ.... Employers must attack the problem from both sides (pp. 32-33).

It is these corporate policies and practices to which I now turn.

#### D. Employee-Fraud-Control Measures

Although the prevalence and the nature of employee fraud is largely unknown, and the causes even less so, organizations have in place several policies and practices that have as their primary or secondary goal the control of employee fraud. Uncertainty surrounding the incidence and the cause of employee fraud makes it difficult to establish a standard against which the effectiveness of an employee-fraud-control program can be judged. Any evaluative research on the effectiveness of fraud-control measures should incorporate a discussion of the effects of the economic environment, the inter-organizational interactions, and the intra-organizational interactions.

The question is, which combination of factors shapes the policies and the measures used by internal audit departments in their attempt to define, deter, prevent, detect, and investigate employee fraud? To answer this question, I begin

by discussing the relationship between the correlates of employee fraud and the control measures used to control employee fraud. Next, I discuss the economic influences, the intra-organizational influences, and the inter-organizational influences (with a special focus on the Certified Fraud Examiners Association) on employee-fraud controls. Finally, attention is directed towards outlining the present state of employee fraud controls as shaped by these factors.

**1. Issues Arising from the Relationship between the Correlates of Employee Fraud and Control Measures**

According to Hollinger and Clark (1983a) and Henry (1978), work group norms are the primary regulator of employee theft and fraud. As such, an organization should emphasize social controls over physical controls, and informal work group controls over formal management controls. The role of formal controls is important to the extent that they shape the possible responses from co-workers; however, unilateral decisions by management only exacerbate the problem of employee fraud (Henry, 1978; Hollinger & Clark, 1983a). Instead, management must understand the dynamic of negotiation that is undertaken in the development and implementation of a theft policy and, to the extent that it is possible, seek the cooperation of workers when creating the desired work climate. This would mean that employees clearly understand the organization's definition of employee fraud, the likelihood of being caught, and the ensuing sanction (Hollinger & Clark, 1983a). Supervisors would have the primary responsibility for

employee theft and fraud control, with internal auditors playing a supplementary role (Henry, 1978).

For those who believe that external situational influences are the determining cause of employee fraud, other policies and procedures are more effective. Again there needs to be some cooperation between the controllers and the controlled. Management should take the primary role of intervening in employees' negative off-the-job situations (ie., those that may influence theft or fraud rates) by assisting employees resolve those difficulties. Such measures may include using credit checks at the time of hiring, offering counseling to individuals undergoing interpersonal problems, or providing financial assistance to individuals with financial problems. For Cressey (1953), the aim is to create in employees a self-perception that prevents them from victimizing the organization.

For the proponents of an opportunity model, the internal audit department's role in the control of employee fraud is similar in importance to that of the supervisory management. Judging from the professional literature addressed to internal auditors, the restriction of opportunities to reduce employee fraud is a more effective approach than using informal controls. Theoretically, by removing all opportunities to defraud, all employee fraud can be eliminated. Practically, however, such a singular focus on opportunities will fail for two reasons. First, the costs of policing and of preventing fraud can be so expensive that the organization may not profit

from its effort. Second, the complexity of most work environments compels management to trust employees with making discretionary decisions about money under their control.

In sum, the perceived cause of employee fraud undoubtedly affects what kind of measures are used by organizations. Unfortunately, the unknown motivation for employee fraud makes the development of an employee-fraud-control program very difficult. When adding to this equation the numerous economic, organizational, and external pressures that influence policies, one realizes that every organization's employee-fraud-control program has been shaped by the pushes and pulls of many competing organizational goals.

## **2. Economic, Intra-, and Inter-Organizational Influences upon Employee-Fraud-Control Measures**

The study of employee-fraud-control measures requires a discussion about dominant factors that affect an organization's employee-fraud-control policy. These economic, intra-organizational, and inter-organizational influences leave their mark, to varying degrees, upon all organizational directives. Although these influences generally do not play a direct role in the offender's decision to defraud or not to defraud, these variables affect the nature of the official response to the fraudulent act once it occurs. Even though a correct understanding of the cause(s) of employee fraud is necessary for the reduction of employee fraud, the economic, intra-organizational, and inter-organizational factors greatly impact the type of fraud-control program implemented.

A study of an organization's employee-fraud-control policy should evaluate the policy's importance in light of other organizational priorities. Pursuing profit, serving customers, expanding market-place share, and maintaining good relations with other organizations all rank higher in priority than the control of employee fraud. When decisions about organizational expenditures are made, fraud-control initiatives usually receive low priority.

The department that has the primary responsibility for the control of employee fraud may experience a lack of cooperation from other departments. The nature of employee fraud and the breakdown of trust between the employer and the employee may run counter to all other company objectives. To openly acknowledge employee fraud may serve to publicize antagonism and conflicts in the workplace. Hence, organizational controllers can either pursue employee fraud and run the risk of increasing any antagonism in the workplace or refrain from determined employee-fraud control and thereby expose the organization to future financial injury.<sup>3</sup>

---

3. Jason Ditton (1979) argued a different opinion in his research on employee theft. In his view, management uses employee-theft control as a means to exert control over the work environment. The discretionary use of sanctions usefully serves the goals of corporate profit-maximization by encouraging individualism over collectivism in the workplace. Supervisors can legally release troublemakers when they charge them with employee theft; meanwhile, they retain desirable employees by overlooking their theft. In this way, the responsibility for employee-theft control is a desired and effective management tool.

#### a) Economic Influences

Probably, the over-riding influence that affects the shape of an employee-fraud-control program is the economic climate internal and external to the organization, such as inflationary pressures, current labour contracts, minimum levels of profitability as set by the board of directors, and the organization's capital liquidity. Although companies may have extra-economic goals, these depend upon the organization's ability to perpetuate its existence through the acquisition of profits. Therefore, employee-fraud control, like all other policies, is pursued mainly for the perceived economic benefits. Henry's (1978) review of the research led him to conclude that the increased attention to hidden economies (in the 1970s in the UK), which he defined as "the illegal trading of goods which are condoned and governed by the work group" (pp. 140-141), comes during difficult economic times when there are pressures to save money.

#### b) Intra-Organizational Influences

The research of Henry (1978), Ditton (1979), and Hollinger and Clark (1983a) focused primarily on the supervisor-employee relationship. Their research portrays the management team as acting in unison on issues of employee theft; there are no exceptions to the norm. For their purposes, this level of analysis was sufficient, but to understand more completely the manner in which departments develop and maintain fraud policies, research should take into

account the internal dynamics of organizational decision-making. Research on employee-fraud-control policies must look beyond the supervisor-employee relationship.

Gardiner and Lyman (1984) analyzed the control of welfare and health-care fraud in the United States as an series games. Although the authors focused primarily on inter-organizational dynamics, this metaphor is extendible to analyzing intra-organizational dynamics. These "games" involve circles of debate surrounding general issues in which "players" who have a vested interest play some role in the decision making. The players can be departments, such as internal audit or corporate security, or a group of workers who have a similar job description, such as insurance claims centre managers or claims adjusters. The "resources" that are accessible to players are determined by their organizational status, since these resources can be unevenly distributed among them. The players' resources may include their control over certain information, their particular expertise, and their place in the chain of command. These "players utilize their resources in accordance with game rules to win desired outcomes of the policy issues which define the game" (Gardiner & Lyman, 1984, p. 29). The issues that are part of an "administration game" may come in conflict with the issues of a "criminal justice game" (Gardiner & Lyman, 1984, p. 29). The broader issues of developing priorities, of emphasizing particular types of fraud, and of establishing the amount of funding available for employee-fraud control are decided by the company's senior



officials. Following the resolution of each game, technical issues are determined by specialists. One result is that the resolution of these games affects the character of the more minor policies, such as employee-fraud control.

Gardiner and Lyman (1984) identified several patterns that characterize game playing. Foremost is the role that incentives play in determining support for an initiative. Players who see a net incentive for complying with a policy will comply. Players who perceive a net disincentive will oppose the policy. Since an effective fraud policy requires cooperation among staff, management, internal audit, and corporate security, incentives need to exist for each player. However, line managers' incentives for employee-fraud control may come into conflict with their incentives to provide efficient service and to maintain a trusting work environment. For internal audit, there are not the same incentives for creating a trusting work environment as there are for accounting for all of an organization's assets. Consequently, when the policy of fraud control comes up for debate, line management tends to push for increased autonomy and the internal audit department tends to push for increased accountability.

Gardiner and Lyman (1984, pp. 109-117) outline several incentives and disincentives that determine the extent to which control agencies, such as internal audit departments, maximize control activities. An internal audit department will be rewarded when meeting at least five objectives: (a)

recovering overpayments and containing costs; (b) improving customer service; (c) building a record concerning "overpayments identified" and "investigations completed" for present and future accounting; (d) maintaining good cooperative relationships by assisting other departments; and (e) achieving the professional satisfaction that comes with completing a complex investigation. Internal audit departments may engage in the following activities in order to avoid the associated unwanted consequences: (a) avoiding those cases that require a great deal of effort; (b) avoiding those responsibilities, such as a lengthy fraud investigation, that have a narrow benefit/cost ratio; (c) focusing on those activities that serve as the basis of their internal evaluation, such as completing a certain number of audits, rather than those activities which are not evaluated, such as the "flagging" of suspicious employee activities; and (d) ignoring those cases where there is the possibility that they will lose control over the investigation.

Gardiner and Lyman (1984) identified other patterns that occasionally arise during the course of the game playing. These patterns include the following: (a) competition between departments over jurisdiction, colloquially known as "turf wars"; (b) conflict between field staff and headquarters over decision-making autonomy; (c) active avoidance of unwanted responsibilities by passing blame onto another group; and (d) inter-departmental antagonism over the supervising

department's ability to second guess the decisions of field staff.

c) Inter-Organizational Influences

Along with economic and intra-organizational influences, inter-organizational factors affect an organization's employee-fraud-control policy. Although Henry's (1978) work focuses on the hidden economy, his discussion of the influence of the private security industry will serve as a basis for my discussion of employee-fraud control. Henry (1978, pp. 140-141) identified three such external pressures: the general trend towards more formalized labour relations; the adoption of principles of industrial democracy; and the growth of the private security industry.

Of all these influences, Henry (1978) argues that the private security industry exerts the greatest pressure on employee-fraud-control measures. Surpassing the growth of the public police force, private policing grew because of the reluctance of public police to become involved in seemingly civil issues, and because of reduced expenditures on public policing (Henry, 1978). According to Henry (1978, pp. 140-141), private police organizations created a public concern over employee theft in at least seven ways: (a) persuading the public, judiciary, and customers that something must be done to control increases in theft losses; (b) motivating industry officials to engage in risk management; (c) using management theory to address security issues; (d) presenting

to employers the concern that "perks" were the "thin edge of the wedge" when it came to theft; (e) advocating tougher policies on reporting and prosecuting fraud; (f) familiarizing managers and supervisors with loss prevention techniques; and (g) pushing for legislation about security concerns.

The private security industry perspective has made inroads into the auditing field indirectly through trade journals and through the expanding influence of the Certified Fraud Examiners Association (CFEA). The professional literature of internal auditors predominantly focuses on the need to remove the opportunities to commit fraud. Included in this literature is a host of security measures for auditors, such as preventative fraud audits and proactive computer fraud detection measures. The CFEA, which comprises police officers, security officials, and auditors, attempts to increase its membership by offering certificates to successful applicants. To join this association, an applicant must have some academic and work experience, pass an entrance exam, and attend a certain number of workshops in which various forms of fraud prevention, detection, and investigation are taught (Certified Fraud Examiners Association, 1993).

### **3. Nature and Extent of Organizational Employee-Fraud-Control Measures**

In the context of the many influences affecting formal employee-fraud-control measures, a set of policies and procedures is developed. My research discusses the measures presently used by internal audit departments, whereas, much of

the previous research has focused on management's role in the hospital, retail, and manufacturing industries (Ditton, 1977, 1979; Henry, 1978; Hollinger & Clark, 1983a). My research focuses on those measures that directly or indirectly involve the cooperation of the internal audit department.

The decision to categorize what policies and operations are *fraud* policies and operations depends partly upon the interpretive skills and purposes of the researcher. At least two issues need to be kept in mind when one begins to make this distinction. First, a policy or procedure may serve multiple purposes, one of which is crime prevention or crime detection. Second, any information originally collected independent of any fraud-control purpose may be used to secure a dismissal or a conviction of an employee at some future date. My research discusses only those policies and practices where the *primary* purpose is employee-fraud control.

a) Corporate Responsibility for Employee-Fraud Control

Following the recommendations of the Cohen Commission and the Treadway Commission, there has been a great deal of debate about the desirable extent of the internal audit department's role in employee-fraud control. With regards to the deterrence of employee fraud, and according to the Statement on Internal Auditing Standards, management is to have the primary responsibility of deterrence (Institute of Internal Auditors, 1985). The internal audit department is not to become involved in "drafting procedures, designing,

installing, and operating systems...[since these activities are] presumed to impair audit objectivity" (Institute of Internal Auditors, 1981, p. 1).

For Grove, Lee, and Hanbery, the Treadway Commission set out the three ways in which companies can accomplish the goal of deterring and detecting fraudulent financial reporting: education of management by the independent auditor and internal auditor; policy development (ie., codes of conduct, accounting controls, administrative controls, management controls, physical security, computer security (The Internal Auditor and Fraud, 1990, p. 3)) by management and internal auditing of those policies; and monitoring of internal controls by the independent and internal auditors (1988, p.14). The internal audit department is to assist

in the deterrence of fraud by examining and evaluating the adequacy and the effectiveness of control, commensurate with the extent of the potential exposure/risk in the various segments of the entity's operations (Institute of Internal Auditing, 1985, p. 3).

Concerning the detection of fraud, the Certified Internal Auditor Code of Ethics states that a Certified Internal Auditor (CIA) must not "knowingly be a party to any illegal or improper activity" (Institute of Internal Auditors, 1968, in Meier & Rittenberg, 1986, p. 37). Whether simple knowledge of an act becomes "party to an act" is unclear; however, it does appear that auditors must act on this knowledge in some way (Meier & Rittenber, 1986, p. 37). At the same time, a CIA must "exhibit loyalty in all matters pertaining to the affairs

of the employer or whomever they may be rendering a service" (Institute of Internal Auditors, 1968).

According to the IIA, the internal audit department should be responsible for the following: (a) "have sufficient knowledge of fraud to be able to identify indicators that fraud might have been committed" (the auditor's knowledge does not have to be equal to that of a person whose primary purpose is to detect and to investigate fraud), (b) be alert to any control weakness and conduct any necessary tests for any indicators of fraud, (c) evaluate the indicators of fraud and decide whether an investigation should be recommended, and (d) "notify the appropriate authorities within the organization if a determination is made that there are sufficient indicators of the commission of a fraud to recommend an investigation" (Institute of Internal Auditors, 1985, pp. 5-6).

Other factors associated with effective fraud detection include a suspicious mindset, appropriate audit techniques and tools, and an audit environment that does not place undue time constraints on the completion of assignments (The Internal Auditor and Fraud, 1990, p. 3). Sweeney argues that the internal audit department has a secondary responsibility to detect fraud. However, if auditors conduct their audit according to professional standards (ie., those that a reasonable auditor would follow as dictated by their profession), they should not be held accountable for fraud detected after an audit (Sweeney, 1976, p. 16). The inability to guarantee fraud detection is due to these factors: (a)

manager's and employee's use of judgment in decision-making, (b) the inherent limitations of internal control measures, (c) the use of sampling methods to evaluate internal controls, and (d) the fact that the majority of the evidence is persuasive rather than conclusive in nature (Murusalu, 1991, p. 58).

The IIA states that the internal audit department is usually part of the investigative team, which includes lawyers, investigators, security personnel, and other specialists inside or outside the organization (Institute of Internal Auditors, 1985, p. 7). If the internal audit department is to become involved in the investigation, it should (a) "assess the probable level and the extent of complicity of fraud"; (b) "determine the knowledge, skills, and disciplines needed to carry out the investigation"; (c) "design procedures to follow in attempting to identify the perpetrators, extent of the fraud, techniques used, and cause of the fraud"; (d) "coordinate activities with management personnel, legal counsel, and other specialists as appropriate throughout the course of the investigation;" and (e) "be cognizant of the rights of alleged perpetrators and personnel within the scope of the investigation and the reputation of the organization itself" (Institute of Internal Auditors, 1985, pp. 7-8). Following the investigation, the internal audit department should, based on the facts of the case, determine if controls need to be implemented, design audit tests to uncover similar frauds in the future, and use the case as an aid to identify future indicators of frauds



(Internal Auditors, 1985, p. 8). In the areas of prosecuting and adjudicating cases of employee fraud, the IIA does not address this issue in any form.

When internal auditors report to senior management about employee fraud during or after an investigation, the IIA gives auditors the following guidelines: (a) "when the incidence of significant fraud has been established to a reasonable certainty, management or the board should be notified immediately"; (b) the management or the audit committee should be informed of any frauds where the previously undiscovered fraud had a materially adverse effect on past financial statements; (c) the written report at the end of the investigation should include all findings, conclusions, recommendations, and corrective action taken; and (d) "a draft of the proposed report should be submitted to legal counsel for review" (Institute of Internal Auditors, 1985, pp. 9-10).

#### b) Definition of Employee Fraud

The only studies that have attempted to describe how controllers define what acts are punishable by dismissal or a criminal charge have been from the perspective of supervisors. Hollinger and Clark (1983a) found that hospital and manufacturing management focus their attention almost exclusively on employee behaviour that obstructs the organization's pursuit of its primary goals. Hollinger and Clark also found that property deviance is perceived to be more serious than production deviance. Henry (1978) and

Ditton (1979) have both concluded that the discretionary application of formal policy is often used strategically, either for distributing "perks" or for dismissing undesirable employees.

c) Deterrence and Prevention of Employee Fraud

According to the IIA, management is to assume the primary responsibility of deterrence. The IIA defines deterrence as "those actions taken to discourage the perpetration of fraud and limit the exposure if fraud does occur" (Institute of Internal Auditors, 1990, p. 3). The Treadway Commission concluded that the "tone at the top" should create a corporate environment that discourages fraud (The National Commission on Fraudulent Financial Reporting, 1987, pp. 32-33). This is accomplished through the establishment of an internal control function and the development of a written code of conduct. When it comes to the development of this code, Henry (1978) advocates cooperation between managers and employees, while Albrecht, Howe, and Romney (1984) assume that this responsibility should be the sole responsibility of the management team.

The Commission recommended that the company's audit committee should be composed entirely of independent directors who annually review the management program to monitor compliance with the code (The National Commission on Fraudulent Financial Reporting, 1987). The audit committee may require the internal audit department to conduct this

review. In a survey of 42 retail companies in the United States, over 50% of the audit committees reported that they look to the internal audit department to detect fraud (McKenzie, 1989, pp. 11-12).

The research has shown that the deterrent effect of a corporate policy is as much related to the extent of its promulgation as it is to the development of its contents. Hollinger and Clark (1983a) found that corporate policies on theft tend to be understated during the course of business, discussed only during initial orientations, or hidden in an employee manual. For example, few employees can recollect their company's theft policy; rather, they remember policies relating to essential work responsibilities (Hollinger & Clark, 1983a). Hollinger and Clark (1983b) found that the deterrence of employee fraud increases with both the increased certainty of detection and the increased severity of the punishment.

#### d) Detection of Employee Fraud

The ability of auditors, security officials, personnel officials, and managers to readily identify employee fraud is questionable. The effectiveness of fraud-detection techniques is unclear, and the threat of failure is a disincentive to those thinking of undertaking fraud-control initiatives. Part of the difficulty rests with the problematic nature of fraudulent intent. Also, the internal auditor's distance away from the facts of a case casts doubt on his or her ability to

accurately second-guess the intentions and decisions of the "experts," who are more intimate with the facts of the situation in question. Auditors are forced to assume the "good faith" of management but to still maintain a sense of professional skepticism (Murusalu, 1991).

The research on detection rates has consistently found that only a small percentage of thefts come to the attention of co-workers, supervisors, security, or police (Henry, 1978; Hollinger & Clark, 1983a). Of those offenses that do come to the attention of co-workers and supervisors, management decisions on whether an offender should be sanctioned affect official offense rates (Hollinger & Clark, 1983a). For example, Gardiner and Lyman (1984) found that security officials focus their attention on those providers who receive a high number of payments and who have billing practices that differ significantly from others.

#### e) Investigation

Although Gardiner and Lyman (1984) found that the initial motivation to investigate fraud is the amount of loss, they found three factors that influence the decision about who should investigate a case of fraud: the ease of proving intent; the investigator's understanding of appropriate investigation techniques; and the investigator's knowledge of financial records.

Henry (1978) identified several abuses of justice associated with the investigation and prosecution policies of

private companies. First, the decision to take legal action often depends "upon the employer's personal knowledge of, or dislike for, the person concerned" (Henry, 1978, p. 130). Second, as a result of inconsistencies among companies' policy of investigation and prosecution, some offenders receive harsher sentences than others. Third, compared with the formal, public, and technical judicial decision-making of public justice, private justice operates with minimal evidential and procedural requirements. Hence, Henry's recommendations for adjudicating employee theft centers on the establishment of workplace courts. With the goal of eliminating the secrecy surrounding dispositions, elected employees and managers would publicly adjudicate decisions.

#### f) Reporting

The research on the reporting of employee theft and fraud has found a general reluctance to report these acts. This reluctance is found in the worker-manager reporting relationship (Henry, 1978; Hollinger & Clark, 1983a) and in the company-police reporting relationship (Crocker & Kukeil, 1953; Henry, 1978; Hollinger & Clark, 1983a; Wagner, 1979). In their study of accountants working at independent audit companies, Crocker and Kukeil (1953) found that auditors are more likely to report thefts by non-accountants than by accountants. Becker and Costello (1991) found that 97% of audit and security departments reported fraud to senior management. However, Mautz, Tiessen, and Colson (1984) found

that 10% of internal audit directors representing various industries could not report the discredited practices of corporate officers (ie., senior management) to the "proper authorities within the organization without fear of jeopardizing their position" (in Tiessen & Barrett, 1989, p. 44).

Henry (1978) offered four reasons why companies under-report employee theft to the public police. First, employers may feel a humanitarian responsibility to someone who has a close relationship with the company. Second, a lack of reporting may indicate pragmatic business sense; any undesirable attention from the press or the court may foster a negative public image. Third, a company may fear reprisals from the offender, especially in a unionized environment. Fourth, the numerous economic costs that a company incurs by investigating and prosecuting cases may inhibit an employer's decision to proceed by the criminal process or by civil action.

#### g) Prosecution

The research on the prosecution policies of companies indicates a reluctance to prosecute (Berghuis & Paulides, 1985; Henry, 1978; Wagner, 1979). Gardiner and Lyman (1984) found that some cases are more likely to be prosecuted than others. Those cases that are more likely to be prosecuted include those where the fraud appears to be blatantly defiant, the case is easier to process, and the control over the

disposition can be maintained (Gardiner & Lyman, 1984). Wilson et al. (1985) identified several obstacles encountered by investigators in their attempt to have prosecutors take on cases of physician fraud. These included the low priority given to fraud cases, the difficulty in determining the offender's intent, and the importance attached to higher profile violent crimes. Gardiner and Lyman (1984) stated that law enforcement officials attempt to perform their tasks in ways that maximize rewards and minimize strains for the organization and the individuals involved.

In their study of reported frauds in the banking and insurance industries in the United States, Albrecht, Romney, and Howe found that 51.2% of reported cases resulted in prosecution. The breakdown of the sanctions are as follows: no action (1.5%); disciplined (0.5%); transferred (0.5%); terminated but not prosecuted (34.1%); terminated and prosecuted (51.2%); and other sanction (12.2%) (1984, p. 25). Of the cases where the perpetrator was terminated and prosecuted (51.2%), 97.7% resulted in a guilty verdict. However, only 31.4% of those so convicted were incarcerated, with 52% of these incarcerated for two years or less (1984, p. 25).

### **III. THEORETICAL FRAMEWORK**

The purpose of my research is to analyze the role of the internal audit department within the Canadian insurance industry. Due to the absence of a well-defined theoretical

framework on employee fraud, this research will proceed both inductively and deductively. Data on the definition, deterrence, prevention, detection, and investigation of employee fraud will be collected and then discussed in light of previous research on formal theft- and fraud-control measures. On the basis of this data, a profile of the internal audit departments' role will be developed. Also, I will develop a description of the factors shaping policies to control employee fraud.

Although several factors influence an organization's employee-fraud-control policy, detailed discussion will be limited to only a few of these. First, I will discuss the cause(s) of employee fraud, as outlined in the literature, in light of the fraud-control measures undertaken by internal audit departments.

Second, there will be a discussion of the intra-organizational dynamics that affect internal audit's employee-fraud-control program. Much use will be made of Gardiner and Lyman's (1984) game metaphor to explain the issue of departmental cooperation, the division of fraud-control responsibilities, the incentives and disincentives for entering into the employee-fraud-control game, and the proactive and reactive nature of internal audit's initiatives.

Finally, there will be a discussion of inter-organizational influences upon an organization's employee-fraud-control measures. I will focus on the attempt of the Certified Fraud Examiners Association to increase its presence



within internal audit departments. Specifically, I will address the issues surrounding the employment of persons with a CFEA designation, the definition of employee fraud, and the beliefs about what "causes" employee fraud.

The discussion will now turn to the questionnaire and the sample.

## CHAPTER 2: METHODOLOGY

### **I. INTRODUCTION**

The purpose of this research is to study internal audit managers' perceptions of the policies and practices of internal audit departments of Canadian insurance companies in relation to the control of employee fraud. The research method includes a literature review, my experience during six months of working in the internal audit department of a western Canadian insurance company, and the collection of questionnaire data. After analyzing the data in light of the extant literature on employee theft, employee fraud, embezzlement, and hidden workplace economies, a profile of perceptions of the policies and activities of internal audit departments will be constructed.

### **II. LITERATURE SEARCHES**

Literature searches are enhanced by using an over inclusive list of key words and by using all possible sources of listings (Cooper, 1989). When conducting my literature search, I perused key word indexes to identify those subject headings that would be used when searching various sources. The literature search included several data bases, and either a computer or a manual search was conducted. Some key words were useful for some sources but not for others. Whenever possible, the key words "employee fraud," "employee theft," "fraud," and "workplace crime" were searched. In an attempt

to reduce "disciplinary bias," I searched several disciplines of thought. The searches undertaken are listed in Appendix 1.

### III. WORKING IN AN INTERNAL AUDIT DEPARTMENT

During the course of the development and distribution of the questionnaire, I was employed for six months by the internal audit department of a large western Canadian insurance company. I was hired to research the role of internal audit departments in other Canadian and American insurance companies and to prepare a report on the methods used by internal auditors in the deterrence, detection, and investigation of employee fraud. Although I did not engage in any employee-fraud-control initiatives on-going at the time, I familiarized myself with the general and specific responsibilities of employee-fraud-control personnel of the various corporate departments. In this way, my work experience assisted me in developing a profile of internal audit department policies and practices.

### IV. DATA COLLECTION

#### A. Choice of Units of Analysis

I undertook several steps to select the units of analysis for this research. First, using the *Financial Post's Top Companies Index* for 1991, 48 of the largest insurance companies in Canada were selected. A company was selected for this index by the publisher if it had

1) annual revenues of \$10 million or more, 2) assets of \$5 million of (sic) more, or 3) 500 employees or more. The editors used some discretion in the

selection process, influenced by the availability of information and by areas of special interest. Most of the information presented has been obtained from the companies themselves supplemented by reference to other published sources considered to be reliable (Gurvich, 1991, p. vii).

Second, I attempted to contact each internal audit manager (sometimes referred to as the director) by phone for the purpose of asking for their participation in the study. Of the 48 companies, two managers could not be reached because a proper telephone number could not be located. Also, as this study focuses on the role of Canadian internal audit departments (as opposed to the internal audit function), all companies without a separate internal audit department at their Canadian site or those without an internal audit department in the company (14/46) were dropped from the sample. It was found that several Canadian subsidiaries have their internal audits conducted by their parent company in the United States. For some smaller Canadian companies, the audit function is carried out by their corporate controller.

Self-administered questionnaires were sent to the remaining 32 companies. The managers returned 18 questionnaires for a 56% response rate. The primary reason for not returning a completed questionnaire, as stated by internal audit managers, was a lack of time to devote to a questionnaire. One company sent back two responses, one for each regional office in Canada. Because their completed questionnaires were sufficiently dissimilar, they were treated as two separate internal audit departments. A second respondent, who is the internal audit manager for three

companies included in the list of 32, sent back a single questionnaire. Since the subject of analysis is the audit department, this act was interpreted as a single response.

In sum, each company in the sample has the following characteristics:

1. It is a Canadian company.
2. It has a separate internal audit department within the organization, or it has an internal audit department in a Canadian parent company.
3. It has an annual revenue of \$10 million or more, has assets of \$5 million or more, or has more than 500 employees.

#### B. Company Goals and Operational Environments

Insurance companies share certain goals and methods. These similarities include the following: (a) each company has the goal of maximizing insurance policy sales and of minimizing its claim payments; (b) for each company, the chief commodity is money, and (c) for each company, the computer is the primary tool used to manipulate money.

Some differences in the method of operation exist among companies. First, the type of insurance sold varies across the group of companies. Some companies sell only automotive insurance, while others sell automotive, life, or general insurance or all three. Second, the nature of the work environment varies among companies. Some companies have extensive computerized operations; others have more limited

operations. Third, some companies directly employ persons to sell insurance policies while, others use independent brokers. The question of whether independent brokers are considered to be, or not to be, employees affects statistical comparisons among companies -- an issue that is discussed in Chapter 3. Finally, three of the companies are government-owned while the others are privately owned.

### C. Preparation of Questionnaire

#### **1. Operational Definitions**

Usually, regulations and controls can be circumvented in more than one way. Due to the numerous ways that fraud may be committed, I operationalized "employee fraud" in the same manner that Hollinger and Clark (1983a) operationalized "employee theft." They divided employee theft into two types: property deviance and production deviance. Then, they identified the more common ways in which these types of deviance occur in the manufacturing, retail, and hospital industries.

In the same way, my research attempts to operationalize employee fraud according to the more common ways it occurs in an insurance company. First, a general definition of "employee fraud" was provided to the subjects.<sup>4</sup> Second, behaviours such as "theft of corporate cash" and "put in a fraudulent claim or loan" were selected to represent employee

---

4. Respondents were asked to define fraud as those "cases where there has been an attempt to use deception to obtain a tangible or non-tangible reward."

fraud. These behaviours were chosen in light of the research and literature (eg., trade journals) on employee-fraud control, the advice given by the three internal audit managers with whom I worked, and the information collected during the pre-test process.

## **2. Structure of Questionnaire**

The questionnaire includes 42 questions and took approximately 45-60 minutes to answer. The questions were pre-coded, but space is provided in each question to allow for other responses. The pre-coded responses in the questionnaire assisted the respondents with their recollection of facts. The use of an "other" response section for each question helped to identify those practices and policies that are used but are not mentioned in the literature or were missed by the author.

## **3. Focus of Questionnaire**

The questions focused on the following: (a) corporate reporting structure; (b) internal audit department structure; (c) internal auditors' education and training; (d) corporate and internal audit department responsibilities for fraud deterrence, detection, and investigation; (e) internal audit department manager's rank-ordering of various acts of employee theft and fraud according to the sanction that should follow; (f) number of employee-fraud investigations conducted in the last 12 months; (g) internal audit department's methods of deterrence, prevention, detection, and investigation; (h) the

focus of control measures; and (i) reporting of fraud investigations. An analysis of the results appears in the next two chapters. A copy of the questionnaire can be found in Appendix 2.

#### **4. Pre-Testing the Questionnaire**

After the SFU Ethics Committee approved this research, the questionnaire underwent a pre-test. I interviewed the managers of ten internal audit departments representing a variety of industries in the Greater Vancouver Regional District. After this pre-test, the questionnaire underwent minor adjustments. In helping to develop the questionnaire, three internal audit managers identified additional response codes for various questions.

In addition to this pre-test, the internal auditors of 13 banks and trust companies were asked to describe their attempts to deter, prevent, detect, and investigate employee fraud. This information served to further ensure that the questionnaire addressed areas of concern relevant to the financial industry.

#### **D. Delivery of the Questionnaire**

After an introductory telephone call, the subjects received a letter requesting their participation in the study and a copy of the questionnaire. Where questionnaires were not returned after two months, a follow-up call was made.



**CHAPTER 3: THE QUESTIONNAIRE: A WINDOW ON THE WORLD OF THE  
INTERNAL AUDIT DEPARTMENT**

**I. INTRODUCTION**

This chapter discusses the questionnaire results under the following headings: (a) company employment, premiums, and computer environment; (b) internal audit departments' structure; (c) organizational responsibilities for employee-fraud control; (d) internal audit department managers' definition of employee fraud; (e) deterring and preventing employee fraud; (f) detecting employee fraud; and (g) the internal audit departments' investigation of employee fraud and the departments' follow-up report. Of the 32 internal auditors contacted, 18 returned a completed questionnaire (56%). Unless otherwise stated, all statistics will be based upon 18 responses.

Before discussing the findings of the research in detail, this chapter begins with a general overview of the findings.

**II. OVERVIEW OF RESULTS**

The typical insurance company employs 2032 people who sell, administer, and disburse millions of dollars to clients in a highly computerized environment.

The internal audit manager has regular access to a Vice-President to discuss administrative issues and has direct access to the President, Chief Executive Officer (CEO), or Chief Financial Officer (CFO) to discuss employee fraud. The average audit department has 10 managers and staff for an employee/auditor ratio of 194:1. Approximately 65% of

auditors have a professional designation granted by an accounting or auditing association. Most of an internal auditor's education about employee fraud comes from attending professional conferences and reading professional literature.

Corporate responsibility for the deterrence, detection, and investigation of employee fraud is widely dispersed throughout the corporation, but the internal audit department is the dominant player. This relative dominance of the internal audit department may be related to the absence of an investigation unit and a data security department in several companies. In a few companies, a single person oversees employee-fraud control, usually an internal audit department manager.

When evaluating the seriousness of employee theft and fraud, factors considered by internal audit include the following: (a) the intention of the offender, (b) who was directly victimized by the theft or fraud (ie., in descending order of seriousness, frauds and thefts against the company, against co-workers, against clients, and against other companies), and (c) the type of theft or fraud. The data indicate that property deviance is perceived to be more serious than production deviance and that cash theft is perceived to be more serious than property damage.

In the attempt to predict future fraudulent behaviour, companies attempt to deter employee fraud by conducting background checks and by administering integrity tests to prospective employees. However, the measures used by the

internal audit department centre on the restriction of the opportunities to defraud by developing secure computer environments and by educating management and employees about internal controls.

In detecting employee fraud, the internal audit department uses a series of computer-assisted measures. Internal auditors focus primarily on employees who use computer systems within the claims centers. To a much lesser extent, internal auditors audit senior management for fraud. Less than one percent of employees were investigated for fraud in the preceding 12 month period. Most frauds were perpetrated in the operations of disbursements and policy sales.

The majority of employee-fraud allegations arise from employee tips, external sources, and internal audits, with internal auditors claiming that employee tips are the most useful source of employee-fraud allegations. Employee tips are a useful source regardless of a company's reporting policy. Notably, few allegations result from management reviews (a fact that may be related to the absence of mandatory reporting policies for managers). A complete record of allegations is seldom kept.

Internal audit maintains a high level of involvement in both civil and criminal investigations, particularly in companies without a separate investigation unit. The investigatory responsibility for employee fraud is shared among various departments. Police seldom conduct the initial

criminal investigation and are more frequently resorted to later in the investigation. Forensic accountants are seldom used by companies.

Internal auditors regularly conduct a preliminary investigation into suspicious transactions, using a variety of company records and interviews. The final decision to prosecute or dismiss, however, rests with another level of management. Dismissals are administered in-house, always without other employees involved in the process, with criminal sanctions processed in a criminal court.

### III. COMPANY EMPLOYMENT, PREMIUMS, AND COMPUTER ENVIRONMENT

#### A. Number of Employees

Of 17 companies responding, the smallest company had 250 employees and the largest company had 6300 employees. The average number of employees was 2032 employees.<sup>5</sup>

#### B. Amount of Revenue, Premiums, and Deposits

Although the questionnaire attempted to identify the yearly revenues, the premiums, and the deposits for each company, an average amount was not calculable. Only one company gave information for all three categories, and two

---

5. All statistics using "number of employees" should be treated as approximations. First, most respondents wrote down rounded figures. Second, these figures are inconsistent, it was discovered, with those figures listed in the *Financial Post's Top Company Index* for 1991. Third, some respondents included in their figures given in my questionnaire the number of independent sales staff who sell insurance policies for the company. Other respondents did not include these persons, thereby under-reporting the total number of persons audited by internal audit.

gave information for two categories. For nine of the 18 companies, the amount of yearly premiums ranged from \$177 million to \$4250 million.

### C. Nature of Companies' Computer Environment

Although research indicates that internal auditors perceive batch processing as less risky than on-line real-time processing and the latter as less risky than a microcomputer under user control (Collier, Dixon & Marston, 1991, p. 51), such a perception may be unjustified. The American Institute of Certified Public Accountants (AICPA) studied 119 cases of fraud, which were reported by independent auditors in the American banking and insurance industries, that were committed using electronic data processing (EDP) equipment. The research found that the type of computer system was not significant, since fraud "occurred in both batch and on-line systems" (1984, p. 6).

In my research, 14 companies have some computer systems that use "on-line real time" (ie., when data are typed into the computer, the computer records are immediately incorporated into the information system) and other systems that use regular batch updates to a company database. The remaining four companies, which have an average of 1268 employees, have microcomputers connected to a company mainframe. From my research, the internal auditors' perceptions about the relative risk of the two types of computer system can not be ascertained. However, since 78% of

the companies operate in a similar environment, a comparison between internal audit departments can be made.

#### **IV. INTERNAL AUDIT DEPARTMENT'S STRUCTURE**

##### A. Reporting Hierarchy for the Internal Audit Department

As expected, the internal audit department is part of the management team and reports directly to the company's senior management. Sixty-seven percent of internal audit departments report regularly to a Vice-President. The priority that senior management gives to employee-fraud control is evidenced by the fact that, when employee fraud is the topic of discussion, 94% of internal audit departments have direct access to the President, to the CEO, or to the CFO. At the same time, the remaining six percent of auditors that do not have access to the top manager may experience the same reluctance as those auditors who felt they were jeopardizing their position if they reported the fraud of corporate officers (Mautz, Tiessen, and Colson, 1984, in Tiessen & Barrett, 1989).

After an employee-fraud investigation, the President, CFO, or CEO receives the final report in 83% of the cases.

##### B. Number of Managers, Staff, Support Staff, and Secretaries

An internal audit department has, on average, three managers, six audit staff, and one support or secretarial staff member. The internal audit department has one staff member for every 194 employees.

### C. Staff Educational Background

The 157 managers and audit staff have 102 professional titles (eg., CA, CGA, CIA) distributed among themselves. Similar to other research, my data indicate that only a small minority of internal auditors have the title of Certified Internal Auditor (CIA) (5 of 157 internal auditors or 3%). It may be that many of the internal audit managers are members of the IIA,<sup>6</sup> which awards the title of CIA. If this is the case, one could expect internal auditors to align themselves with the IIA statement on the deterrence, detection, investigation, and reporting of fraud (Institute of Internal Auditors, 1985).

Those experienced in fraud investigation suggest that internal auditors who investigate employee fraud should be able to collect and retain evidence, conduct interviews, use a variety of investigative procedures, conduct financial analysis, collect and manipulate data, and have a basic understanding of civil and criminal law (Leech, 1990, p. 3). In light of this responsibility, trade journals repeatedly call for increasing the knowledge base of auditors in relation to employee-fraud control. One way in which this education can be accomplished is through the attainment of a CFE professional title, which is awarded to those who have studied the many responsibilities surrounding employee fraud. However, in my research, only one auditor has this professional title, and no auditor has a professional title

---

6. Research has found that many internal audit department managers are members of the IIA (Mautz, Tiessen & Colson, 1984, in Reinstein & Weirich, 1988, p. 45).

from any other security association. All other professional titles were granted by accounting, auditing, or insurance educational institutions.

In my research, when internal auditors were asked how they were educated about employee fraud, the respondents identified the following ways: attend fraud seminars or conferences sponsored by the IIA or by the CFEA association (65%); read professional literature (59%); use in-house discussions (53%); and use the resources of anti-fraud organizations (35%) (Table 3.1). This moderate level of education appears to reflect the findings of Albrecht, Howe, and Romney that internal auditors have limited training "regarding the legal rules associated with evidence or action to ensure the usability of audit evidence in a court case" (1984, p. 29).

---

**Table 3.1 Internal Auditors' Education  
on Employee Fraud**

---

	Number of Responses	%
IIA or CFE Conferences	11	65
Personal Readings	10	59
In-house Discussions	9	53
Anti-fraud Organizations	6	35
University/College/Technical Schools	2	12
Other	2	12
Consultants	1	6

---



## V. ORGANIZATIONAL RESPONSIBILITIES FOR EMPLOYEE-FRAUD CONTROL

### A. Corporate Use of Investigation Units

The investigation units of insurance companies are staffed by persons with prior training and experience in public police work. These units focus on the detection and investigation of external fraud, and they may be involved in the investigation of internal fraud. If involved in an internal investigation, they tend to perform the traditional investigative work (ie., witness interviewing, document collection, public record searches, etc.,) (Kramer, 1989, p.8). Five companies in my sample have an independent investigation unit. The other 13 companies control external fraud by having an investigative function carried out within the claims department, within the internal audit department, or by external security firms. Since the presence of a separate investigation unit within a company may affect the investigative responsibilities of the internal audit department, companies with a separate investigation unit will be analyzed separately.

### B. Central Responsibility for Employee-Fraud Control

When using a conservative estimate of the incidence of employee fraud, the average auditor will detect and investigate fraud infrequently throughout his or her career. If one combines this fact with the moderate level of education about fraud that auditors receive, one can conclude that the average auditor's fraud-control skills are limited. It is

possible that such an auditor is more likely to ignore an indicator of fraud or to compromise an investigation than an auditor well-experienced in fraud control.

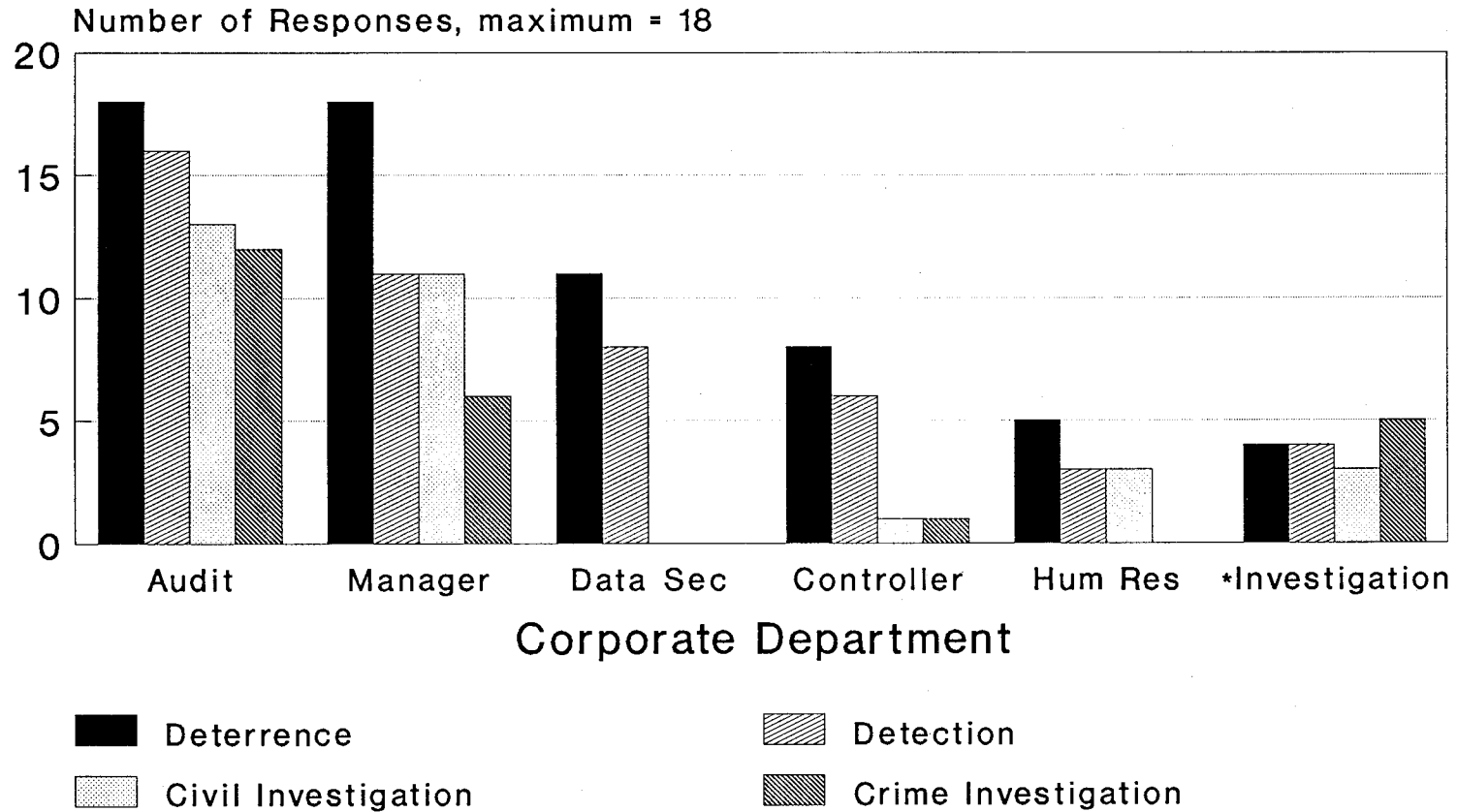
In what may be an attempt to address this issue, five companies (27%) have placed the primary responsibility for employee-fraud control on an individual manager. In four of these companies, one of which has a separate investigation unit, the internal audit department manager has this responsibility. In the other 13 companies, the responsibility for employee-fraud control is distributed among various departments.

### C. Responsibility for the Deterrence, Detection, and Investigation of Employee Fraud

#### **1. Deterrence and Detection**

Although the IIA clearly states that the deterrence of fraud is the responsibility of management, internal audit managers perceive deterrence as a primary or a secondary role for their department (Figure 3.1).

Figure 3.1 Corporate Responsibility for the Deterrence, Detection, and Investigation of Employee Fraud



\* Only 5/18 companies have a separate Investigation Unit

My research found that internal audit department managers believe their department has a primary or a secondary responsibility in the detection of employee fraud. According to internal auditors, in 89% of companies, the internal audit department is responsible for fraud detection; in 61% of companies, line managers are responsible for fraud detection (Table 3.2). The high level of responsibility afforded to the internal audit department occurs even in those five companies with a separate investigation unit. In these companies, the investigation unit is less involved in employee-fraud detection in 40% of cases.

---

**Table 3.2 The Responsibilities for Detection of Employee Fraud by the Internal Audit Department and Line Management**

---

	<u>Audit Responsible</u>	<u>Audit Not Responsible</u>
Managers Responsible	10	1
Managers Not Responsible	6	1

---

These findings are consistent with research on internal audit departments representing various industries in the United Kingdom. In the latter study, it was found that the responsibility for the prevention and detection of computer fraud was placed specifically on the internal audit department (59% (prevention) / 52% (detection) of companies) (Collier, Dixon & Marston, 1991, p. 50). In the same study, the

responsibility of the internal audit department for the prevention and detection of fraud was either assigned formally (46% / 38% of companies), informally (38% / 36%), or self-imposed (31% / 28%) (Collier, Dixon & Marston, 1991, p. 50).

Another consistency between my study and the U.K. study is the finding that the responsibility for deterrence and detection is shared among departments. In my research, internal audit managers perceive the deterrence of employee fraud as a responsibility of line management, the internal audit department, the investigation unit (or corporate security department), the data security department, and the corporate controller. With regards to the detection of employee fraud, only two of 17 (12%) respondents perceive internal audit department's responsibility to be exclusive. Of the remaining 15, four (24%) perceive the detection of employee fraud as a shared responsibility between the internal audit department and one other department. The remaining 11 (65%) respondents perceive the detection of employee fraud as a responsibility to be shared among the internal audit department and three or more departments (Figure 3.1). Other departments (if they exist in the company) partially responsible for fraud detection include the data security department, the division of corporate control, the human resources department, the corporate law department, and the investigation unit.

## 2. Investigation

Due to the criminal and civil nature of fraud, an allegation of employee fraud may be resolved in either a criminal court or a civil court. The manner in which an allegation of fraud is settled may determine who conducts the investigation and what procedures are used during the investigation. Extant research suggests that employee-fraud allegations are more often settled as a civil issue than as a criminal issue (Henry, 1978; Hollinger & Clark, 1983a). My research did not attempt to identify the percentage of employee-fraud cases that led to civil proceedings or criminal proceedings or both. My research, however, did survey which departments had a responsibility in the case of both civil and criminal investigations.

Generally, I found that when a case proceeds towards a civil hearing (in 13 of 17 companies (76%)), the internal audit department has a primary or secondary investigatory responsibility. In these 13 companies, the line management in seven companies (54%) does not have any investigatory responsibility. In four of these 13 (31%) companies, the internal audit department conducts the investigation exclusively. In the five companies where the internal audit department does not have an investigatory role, primarily line management conducts the investigation.

In the case of an investigation leading to a criminal hearing, my research indicates that the internal audit department has a high level of investigatory responsibility.

(12 of 18 companies or 67%). Line managers have an investigatory responsibility in six of 18 companies (or 33%).

a) Companies Without a Separate Investigation Unit

When the results were analyzed after separating companies without separate investigation units from those with separate units, the internal audit department still has a high level of responsibility in the investigation. For instance, in companies without a separate investigation unit, the internal audit department is most likely to conduct internal civil and criminal investigations alone (5 of 13 companies or 39%). In these 13 companies, when there is inter-departmental cooperation on employee-fraud investigations, internal audit has a higher participation rate in both civil (9 of 13 companies or 69%) and criminal investigations (9 of 13 companies or 69%) than have other departments (Table 3.3).

**Table 3.3 Responsibility For Employee-Fraud Investigations  
in the Thirteen Companies without a Separate  
Investigation Unit**

<u>Type of Hearing</u>	<u>Civil</u>	<u>Criminal</u>
Audit alone	5	5
Manager alone	3	2
Corporate Law alone	0	1
Human Resources alone	0	0
Audit & Corporate Law	1	1
Audit & Manager	1	1
Manager & Corporate Law	1	1
Audit & Police	0	1
Audit & Manager & Corporate Law & Controller	1	1
Manager & Audit & Human Resources	1	0
<u>Total</u>	<u>13</u>	<u>13</u>

b) Companies with a Separate Investigation Unit

As was the case in companies without a separate investigation unit, the internal audit department of companies with a separate investigation unit maintained a high level of responsibility in both the civil and criminal investigative process. In cases that will be adjudicated in a civil hearing, the internal audit department usually plays some part in the employee-fraud investigation (in 4 of 5 companies). When the case will be adjudicated in a criminal court, the internal audit department also plays a role in the investigation (3 of 5 companies); however, the internal audit department's role in criminal investigations is slightly less



than that of the investigation unit (4 of 5 companies). Whether a civil or a criminal case, the internal audit department shares the investigatory responsibility with another department in seven of possible 10 cases (Table 3.4).

**Table 3.4 Responsibility for Employee-Fraud Investigations in Companies with a Separate Investigation Unit**

<u>Type of Hearing</u>	<u>Civil</u>	<u>Criminal</u>
Audit alone	0	1
Investigation Unit alone	0	2
Manager alone	0	0
Human Resources alone	0	0
Audit & Manager	1	0
Audit & Investigation Unit	0	1
Audit & Human Resources	1	0
Manager & Investigation Unit	1	0
Audit & Manager & Investigation Unit	1	1
Audit & Manager & Human Resources	1	0
<b>Total</b>	<b>5</b>	<b>5</b>

c) Companies Using a Committee to Oversee Employee-Fraud Investigations

Although the IIA statement on the deterrence, detection, investigation, and reporting of fraud does not suggest a committee format to oversee fraud control, the statement does suggest that all available resources within an organization be utilized. My data do not identify the extent to which the internal audit department fulfills the suggestion that it "coordinate activities with management personnel, legal

counsel, and other specialists as appropriate throughout the course of the investigation" (Institute of Internal Auditors, 1985, pp. 7-8). However, it does indicate that only three of 18 companies (17%) have established a formal committee to oversee employee-fraud investigations.

Of the three companies with a formal committee, two have representatives of various departments sit on a committee and oversee employee-fraud investigations. In one of these companies, the committee was represented by the internal audit department and by two company vice-presidents. The other company's committee had representatives from the corporate law department, the treasury department, the investigation unit, the human resources department, and a senior departmental manager. The committee that oversees employee-fraud investigations for the third company was comprised of the audit committee of the board of directors. Notably, neither employees nor a legal department were said to be represented on any of these committees. In the three companies, the internal audit department is always involved in both the civil and the criminal investigations. Also, the internal audit department usually shares the investigatory responsibility with another department (4 of 6 companies) (Table 3.5).

**Table 3.5 The Responsibilities of Committees to Oversee Employee-Fraud Investigations**

<u>Type of Hearing</u>	<u>Civil</u>	<u>Criminal</u>
Audit alone	1	1
Audit & Investigation Unit	0	1
Audit & Police	0	1
Audit & Manager & Human Resources	2	0
<u>Total</u>	<u>3</u>	<u>3</u>

d) Role of Legal Counsel in Employee-Fraud Investigations

It has been recommended that legal counsel be sought, whether internal or external, when conducting an investigation to establish attorney-client privilege and to otherwise protect the company's interests (eg., prevent disclosure of interview notes, of memoranda, and of other papers that may be harmful in a subsequent legal action against the company) (Kramer, 1989, p. 8). However, in my research, few companies identified their legal counsel as part of either the civil (17% of companies) or the criminal (17% of companies) investigation process.

Similar to Albrecht, Howe, and Romney's study (1984, p. 29), my research indicates that few companies have a formal written policy outlining the steps that are to be taken in order to protect the company, to protect the perpetrator's rights, or to gather and secure evidence (1984, p. 29). Instead, each new investigation is shaped by the

investigator's past experience thereby exposing the company to the potential of future financial injury.

e) Use of Police and Forensic Accountants in Employee-Fraud Investigations

The IIA statement on fraud encourages the use of specialists inside or outside of the organization (1985, p. 7). My study found that very few companies turn to the police in the course of their preliminary, internal investigation. For example, no respondent identified the police as having a primary responsibility for the investigation of employee fraud. Even in the 13 companies without a separate investigation unit, only one company uses the police during the preliminary investigation (8% of companies). However, in six of 18 companies (33%), once the preliminary investigation has been completed (usually by the internal audit department), the case is turned over to the police (the data did not indicate the consistency of this practice). Only three of 18 companies (17%) used the services of an external forensic accountant.

**VI. INTERNAL AUDIT DEPARTMENT MANAGERS' DEFINITION OF EMPLOYEE FRAUD**

In its statement on the deterrence, detection, investigation, and reporting of fraud, the IIA identifies 13 types of fraud, which result in either positive or negative financial consequences for the company (The Institute of Internal Auditors; 1985, pp. 1-2). The IIA, however, does not recommend a penalty for any of these offenses. In order to

determine how companies would punish offenders, I asked internal audit managers whether certain of these acts (marked with an asterisk in Table 3.6) would lead to an offender's dismissal from work or to a criminal charge if this was a "first-time" offense.

**Table 3.6 Number of Companies That Would Fire or Dismiss an Employee for Selected Acts of Fraud, Theft, and Misconduct**

	Number of Responses <sup>7</sup>	%
*Fraudulent claim or loan	16	100
Theft of corporate cash	16	100
*Assist in corporate tax evasion	14	88
Intentional damage of equipment	13	81
Take co-workers' property	13	81
Borrow corporate money without approval	11	69
*Use of corporate information for personal business	11	69
*Exaggerate travel expenses	9	56
Shortchange or overcharge customers	9	56
Take money or gifts from clients	7	44
Let family or friends use corporate perks	6	38
For interest, read restricted data sources	4	25
Fail to report theft of company property	4	25
Copying retail software for personal use	3	19
Theft of company time	3	19
Removal of office supplies	3	19
Working under the influence of drugs or alcohol for one day	1	6
Unauthorized use of office equipment	0	0
Unauthorized use of company vehicles	0	0

7. One respondent stated that some cases would lead to a "warning," and other cases would be a matter of "judgement." "Warning" responses were not interpreted as resulting in firing or criminal charge, but "judgement" responses were so interpreted.

When analyzing this data, two assumptions were made. First, the internal audit department managers' definitions of employee fraud reflect those of senior management. Second, it is assumed that those acts that receive a sanction of dismissal or a criminal charge are more serious than those that do not receive such a penalty. From my study, at least five conclusions can be made.

First, as a general pattern, internal audit department managers perceive property deviance as more serious than production deviance, as was found in the Hollinger and Clark (1983a) study. For example, all companies dismiss or criminally charge employees who engage in a "theft of corporate cash." In contrast, only 25% of companies dismiss or criminally charge employees who "read restricted data sources," only 19% dismiss or criminally charge employees for "time theft," and only 6% dismiss employees who are "working under the influence of drugs."

Second, within both categories of property and production deviance, internal audit department managers view some acts as more serious than others. In the category of property deviance, all companies dismiss or criminally charge employees who "create a fraudulent claim," but only 56% of companies dismiss or criminally charge employees who "exaggerate their travel expenses," even though both acts are a fraudulent expense for the company. With regards to production deviance, 44% of companies dismiss employees who without authorization "receive money or gifts from business clients," but no company

will dismiss or criminally charge employees who engage in "the unauthorized use of company vehicles" or in "the unauthorized use of office equipment."

Third, the offender's intention is an important factor in the decision whether or not to punish. For example, a dismissal or a criminal charge is more likely to follow a "theft" of company cash (100% of companies) than to follow the "borrowing" of cash (69% of companies).

Fourth, the internal audit department managers' perception of seriousness is in part based upon who was victimized by the act. This research found that internal audit department managers perceive those offenses that directly victimize the company as the most serious. In descending order of seriousness, punishable acts are those which victimize the company, co-workers, customers, and other companies. For example, 81% of companies dismiss or criminally charge employees who engage in a "theft of employee property" (co-worker is the victim) whereas only 56% of companies dismiss or criminally charge employees who "shortchange or overcharge a customer" (customer is the victim), and only 19% of companies dismiss or criminally charge employees who "copy retail software for personal use" (another company is the victim).

An exception to the above pattern is the finding that companies perceive as serious any attempt to alter company records for the purpose of tax evasion. It is possible that the company's concern over a fraud committed against an

external organization may be serving self-interest. A company may be liable for an employee's criminal act if the employee acted within the scope of employment and for the company's benefit (Gill, 1986).

Fifth, although companies generally disagree as to what property and production deviances should be sanctioned, some offenses are correlated with a high level of agreement among companies in their decision whether or not to dismiss or criminally charge employees. In 26% of offenses listed in Table 3.6 (ie., fraudulent claim or loan, theft of corporate cash, unauthorized use of a company vehicle, unauthorized use of office equipment, and working for one day while under the influence of drugs or alcohol), 94% of companies are in agreement whether or not to dismiss or criminally charge an employee.

## **VII. DETERRING AND PREVENTING EMPLOYEE FRAUD**

### **A. Corporate Measures Undertaken to Deter and Prevent Employee Fraud**

According to the IIA statement on fraud, management is responsible for the deterrence of fraud. The Treadway Commission recommended that management set the "tone at the top" by establishing an internal control function (which all companies in my sample have done by creating an internal audit department) and by developing a written code of conduct (which 88% have done).



My data indicate that the managers of Canadian insurance companies attempt to carry out this responsibility by educating management and employees about employee fraud and by restricting opportunities for fraud. Deterrence techniques include (Table 3.7) developing a corporate code of ethics or standard of conduct (88%), educating managers about internal controls (77%), and educating employees about the corporate internal controls and employee-fraud policies (53%). However, only a few companies publish information about cases of employee fraud (18%). In addition to establishing an internal audit function, many companies attempt to prevent employee fraud by assessing an employee's propensity for theft. For example, companies conduct credit or criminal background checks (59%) and administer tests designed to determine personal integrity (29%). The use of credit checks is much higher in my sample than in studies of U.S. companies. In the U.S., only 26% of companies representing various industries obtained a credit report on potential new professional employees (McKee & Bayes, 1987, p. 55).

**Table 3.7 Prevalence of Corporate Deterrence Methods**

	Number of Responses	%
Develop a code of ethics	15	88
Education of managers about internal controls	13	77
Credit or criminal checks of employees	10	59
Education of employees about internal controls and fraud policies	9	53
Administer psychological test (integrity) to employees	5	29
Publication of past cases of fraud	3	18
Managers give sign-off statements attesting to their adherence to internal controls	3	18
<hr/>		
17 Respondents		

B. Internal Audit Department's Measures Undertaken to Deter Employee Fraud

In spite of IIA statement that the internal audit department does not have a primary responsibility in fraud deterrence, internal audit departments are directly involved (albeit in a supportive role) in the process, both in reducing and monitoring opportunities, and in educating corporate staff about internal controls. This is evidenced by the internal audit departments' attempts to do the following: (a) test manual controls to see if they can be circumvented (88%); (b) assist in the development of manual controls (88%) and information systems (82%);<sup>8</sup> (c) educate management on internal controls (71%); and (d) educate employees on internal controls (41%) (Table 3.8). The internal audit departments'

8. For a list of software products useful for increased data security, see Graham and Freely's (1990) article.

involvement in the development of computer controls is similar to internal auditors in the U.K. (Collier, Dixon & Marston, 1991, p. 50).

**Table 3.8 Measures Undertaken by the Internal Audit Department to Deter Employee Fraud**

	Number of Responses	%
Test strength of manual controls to see if they can be circumvented	15	88
Assist in the development of manual controls	15	88
Assist in the development of information systems	14	82
Education of managers about internal controls	12	71
Education of employees about internal controls and fraud policies	7	41
Assist in the development of a code of ethics	4	24
Credit or criminal checks of employees	1	6
Publication of past cases of fraud	1	6
Administer psychological test (integrity) to employees	0	0
Managers give sign-off statements attesting to their adherence to internal controls	0	0

In spite of the fact that, in one study, 30% of prospective employees investigated misrepresented themselves on job applications, research has found that 48% of internal audit departments representing various American industries

never audit their company's background investigations, and 15% conducted such an audit yearly (McKee & Bayes, 1987, p. 54). Of those audit departments that did audit background investigations, most (43%) made simple verbal inquiries about what policies were in place and who was responsible for them, and only 14% selected a sample of newly hired employees and conducted an independent background investigation (McKee & Bayes, 1987, p. 55). Although my questionnaire did not specifically ask if the internal audit department audits its company's background investigations, my data (Table 3.8) indicate that only one of 17 (6%) internal audit departments carried out their own criminal or credit check on new employees, either as part of the hiring process or as part of an audit.

### C. Employee Involvement in Deterring Employee Fraud

The extent of employee involvement in employee-fraud control is very limited. It appears to be the case that employees do not have a formal role in the definition of, or in the deterrence of employee fraud. Employee participation is restricted to the reporting of employee fraud. Eight of 18 (44%) companies encourage their employees to report serious employee fraud. In the case of four companies (24%), employees who fail to report a case of theft or fraud may be dismissed.

## VIII. DETECTING EMPLOYEE FRAUD

### A. Incidence and Nature of Employee Fraud

Of 18 respondents, 14 (78%) reported that at least one investigation into fraud or theft had been conducted in the previous 12 months for an average of 5.2 investigations per company. This average indicates that one out of every 375 employees was investigated in the 12 month period.

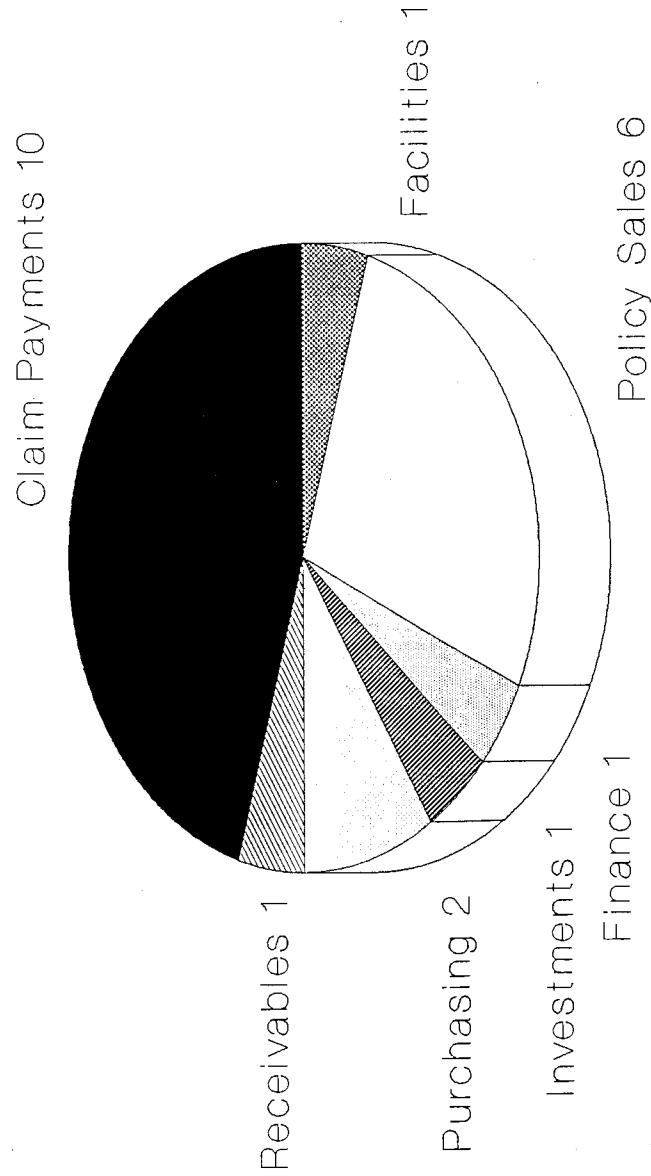
The rate of fraud revealed in my study, which is based on estimates provided by internal audit department managers, is higher than the rate of fraud revealed in studies that compute a fraud rate based on estimates offered by internal audit department managers. Conversely, the rate of fraud revealed in my study is lower than the rate of fraud revealed in studies that use self-report questionnaires. In the AICPA study of electronic data processing (EDP) fraud in the banking and insurance industries, of the 854 insurance respondents, there were only 34 cases of EDP-related fraud, an average of one fraud for every 25 companies (American Institute of Certified Public Accountants, 1984). It should be noted that the AICPA study focused on only one of many types of fraud. They defined EDP-fraud as meeting three conditions: a fraudulent act was done, the act had an impact on the financial statements, and EDP was "directly involved in the perpetration or cover-up of the scheme" (1984, pp. 3-4). In my research, respondents were asked how many allegations of fraud or theft had been investigated in the past 12 months.

The difference in how fraud is defined may explain, at least partly, the differences in the statistics.

My research found that the majority of frauds investigated were detected using sources other than an internal audit. Regardless of the actual incidence of fraud in the insurance industry, the finding that fraud is not usually uncovered in an internal audit means that the internal auditor is largely unsuccessful in fraud detection.

Respondents were asked to identify those corporate operations in which employee fraud occurred in the previous 12 month period. The departments that disbursed funds (ie., claims) were identified by 56% of the respondents. Next, respondents identified departments that generated revenue through policy sales (33%) (Figure 3.3). This would appear to be consistent with the AICPA's findings that most reported EDP-related frauds involve the manipulation of input data (ie., "introduced unauthorized transactions or altered or manipulated authorized transactions" (1984, p. 13)).

**Figure 3.2 Company Operations in Which Employee Fraud Occurs Frequently as Perceived by Audit Managers**



**16 Respondents**

## B. Focus of Employee-Fraud-Detection Measures

Of the time devoted to detecting fraud, the internal audit department appears to focus the majority of its effort on detecting employee fraud rather than management fraud (particularly fraud by senior management). Only 17% of respondents reported using any internal audit measures specifically to detect fraud by senior managers. According to two (11%) of the 18 respondents, the detection of management fraud is the responsibility of the external auditor or of a higher level of management. My finding that internal audit departments focus primarily on employee fraud is contrary to the findings of Mautz, Tiessen, and Colson (1984), who studied the internal audit departments of various American industries. Mautz, Tiessen, and Colson (1984) found that internal audit departments audit employees, middle managers, and senior managers with the same frequency (Tiessen & Barrett, 1989, p. 44). These researchers, however, found that these same internal audit departments usually did not audit certain senior management activities (eg., changes in organizational structure, development of departmental or company budgets, and development of appropriate evaluation measures for branches or departments) (Mautz, Tiessen & Colson, 1984, in Tiessen & Barrett, 1989, p. 44).

If the intention of internal audit departments is to detect the greatest *number of frauds* (as opposed to the greatest amount stolen by fraud), they would need to focus on employees. There is some empirical support for the belief



that the majority of frauds are committed by employees rather than by supervisors, managers, and owners. For example, from their survey of internal audit directors in the insurance industry, Albrecht, Howe, and Romney found that "66.7 percent of the [fraud] perpetrators were clerical workers (1984, p. 22)."<sup>9</sup> Also, Guercio, Rice, and Sherman (1988) found that clerks were involved in 56% of fraud cases, supervisors in 22% of cases, management involved in 19% of cases, and part-owners in 3% of cases (Ernst & Young, 1989, p. 11).

However, if internal audit departments wish to detect frauds that result in the *greatest financial loss*, they should focus on the detection of fraud by supervisors, managers, and owners. An AICPA study found that when a supervisor or manager perpetrated EDP-fraud, the schemes were undertaken over longer periods of time and involved larger dollar amounts (1984, p. 7).<sup>10</sup> Furthermore, Guercio, Rice, and Sherman (1988) found that, on average, clerks stole \$34,579, supervisors stole \$55,622, managers stole 208,898, and part-owners stole \$145,357 (Ernst & Young, 1989, p. 11). Hence, the effectiveness of internal audit departments in limiting the amount stolen as a result of fraud would be enhanced if

- 
9. The authors also found that in "other industry types, the perpetrators were more often described as supervisors" (1984, p. 22). Of all frauds in the insurance industry, 46.4% involved a theft of \$40 000 or less, 35.7% involved a theft of between \$40 000 and \$100 000, and 17.9% involved a theft over \$100 000 (1984, p. 18).
  10. Also found was that computer personnel (ie., systems and applications programmers and operators) were less prominent fraud perpetrators in the insurance industry (Mautz, Tiessen & Colson, 1984, in Tiessen & Barrett, 1989).

departments directed much of their detection efforts towards the detection of fraud by those in authority.

In addition to finding that internal audit departments focus their detection efforts on employee fraud, my research found that they vary in their surveillance of company operations. Some corporate activities are infrequently audited (eg., background investigations conducted by the human resources department). Those employees who disburse funds are more likely to come under the review of auditors than those who deal with physical inventory. One respondent stated that entire branches, including managers and employees, are audited and that all suspicious matters are investigated further. Some support for this differential treatment exists. The AICPA found that claims processors and policy service clerks comprise the majority of EDP-fraud perpetrators (1984, p. 7). However, even if it were true that some groups of employees commit more fraud than others, or that employees commit frauds more frequently than managers, or that managers steal larger sums of money than employees, a deliberate and exaggerated bias in fraud detection measures and policies may become a contentious legal and ethical issue.

### C. Corporate Measures Undertaken to Detect Employee Fraud

It was found that every respondent identified at least one way in which their company attempts to detect employee fraud. However, there does not appear to be a consistent pattern among companies. The more common methods of detecting

employee fraud include the following: identify conflicts of interest (67% of companies); receive tips from external sources (61%) and employees (50%); use a continuous-auditing program to identify exceptional transactions (47%); verify the existence of vendors, suppliers, or employees (50%); and conduct surprise audits (44%) (Table 3.9).

Pilot studies have found that using a "threat team" (ie., a group of specially selected company employees to detect possible fraud schemes) does lead to the detection of weakness in the system of internal controls in both manual and automated systems with little cost (Allen, 1981). Along the same lines, my questionnaire asked if company managers assist in the development of tests to detect fraud. Of the 18 respondents, only six (33%) stated that they use this method. In light of the limited role of managers in developing new fraud-detection tests in cooperation with the internal audit department (only 33% of companies used manager/internal auditor cooperation) and the infrequency that the internal audit department teaches managers how to detect fraud (only 28% of companies did this), it may be the case that internal audit departments have taken on some responsibility for implementing employee-fraud-detection measures (Table 3.9).

**Table 3.9 Measures Undertaken by Insurance Companies  
to Detect Employee Fraud**

	Number of Responses	%
Check for areas of a conflict of interest	12	67
Receive calls from external sources and follow-up on those reports	11	61
Encourage employees to report serious employee fraud	9	50
Verify of the existence of vendors, suppliers, or employees	9	50
Set up a continuous auditing system that produces exception reports	8	44
Conduct surprise audits	8	44
Cooperate with management in developing new tests to detecting fraud	6	33
Educate managers on how to detect employee fraud	5	28
Use an external forensic accountant or a fraud auditor	3	17

D. Internal Audit Department's Measures Used to Detect Employee Fraud

Respondents were asked to identify those measures undertaken by their internal audit department in their attempt to detect employee fraud. Across internal audit departments, a variety of computer-assisted methods are used. The extent to which these measures are used varies. The data indicate that, when a given measure is used by the company, the internal audit department is the one most responsible for

executing this responsibility. A primary measure used by internal audit departments includes the identification and evaluation of "exceptional" transactions (65% of companies). Although there are numerous computer controls that dictate the amount of funds that an employee can disburse or the sources of data accessible to each employee, "exception reports" are used to ensure that employees stay within their authorization and input only correct (ie., non-fraudulent and accurate) data. In companies I studied, exceptional transactions are identified by highlighting data security violations (eg., unauthorized access to a program) (59% of companies), by developing a continuous auditing system (41%), and by comparing information between company databases (28%). These reports highlight suspicious transactions that are usually reviewed by internal audit in the course of an internal audit (Table 3.10).<sup>11</sup> Greenberg, Wolf and Pfeister (1986) found that the benefits of computer-assisted matching programs greatly outweigh the costs of implementing them.

This high level of involvement by the internal audit department in detecting fraud through computer-assisted methods appears to be related to that department's technical expertise. Internal audit is staffed by persons educated in accounting and computing skills or both. However,

---

11. The State Farm Life Insurance Company (U.S.) has developed a program using 33 "embedded audit hooks that monitor 42 different transactions. Any transactions that meet the preselected criteria are identified in a report created for the internal audit department" (Leinicke, Rexroad & Ward, 1990, p. 26).

investigation units are staffed primarily by those with experience in interviewing, techniques and in physical controls. Some support was found for this conclusion in that in each of the investigation units (5 of 18 companies or 28%) no staff member conducts an EDP audit or a fraud audit.

In a minority of companies, internal audit departments use methods that require cooperation with other departments or persons. For example, some internal audit departments receive tips from external sources (35% of companies), encourage employees to identify employee fraud (18%), and educate managers about how to detect fraud (18%).

**Table 3.10 Measures Undertaken by Internal Audit  
Departments to Detect Employee Fraud**

	Number of Responses	%
Develop a system of identifying exceptional transactions*	11	61
Evaluate exception reports exceeding a certain monetary amount*	11	61
Evaluate exception reports outlining data security violations*	10	56
Check for areas of a conflict of interest	9	53
Set up a continuous auditing system that produces exception reports	7	41
Conduct surprise audits	6	35
Receive calls from external sources and follow-up on those reports	6	35
Cooperate with managers in developing new tests to detecting fraud	5	29
Verify the existence of vendors, suppliers, or employees	5	29
Run company databases against each other to detect suspicious employee activity*	5	28
Educate managers on how to detect employee fraud	3	18
Encourage employees to report serious employee fraud	3	18
Use dial up "front-ends" or "traps" to catch computer hackers*	3	17
Develop programs that are used to review physical inventory on a regular basis*	2	11
Use an external forensic accountant or fraud auditor	1	6
Conduct virus scans of company software*	1	6
Run external databases against company databases*	0	0

\*Total out of 18, all others out of 17

Another method used by a minority of internal audit departments (5 of 18 companies or 28%) is that of the fraud audit (ie., an audit in which the primary purpose is to identify fraud). Usually, a fraud audit involves the examination of exceptional transactions. For those five internal audit departments that conduct a fraud audit, the following responses were given:

- Many are used.
- Do not wish to specify. I will say knowledge of the employee's background is helpful.
- We look at the internal control environment study for that employee or department where he works (ie., lack of segregated duties).
- We perform substantive based tests which are tailored to looking for symptoms or patterns of fraudulent activities (eg., in a claims fraud, we look for repeated payments to a company from the same person).
- Surprise audits are done. We take head office files and match them with branch files and then list all service type companies used. If excessively used, further investigation is conducted. The president and officers are not aware which branch is audited.

In those cases where internal audit departments occasionally audit for fraud among senior management (5 of 18 companies or 28%), the respondents stated the following:

- Certain employees must report their buys and sells to audit. Audit then compares these sells with company records and see if a conflict exists.
- Same methods as used for other management staff
- Special internal audit procedures during audits
- A manager more senior to a manager will investigate the nature of the action against



the company to determine the extent of the fraud and its implications.

- External auditors do this.
- None to check

#### E. Reporting of Employee-Fraud Allegations

##### **1. Receiver of Employee-Fraud Allegations**

In the companies I studied, employee-fraud allegations are usually directed to line management (61% of companies) or to the internal audit department (50%) (Table 3.11). In companies where a single person oversees employee fraud control, primarily that person receives employee fraud allegations.

---

**Table 3.11 Receivers of Employee Fraud Allegations**

---

	Audit notified	Audit not notified
Manager Notified	5	6
Manager Not Notified	4	3

---

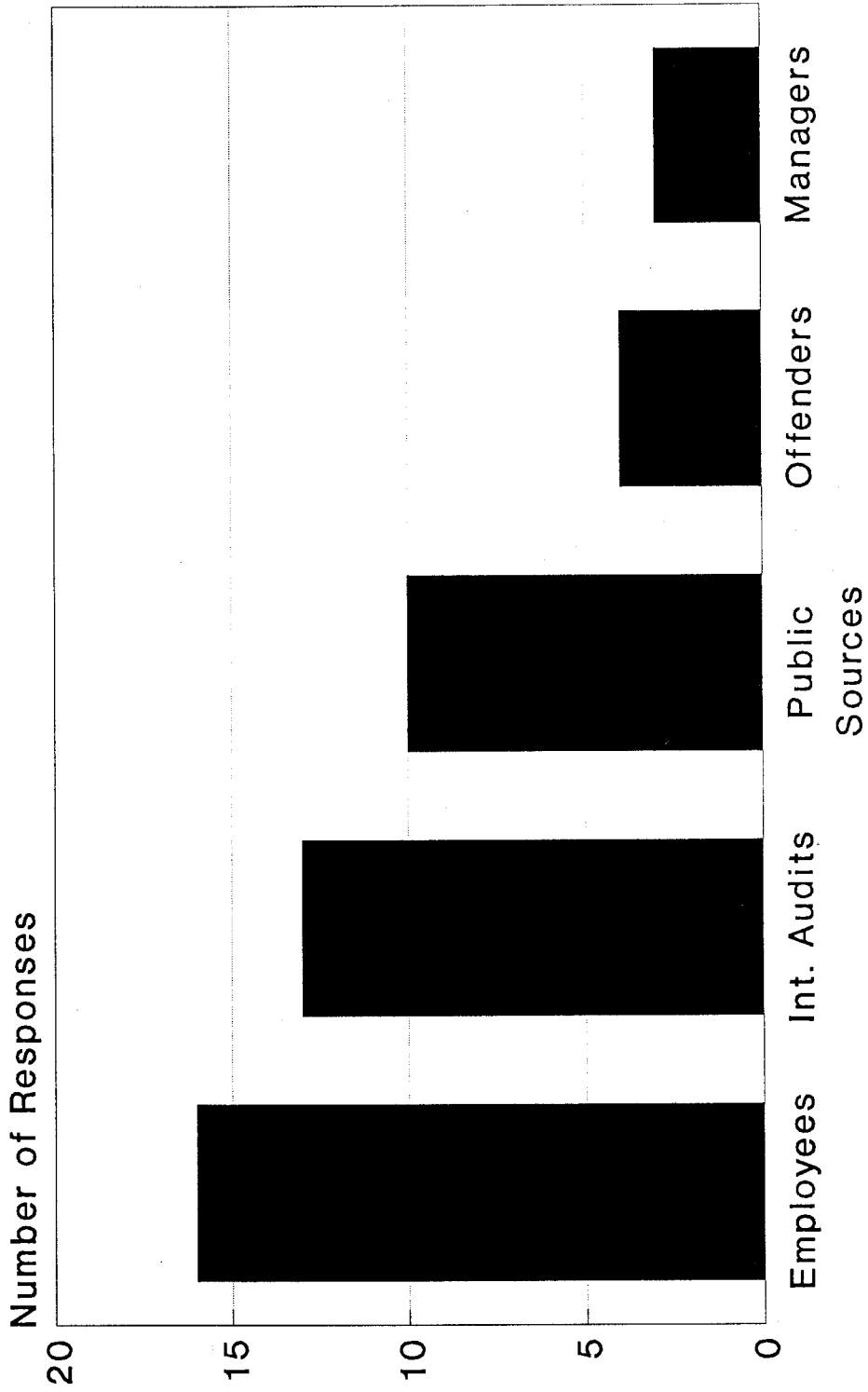
##### **2. Sources of Employee-Fraud Allegations**

Internal audit department managers identified employee tips (89% of respondents), internal audits (67%), and tips from persons outside the company (56%) as useful sources of employee-fraud allegations (Figure 3.3). The usefulness of employee tips to my respondents is consistent with the findings of two other studies. Albrecht, Howe, and Romney

found that internal audit directors reported that most frauds are detected through employee tips, customer complaints, or external tips (32.8%), with only 18% detected through an audit and 18.4% detected through regular departmental reviews (1984, p. 29). The AICPA study of EDP-related fraud found that the person who first found the fraud included other employees (eg., clerks) (47%), middle management (21%), and internal auditors (15%) (1984, p. 18).

The relative infrequency that employee fraud is detected during a managerial review, although consistent with the research, may be partly a function of an absence of a mandatory reporting policy requiring managers to report employee fraud. In no case was there mention or evidence of a mandatory reporting policy. It may be the case that the absence of a mandatory policy to report affords managers the discretion to deal with employee fraud outside of the influence of the internal audit department. In response to this managerial inaction, and the expectation that the internal audit department has a responsibility to detect fraud, the internal audit department may be sufficiently motivated to create and to implement its own measures for fraud detection.

Figure 3.3 Sources of Employee-Fraud Allegations as Identified by Internal Audit Managers



18 Respondents

My study found that some insurance companies dismiss those employees who fail to report employee theft or fraud (24% of companies). Other companies simply encourage employees to report serious fraud (44%). This attempt to have employees undertake a surveillance role, which some research indicates is beneficial (Litton, 1990, p. 32) and many writers advocate (Baker, Barrett, & Radde, 1976; Hollinger & Clark, 1983a; Thompson, 1986; U.S. General Accounting Office, 1986), is consistent with the belief that many perpetrators commit fraud as a result of situational factors. Upon further analysis, my data suggest that employees report employee fraud regardless of whether a company has a reporting policy. For companies that encourage employees to report fraud, employee tips were deemed to be a useful source of allegations in all but one of the nine companies with such a policy. Where companies did not deliberately encourage employees to report fraud, employee tips were equally as useful (Table 3.12).

---

**Table 3.12 Employee Tips and Corporate Reporting Policy**

---

	Useful	Not Useful
Encourage employee Reporting	8	1
Do not encourage employee reporting	8	1

---

Companies also receive tips from persons external to the company. As is the case with employee tips, allegations from

external sources are perceived to be useful sources of allegations. However, internal audit department managers perceived external tips to be less useful than employee, or internal, tips. Eighty-nine per cent (16 of 18 respondents) of internal audit department managers perceived employee tips as useful in identifying fraud, whereas 61% (11 of 18 respondents) of internal audit department managers perceived external sources as a useful source of identifying fraud. The intimacy that employees have with their work environment probably accounts for this difference in perception (Table 3.13).

---

**Table 3.13 External Tips and Corporate Reporting Policy**

---

	Useful	Not Useful
Company receives tips from external sources	8	3
Company does not receive tips from external sources	3	4

---

Several authors of articles in trade journals suggest that fraud can be detected in an audit, whether in a regular audit or a fraud audit. The AICPA study on insurance companies found that the events or factors that triggered the detection of EDP-related fraud were a tip or some unusual behaviour of the perpetrator (44%), internal controls (29%), a routine audit (12%), a customer complaint (12%), and a non-

routine study (3%) (1984, p. 17). My research found that internal audit department managers listed the following as primary ways of detecting fraud: an internal audit (67%); a fraud audit (60%);<sup>12</sup> and an independent, or external, audit (11%). It seems that internal audit department managers perceive the auditing of records to be a particularly useful measure in the detection of fraud.

In those companies where the internal audit manager has the overall responsibility for employee-fraud control (4 of 18 companies or 22%), the respondents found that the regular internal audit and the specialized fraud audit were equally effective detection devices (3 of 4 cases). In those companies where an internal auditor did not have overall responsibility for employee-fraud control, regular internal audits (9 of 14 cases or 64%) and specialized fraud audits (0 of 14 cases) were perceived as less profitable sources of employee-fraud allegations (Figure 3.3). It seems that fraud audits, if they are actually attempted, are useful sources of allegations.

### **3. Recording of Employee-Fraud Allegations**

The questionnaire asked whether or not companies kept a record of employee fraud investigations. Fifteen of the 18 (83%) respondents indicated that the company had no "fraud log" book. This frequency is greater than that found by

---

12. This statistic is based on the five of the 18 respondents who indicated that their department conducts a fraud audit for the purpose of detecting fraud.

Hollinger and Clark (1983a) who found that over 33% of retail, manufacturing, and hospitals had no records on the disposition of employee thieves. Possibly, the absence of an employee-fraud log book may be further evidence that mandatory reporting policies do not exist in these companies.

F. Uniformity in the Skill Level of Internal Auditors in Employee-Fraud Detection

Several writers have maintained that well-trained personnel are essential for detecting employee fraud (Baker, Barrett, & Radde, 1976; Bologna, 1984; Goldstein, 1989). The IIA's "Standards for the Professional Practice of Internal Auditing" states that "the director of internal auditing should establish and maintain a quality assurance program to evaluate the operations of the internal audit department" (1985, Section 560). This program is designed to ensure that the work of the internal audit department conforms to standards<sup>13</sup> applicable to the department. This review could be conducted by supervision of work carried out by the department, by periodic internal reviews (at least every three years), or by external reviews by qualified persons independent of the organization.

Of the 14 companies responding to this question, only three respondents (21%) stated that they evaluate their auditors' compliance to in-house standards for detecting and investigating employee fraud. Research by Zeitlin and Nelson

---

13. Although not mentioned in the 1981 Standards, this would include the IIA's "Statement on the Deterrence, Detection, Investigation, and Reporting of Fraud" (1985).

(1986) found a similar pattern when only 24% of internal audit departments plan to institute a quality control program (as mentioned in the Section 560 of the "Standards for the Professional Practice of Internal Auditing," 1981) within the next three years (in Reinstein & Weirich, 1988, p. 47). The significance of this finding becomes more evident when one considers the finding of Albrecht, Howe, and Romney that internal auditors have limited training "regarding the legal rules associated with evidence or action to ensure the usability of audit evidence in a court case" (1984, p. 29).

**IX. THE INTERNAL AUDIT DEPARTMENTS' INVESTIGATION OF EMPLOYEE FRAUD AND THE DEPARTMENTS' FOLLOW-UP REPORT**

A. Nature of the Internal Audit Department's Investigation

According to the IIA, in addition to coordinating the investigation, the internal audit department should "design procedures to follow in attempting to identify the perpetrators, extent of the fraud, techniques used, and cause of the fraud" (Institute of Internal Auditors, 1985, pp. 7-8). From my research, it appears that there is a high level of consistency among internal audit departments and a high level of compliance with the IIA guidelines. The departments' investigation includes determining how the irregularity was perpetrated (100% of companies), documenting the extent of loss (94%), searching for evidence of additional impropriety (94%), securing all relevant evidence (83%), identifying the



perpetrator of the offense (72%), and determining the location of the offender at the time of incident (67%) (Table 3.14).

---

**Table 3.14 Nature of the Internal Audit Departments' Investigation into Employee Fraud**

---

	Number of Responses	%
Determine how act was perpetrated	18	100
Document extent of loss	17	94
Expand sample and look for additional impropriety	17	94
Secure relevant evidence	15	83
Identify perpetrators	13	72
Determine location of perpetrator at time of incident	12	67

---

The competence of internal auditors in the Canadian insurance industry to properly collect evidence is unknown. Albrecht, Howe, and Romney (1984) found that internal auditors have limited training with regards to the legal rules of evidence or the collection of that evidence. In my research, it was found that auditors underwent only a moderate level of training on employee-fraud control. Add this finding to the fact that the respondents infrequently sought the advice of legal counsel during the *initial* aspects of the investigation (17% for both civil and criminal investigations), and it raises the question whether internal audit departments are

effectively building cases that will have a perpetrator dismissed or criminally charged.

B. Sources Used in an Investigation

In the internal audit department's investigation, auditors utilize information from a variety of sources. The relevance of each source depends upon the nature of the investigation. There appears to be a preference for using work-related records (eg., manager information, performance records, and travel expense files) over external sources of information (eg., credit reports, pre-employment records, police) (Table 3.15).

---

**Table 3.15 Sources of Information Used in the Internal Audit Departments' Investigation into Employee Fraud**

---

	Number of Responses	%
Manager information	16	89
Performance records	15	83
Travel expense files	15	83
Insurance claim or Loan files	14	78
Payroll files	10	56
Credit reports	10	56
Suspect's interview	10	56
Pre-employment records	9	50
Other - Police	1	6

---

C. Procedure Following an Internal Audit Department's Investigation

Following the internal audit department's investigation and before the decision to dismiss or criminally charge is made, the case is usually turned over to a different person or department within the company to dismiss the perpetrator, or to the police before a decision to dismiss or to prosecute is finalized. Of the 18 companies, six (33%) internal audit departments turn the case directly over to the police following their own investigation. Although the IIA (1985) advocates that internal audit department make use of specialists in fraud-investigation who are external to the company, this is the first significant use of such experts in the control of insurance company employee fraud. The remaining 12 companies require the internal audit department to pass the case over a different level of decision-making within the company. In those 12 companies, the case was turned over to the legal department (4 of 12 or 33% of companies), to senior management (4 of 12 or 33%), or to the investigation unit (4 of 12 or 33%).

D. Responsibility for Issuing a Report Following an Investigation

Following an employee-fraud investigation, 100% of companies have someone file an internal report, which is received by the President or CFO in 83% of companies and the Audit Committee in 44% of companies. This report is written by the internal audit department in 78% of companies and by line management in 11% of companies. The report by the

internal audit department identifies the internal controls that were contravened (100%), and some ways to rectify the problem (94%). Some auditors go beyond the guidelines stated by the IIA by giving a list of appropriate sanctions for the offender (69%).

In the effort to limit future injury to the corporation, internal audit departments are encouraged to have their fraud-investigation reports reviewed by legal counsel (Kramer, 1989, p. 8). Although the questionnaire did not ask whether every report to others in the company was initially submitted to legal counsel for review, one may infer from a combination of several responses that the legal department tends to be involved near the end of the investigative process. For those reports distributed at the early stages of the investigation (and possibly those distributed at the later stages as well), it is likely that the legal department does not review these reports.

The AICPA study of 119 EDP-related frauds reported by the auditors of American banks and insurance companies found that the frauds did not involve sophisticated techniques. Rather, they were the result of "weakness in the system of internal accounting control" (1984, p. 6).<sup>14</sup> In the companies I examined, in the effort to prevent future cases of employee

---

14. When internal audit directors were asked about the cause of fraud in the study conducted by Albrecht, Howe and Romney, 50.3% cited the lack of internal controls as the cause of fraud, 37.3% cited the failure to enforce controls, and 12.4% cited a manager's override of controls (1984, p. 28).

fraud, most companies (94%) conduct a follow-up review to ensure proper controls are in place. Most often, it is the internal audit department that completes this follow-up (75% of companies), which is done during a future internal audit.

#### **X. PROSECUTION AND ADJUDICATION OF EMPLOYEE-FRAUD CASES**

My research found that it is management, and not the internal audit department, that decides whether a case of employee fraud will be adjudicated in a civil hearing or treated as a criminal case. In cases tried criminally, the case will be heard in a Provincial Court.<sup>15</sup> For cases where the sanction is dismissal, the role of prosecutor and judge is undertaken in-house by management staff. No respondent reported active involvement by employees either in the definition of employee fraud or in the adjudication of employee-fraud allegations.

These results will now be discussed in the context of the literature on hidden economies, employee theft, and employee fraud.

---

15. The case of *R. v. Olan, Hudson and Hartnett* (1978) outlines the elements of a case of criminal fraud.

**CHAPTER 4: EXPLANATIONS FOR THE INTERNAL AUDIT DEPARTMENTS'**  
**EMPLOYEE-FRAUD-CONTROL PROGRAM**

**I. INTRODUCTION**

This chapter discusses the general patterns found in the questionnaire data in light of the following questions:

(1) To what extent are situational factors and dispositional factors perceived to be the cause of employee fraud?

(2) What intra-organizational incentives influence the policies and procedures of internal audit departments?

(3) To what extent are employees involved in employee-fraud control? and

(4) To what extent is the private security industry influencing the definition, deterrence, prevention, detection, and investigation of employee fraud?

**II. INTERNAL AUDIT MANAGERS' DEFINITION OF EMPLOYEE FRAUD**

**A. Reasons for the Internal Audit Managers' Perception of Offense Seriousness**

There are three reasons why internal audit managers have adopted their prioritization of the seriousness of different types of fraud. One factor is the definition of fraud created by their company. Hollinger and Clark argued that the acceptability of an act is determined by the debate between supervisors and the work-group about structural and interpretive factors (1983a, p. 133). As part of the extended supervisory team, internal auditors may come to incorporate definitions that are particular to that company.

A second factor that affects internal auditors' perceptions, specifically with regard to their perception that property deviance is more serious than production deviance, is the assumption that production deviance is not a serious economic or social problem, an assumption contested by private security officials. With only one audit member having a professional title from a private security association (CFEA), the day-to-day influence of private policing on the internal audit department is marginal. (Many internal auditors attend CFEA conferences and read professional literature written by private security officials.) Perhaps more attention should be focused on production deviance. Baker and Westin found that management perceived "substance abuse and chronic absenteeism ... along with petty theft and abuse of services as much more serious problems overall than major theft and fraud" (1987, p. 7). Furthermore, research indicates that production deviance is more economically costly than property deviance (Hollinger & Clark, 1983a). In the absence of any external motivation to punish production deviance by dismissal or a criminal charge, this apparent refusal by auditors to seek severe sanctions for production deviance may indicate a preference to deal with these issues in a manner different than that of fraud. Although production deviance may be treated differently than fraud, auditors may come to define an employee "perk" (Ditton, 1977c) as a criminal matter.

If auditors expand their definition of theft and fraud, it is probable that such a change would emphasize the acts of

employees over those of managers. As part of the management team, and based on the tendency of individuals to notice positive characteristics of their group and negative characteristics of others, internal auditors may perceive employees as more prone than managers to put the financial health of the company at risk. Research that identified clerks as the most likely to commit fraud would be useful to internal auditors when establishing a basis for their emphasis on employee-fraud investigations.

As well, the relative powerlessness of employees facilitates greater emphasis on their activities over those of managers. Not only are employees perceived as more dangerous than managers, but their powerlessness makes supervision of their work much easier. This makes the deviance of powerless groups easier to detect and easier to sanction more frequently (Williams & MacShane, 1988). This change in the auditors' perception will undoubtedly lead to similar changes in deterrence and detection measures.

#### B. Implications of Internal Audit Managers' Definition and Perceived Seriousness of Employee Fraud

As was the case with Gardiner and Lyman's (1984) finding that definitions of fraud and abuse vary among government departments, definitions of property and production deviance differ among the auditors of different insurance companies that I studied. One consequence of this variation is that there are differences in the frequency of fraud among companies. Therefore, the frequency of fraud in one company



may differ significantly from that in another. In my research, one company reported that 0.3% of their employees were investigated for fraud or theft in the preceding 12 months, and another reported that none were investigated.

Another consequence may be that certain groups will receive a higher level of surveillance than another which has similar opportunities to defraud. If internal auditors believe that employees are more likely to commit fraud, employees will receive greater surveillance. In my research, few internal audit departments search for management fraud, particularly senior management fraud. However, on a monetary basis, research on the insurance industry indicates that management fraud is at least of equal threat to a company's financial well-being as employee fraud (Ernst & Young, 1989).

Another consequence is that an inequality in the sanction received by perpetrators among different companies may exist. For example, employees who exaggerate their travel expenses in "Company A" may be dismissed from their job or have a criminal charge laid against them; meanwhile, employees in "Company B" may commit the same act without receiving either of these serious punishments. In light of this finding, Henry's (1978) argument that variations in sanctioning may lead to an abuse of justice would appear to hold true for the Canadian insurance industry.

### III. THE INTERNAL AUDIT DEPARTMENT'S DETERRENCE AND PREVENTION OF FRAUD

#### A. Corporate Responsibility for Deterrence and Prevention

All 18 respondents saw both the internal audit department and line management as having responsibility for the development of adequate controls to prevent employee fraud. In addition, and although discouraged in the IIA statement on fraud, the internal audit departments of the Canadian insurance industry take on some responsibility in development of internal controls in the effort to prevent employee fraud. Instead of simply evaluating existing internal controls, they provide assistance to management in the development of manual and computer controls (83% of companies in both cases) and in the education of managers about internal controls (67%). In addition to their involvement in preventing employee fraud, internal audit departments make recommendations to senior management about how offenders should be sanctioned (69% of companies). Hence, internal audit departments play an active role in the deterrence of employee fraud.

#### B. Emphasis of Deterrence and Prevention Measures in Favour of Detection Measures

When asked what types of prevention and detection measures are used by the internal audit department, the respondents appear to use preventative measures more than detection measures. Since the internal audit department is obliged to serve the needs of management, the auditor's preference can be assumed to reflect that of management's.

Indeed, this managerial preference is similar to that found by Baker and Westin's (1987) study in which most senior corporate professionals in the United States preferred on-the-job controls over pre-employment screening and criminal justice intervention. It is, however, not known to what extent management ideas *determine* the policies and practices of internal audit departments and to what extent management perceptions are *shaped* by internal audit departments. Also, the extent to which the factors that shape *both* management and internal audit departments are similar is not known.

In addition to the direct control that senior management has on the policies and practices of internal audit departments, two other factors may account for the emphasis on deterrence measures. First, the educational background of internal audit staff emphasizes the restriction of opportunities over the detection of fraud. In the course of obtaining the title of CA, CMA, or CGA, the auditor is primarily trained to evaluate internal controls. In my research, only one of 157 internal audit department staff had a certificate or professional title from an association that emphasized detection nearly as much as it did prevention (CFEA), and only five of the 157 had the title of a Certified Internal Auditor (CIA). Also, those departments that engaged extensively in fraud detection had an investigation unit incorporated into their audit department.

A second factor that may influence the preference of deterrence measures over detection measures, but that cannot

be evaluated by my data, is that a cost/benefit analysis favours deterrence. Because the cost of enforcement is not free and before a decision on what measures should be taken, a community must decide how much theft it can afford (Carter, 1974). However, an accurate analysis is not possible since the cost for loss prevention is not precisely known and the effectiveness of any control measure is uncertain (Gardiner & Lyman, 1984).

In spite of this uncertainty, it is likely that the cost of detection is greater than the cost of prevention since the development of detection measures, the cost of an investigation, the cost of disruption to the work environment,<sup>16</sup> the potential amount of money stolen, and the legal costs of recouping the remaining money (if there is any) can be substantial. The FBI reported that, in 1987, internal theft was responsible for approx. 62% of the \$861 million in losses to financial institutions in the United States. Sixty-two percent of the 10 620 cases that involved a federal crime were perpetrated by an official or employee of the institution (United States Department of Justice, 1987). Instead of exposing the company to this magnitude of risk, by curbing the opportunities to defraud and by increasing the deterrent effect that is the result of an increased level of security

---

16. Workplace efficiency can be disrupted if allegations of fraud are discussed openly. Albrecht and Williams (1990) found that employee or manager fraud results in a sequential, characteristic response pattern within a work environment: denial of the act, anger towards co-workers and investigators, attempt to bargain to return to the status quo, depression, and acceptance.

"awareness" within the organization, the potentially significant costs of future frauds can be minimized. At the same time, this principle of economic rationality would require that the cost of prevention measures will be weighed against the potential loss or the potential loss in productivity.

Based on this principle of economic rationality, one might expect internal audit departments to limit their prevention and detection measures to those acts that result in a substantial economic loss. Internal audit departments would need to weigh the costs of prevention against the estimated losses and then establish criteria for what is a tolerable level of theft. My research, however, identified a few companies that punish offenders for thefts that do not cause economic harm to the company. For example, 17% of companies would either dismiss or criminally charge an employee who copied retail software for personal use. Perhaps these auditors believe that an individual who will engage in criminal behaviour against another company is likely to commit offenses against his or her own.

#### C. The Emphasis on Situational Factors in Deterrence and Prevention Measures

Corporations address both situational factors (ie., quality of opportunity to commit fraud) and dispositional factors (ie., one's propensity for theft). For example, companies screen employees at the point of hire by using criminal and credit checks (61%) and administering "integrity

tests" (28%) (only one internal audit department conducted either of these measures). Also, most companies use other measures such as a code of conduct (94%) or educate employees about internal controls (58%). In accordance with the findings of research (Albrecht, Romney & Howe, 1984; Henry 1978; Hollinger & Clark, 1983a; Litton, 1990), the preferred preventative measures used by internal audit departments focus on changing the work environment more than changing dispositional characteristics. This is evidenced by their involvement in developing manual and computer controls.

Certain situational factors identified in the extant research are not addressed by the internal audit departments or the company. In particular, the employees' level of job satisfaction and the employees' external economic pressures were not identified as matters of concern. Although most companies did conduct a credit check at the initial point of hiring an employee (61%), there is no indication that this is an ongoing process, even though Cressey (1953), Albrecht, Howe, and Romney (1984), and the American Institute of Certified Public Accountants (1984) all found that money was a primary motivator for fraud.

#### D. The Internal Audit Departments' Use of the Work Group Environment to Deter Employee Fraud

Research indicates that the work group environment can assist in the deterrence of property and production deviance (Hollinger & Clark, 1983a). By increasing both the certainty of detection and the severity of punishment, employee fraud

can be deterred (Hollinger & Clark, 1983b). To a limited extent, internal audit departments attempt to use the work group environment to prevent employee fraud by educating employees about internal controls and the corporate fraud policy (44% of departments), by educating managers about internal controls (72%), and by publishing internally information about past cases of detected fraud (6%). Notably, the internal audit departments' invitation to managers to cooperate with them in their development of fraud control measures is not made to employees. Although my research did not attempt to assess the effectiveness of any internal auditor/manager cooperation, both Henry (1978) and Hollinger and Clark (1983a) argue that the effectiveness of unilateral initiatives by management is limited.

#### **IV. DETECTION OF EMPLOYEE FRAUD**

##### A. Corporate Responsibility for Employee-Fraud Detection

As in the case of deterring employee fraud, the responsibility for the detection of fraud is most often shared by two or three departments (78% of companies). The fact that internal audit departments undertake this responsibility indicates a move within the internal audit profession towards a greater fraud control emphasis (Juliani, Jayewardene, & Talbot, 1983). Several incentives for the internal audit department account for this involvement.

First, management has encouraged internal audit departments to take on this responsibility. The internal

audit department's audit schedule is approved by the management team. Mautz, Tiessen, and Colson found that the schedule is determined (in descending order of influence) by the corporate audit committee, the CEO, the CFO, the controller, the external auditor, and operating management. The internal audit department managers reported that their department was seldom directly involved in the schedule's development (only one percent stated they were directly involved) (1984, p. 42).

Another way that management encourages the internal audit department to undertake a responsibility for detection is through management's own failure to carry out this responsibility well. It is evident in both my and other research (American Institute of Certified Public Accountants, 1984; Gardiner & Lyman, 1984) that management reviews are a comparatively poor source of employee-fraud allegations (18.4% of respondents in my study identified the management review as a useful source).

Again, several incentives or disincentives to detect and report fraud to the internal audit department may account for management's poor reporting rates. These include the following: (a) line managers desire greater autonomy over their work environment (Gardiner & Lyman, 1984), (b) line managers are motivated by the principle of administrative and financial efficiency (Gardiner & Lyman, 1984), (c) the act in question may not be one that a manager would define as a fraud even though an internal auditor may define it as such, (d) it



is difficult to accurately distinguish between intentional and unintentional employee errors,<sup>17</sup> and (d) there is a distinct possibility that the fraud will be perceived as a reflection of managerial inabilities. The incentives to maintain workplace operations and to maintain autonomy may outweigh the incentives to detect or report fraud (Gardiner & Lyman, 1984; Kirkendall, 1990).

Managerial discretion is further facilitated by the absence of a mandatory reporting policy for line managers.<sup>18</sup> Also, line managers may believe that the internal audit department is to be distrusted (Kirkendall, 1990).<sup>19</sup> As a possible response to this perception, some internal audit departments have developed computer-assisted methods to increase their detection rates (41% of departments have set up a continuous-auditing system to detect frauds, 61% produce exception reports of transactions exceeding a specified authorization or a monetary amount).

- 
17. In their study of welfare fraud, Gardiner and Lyman (1984) found that quality control reviews by managers did little to distinguish between intentional and unintentional client errors.
  18. Thornhill (1990) advocates the establishment of a company policy that outlines the lines of responsibility for reporting employee fraud, how this information is to be transmitted to the internal audit department, and how the company will deal with personnel who either participate in or know about fraud but who do not report it.
  19. This uncooperative relationship is particularly evident between line management and the inspector general in the United States. In 1978, the U.S. Congress established the statutory offices of the inspector general in 12 U.S. government departments or agencies. These auditors were assigned the responsibility of detecting fraud and waste in government (Kirkendall, 1990, p. 4).

This self-imposed responsibility is also influenced by external forces that encourage internal audit departments to protect and to further their professional status. An internal audit department's expertise in financial and computer systems, access to senior management, and status as a business analyst gives it a strategic advantage over other departments in overseeing employee-fraud control. The consistent and predominant role of the internal audit department in all areas of employee-fraud control indicates its relative ability to effect its goals. Other internal auditors, including those associated with the CFEA, encourage internal auditors to take advantage of these professional opportunities (Townsend, 1989) by expanding the organization's control of employee conduct (Reinstein & Weirich, 1988). Finally, internal auditors are motivated to control fraud because of the possibility that they may be held civilly responsible for failing to undertake some detection measures as part of their job function (Meier & Rittenber, 1986).

My research found that not only do 89% of internal audit departments have some responsibility to detect fraud, but also that 19% of those departments are solely responsible for fraud detection. In addition, four internal audit department managers (22% of companies) see themselves as having the responsibility of overseeing employee-fraud control for the company. This level of responsibility represents a dramatic change in the internal audit department's historical role.

Although the internal audit department may receive this role formally or informally, or self-impose it, at least two disincentives may deter the other 81% of internal audit departments from taking on a similar level of responsibility. First, sole responsibility raises the expectation that the internal audit department is sufficiently competent to prevent and detect employee fraud, even in areas where the internal audit department has little control. In the case of a shareholders' lawsuit, internal auditors may find themselves liable for damages (Meier & Rittenber, 1986). Second, when one department has sole responsibility for employee-fraud control, other departments may become less involved in prevention and detection efforts. Instead of a "turf war," there is a surrender of fraud-control responsibilities. As a matter of efficiency, more employee fraud can be prevented and detected if several departments utilize their expertise.

#### B. Role of Employees In Detecting Employee Fraud

The most reliable sources of employee-fraud allegations are employee tips and tips from external sources. Employee tips are a useful source, regardless of whether a company has a policy to encourage employees to report fraud. In spite of the usefulness of employee tips, and using Hollinger and Clark's (1983a) statistics on the incidence of employee fraud as a basis for discussion, it appears that employees and external sources either are not aware of all employee fraud or are not willing to report it. Several reasons exist for

employees' failure to report employee fraud when it is detected: employees may perceive the responsibility of detection to be a managerial one; employees may disagree over what constitutes employee fraud; employees may disagree with the likely punishment; or employees may fear that future promotion is unlikely after one disrupts the work-group's solidarity by reporting a co-worker.

As companies are encouraged to utilize employees as a method of organizational control, the intrusiveness of employee reporting may be increased (Baker, Barrett, & Radde, 1976; Hollinger & Clark, 1983a; Thompson, 1986; United States General Accounting Office, 1986). Already, some companies and internal audit departments attempt to use more intrusive measures to detect employee fraud. In my research, four of 16 companies (25%) require employees to report employee fraud. Four of 16 internal audit departments (25%) are increasing the level of supervision by teaching managers how to detect employee fraud.

Hollinger and Clark (1983a) argue that the unilaterally enacted policies and procedures by management are "ineffectual in constraining employee deviance unless they are also simultaneously reflected in the informal normative consensus of the work force" (p. 126). Furthermore, Henry (1978) argues that an employee-fraud-control policy should be shaped by the workplace community. The absence of employee involvement in the definition, deterrence, and sanctioning of employee fraud

in my research evidences a unilateral undertaking by management.

C. The Effectiveness of Internal Audit Departments' Detection Measures

Research has found that three percent of employees engage in fraud (Hollinger and Clark, 1983a); that fraud exists in all companies, although at varying levels (Hollinger and Clark, 1983a); and that the internal audit seldom detects fraud (12% of cases) (American Institute of Certified Public Accountants, 1984). If these findings can be extrapolated to the Canadian insurance industry, it appears that the internal audit department's measures are ineffective tools to uncover employee fraud. This inefficiency is not due to the internal auditors' hesitation to punish employee fraud, since most internal auditors in my research recommend a punishment of dismissal or criminal charge for most cases of property theft (including embezzlement).

The inefficient detection measures are the result of other factors. Within the broader policy decisions about fraud detection made at the senior management level, the more specific decisions on "how to detect" are made by technical experts, in this case the internal audit department (Gardiner & Lyman, 1984). It appears that internal audit departments choose to make their fraud detection efforts a peripheral focus of the regular audit. Only 27% of departments undertake a fraud audit separate from the regular audit. Most companies will identify some exceptional transactions to be analyzed as

part of the regular audit. The regular internal audit was listed by 67% of respondents as a primary way to detect fraud. However, other research indicates that the internal audit department is actually responsible for identifying only a minor number of cases (12% of cases) (American Institute of Certified Public Accountants, 1984).

By attempting to identify fraud during the course of the regular audit, the auditor faces important time constraints. During an audit, the internal auditor's first priority is to identify errors within the sample that is tested. Once an error has been identified, little time is left to determine the intentions behind the act.<sup>20</sup> In the case of management fraud, the auditing process may take even longer (Baker, Barrett, & Radde, 1976; Edlund, 1979) with every expansion of the investigation increasing its cost (Thornhill, 1990, pp. 30-31). Hence, internal auditors must be able to detect and investigate fraud expeditiously. Since organizations do not deem the detection of fraud as a major goal (Baker & Westin, 1987), it can be expected that internal audit departments are evaluated on their performance on compliance audits rather than on their performance on fraud audits.

In addition to time constraints, the detection of fraud is very difficult. First, internal auditors are expected to

---

20. Hylas and Ashton studied in detail 281 "errors" identified in 152 independent audits conducted by a single firm (any frauds would be part of fraudulent financial reporting). In their analysis, they concluded that 10 of the 281 errors (3.6%) were in fact intentional (Hylas & Ashton, 1982, p. 760).

respect the fact that a certain level of trust is necessary within complex work organizations. The basic concept behind auditing is that the auditee be given the benefit of the doubt (Thornhill, 1990, p. 30). This then forces auditors to be sufficiently competent to second-guess the decisions made by those who have an intimate knowledge of company policies (Gardiner & Lyman, 1984). Employees are hired to make specific decisions while using sometimes ambiguous policies. A system of internal control that results in complete confidence in the accuracy of all information and in the conduct of all employees and management would significantly impair the quality of the organization's service to the client.

Second, internal auditors are not specifically trained to detect fraud (Baker, Barrett, & Radde, 1976; Bologna, 1984; Goldstein, 1989). Professional accounting and auditing courses focus on the identification of errors and the development of workplace controls. In this research, it was found that internal auditors received only a moderate level of education specifically related to employee-fraud control (65% through IIA or CFEA conferences, 59% through personal readings).

A third reason for the departments' ineffectiveness centers on the elusiveness of a sampling method to accurately identify fraud. Unlike a case of murder, there may be no "dead body" or eyewitness testimony with which one can begin the investigation. To draw out a manageable number of cases

and thereby increase an auditor's chances of successfully identifying fraud, a sampling method must be used.<sup>21</sup> One way this can be accomplished is by developing a profile of the average behaviour and then focusing on persons whose patterns of behaviour deviate from this norm (Gardiner & Lyman, 1984). This is often accomplished successfully using a computer-assisted matching program (Greenberg, Wolf & Pfeister, 1986). This method would be effective for the many reported cases of EDP-related fraud that characteristically involve only minor forms of concealment such as file maintenance (American Institute of Certified Public Accountants, 1984, p. 16). Perpetrators in this AICPA study appeared to believe that their fraud would be overlooked in the large volume of transactions or be "written off as unreconciled items" (1984, p. 16).

In my research, 41% of departments have set up a continuous-auditing system to detect frauds, and 61% produce exception reports of unauthorized access into a computer file or of transactions exceeding a specified monetary amount. However, even these methods do not appear to detect all employee fraud (cf. Hollinger and Clark's (1983a) finding that three percent of employees commit fraud).

---

21. An Inspector General study estimated that "the complete verification of every aspect of a food stamp application would take 12 hours and would cost eight times as much in additional salaries as it would save in reductions in fraud and error (Stover, 1981 in Gardiner & Lyman, 1984, p. 57).



Anderson and Young (1988) recommend that internal auditors would make the best use of their time and resources by taking a strategic approach to fraud detection. Auditors presently use a technique of risk analysis that results in giving identical attention to each auditable unit within a given risk class (Anderson & Young, 1988, p. 23). Instead, auditors should incorporate the auditee's anticipation of the effectiveness of the audit work into their audit plan, in a way similar to guessing the move of an opponent in a game (1988, p. 24). The internal audit department is then able to influence the behaviour of the auditee and thus the effectiveness of the audit plan by controlling the allocation of audit resources among auditable units (eg., one method would be to conduct surprise audits) (Anderson & Young, 1988, p. 23). To be successful, this manner of auditing would require that the auditor have extensive knowledge in fraud control. This is a fact not evident in my study or other studies. However, 39% of internal audit departments in my study do undertake surprise audits.

In my study, only one audit department mentioned that their fraud audit incorporates employees' background. To further increase the effectiveness of the internal audit departments' detection measures, auditors should take into consideration employees' external financial pressures (Cressey, 1953), level of job satisfaction (Hollinger & Clark, 1983a), and situational influences (Albrecht, Howe & Romney, 1984). The impracticality of creating such a sample would be

a disincentive. More importantly, the intrusiveness of such a sampling method would certainly give rise to considerable legal and ethical debate.

Another reason for the ineffectiveness of the internal audit departments' measures is their near exclusive focus on employee fraud. Since senior management controls the scope of the audit schedule and since it is unlikely that senior management openly welcomes scrutiny by those they manage, this control discourages the internal audit department from searching for fraud amongst the activities of senior management. Indeed, my data indicate that only 17% reported using any measures specifically for this purpose. This is consistent with the findings of Mautz, Tiessen, and Colson where, in some companies, "the scope of internal audit did not extend to the examination of senior management activities" (1989, p. 43). This was particularly true for activities conducted solely by senior management (1989, p. 44). The rationality of this emphasis is questionable in light of research that suggests that, although more clerks than managers steal money, the average take of manager fraud is higher than the average employee fraud and that a single manager fraud may exceed the value of many employee frauds (Guercio, Rice & Sherman, 1988).

A final reason behind the ineffectiveness in detecting fraud is the internal audit departments' failure to audit certain company operations, such as background investigations. Although one study found that 30% of individuals

misrepresented themselves on job applications (McKee & Bayes, 1987), internal audit departments either did not audit this activity or, if they did, only conducted a cursory evaluation. The same appears to be true of the internal audit departments in my research with only 6% conducting a credit or criminal check.

#### **V. THE NATURE OF THE EMPLOYEE-FRAUD INVESTIGATION AND ITS ADJUDICATION**

The internal audit department plays a predominate, although shared, role in the investigation of civil cases (72% of companies) and criminal cases (67% of companies). In this case, the internal audit department appears to conduct a preliminary analysis of the error or suspicious transaction, but will, at some point in the investigation, pass the responsibility for the investigation over to another department. Significantly, there are internal audit departments that claim to have sole responsibility for investigating civil cases (11% of companies) and criminal cases (33% of companies). However, the nature of their responsibilities cannot be determined from this study.

There is a moderate level of inconsistency among internal audit departments when it comes to what sources are used in an investigation. Although internal auditors consistently use information from a perpetrator's manager and performance records (89% / 83% of companies), there is much less uniformity in the use of pre-employment records and credit reports (50% / 56% of companies). This would confirm Henry's

(1978) conclusion that there is a considerable exercise of discretion in internal investigations. It is possible that this discretion also exists within departments since only 17% of internal audit departments assess the uniformity among audit staff in their ability to investigate fraud.

Also, it also appears to be the case that internal audit departments may be exposing their company to future civil harm. The data across companies indicate that the legal department is not consistently consulted and that legal counsel is not sought before preparing reports for senior management during and after an investigation. Again, this may be due to the internal auditors' failure to appreciate the many precautions that should be undertaken in the course of employee-fraud control.

The private security industry only has a secondary responsibility in employee-fraud investigations. Police are occasionally used to complete an internal investigation (33% of companies), and forensic accountants are infrequently used at any stage (17%). With only one of 157 auditors holding a CFE title, the Certified Fraud Examiners Association is influential only in terms of educating internal auditors about employee-fraud issues.

The final stage of the investigatory process, the decision of how a case will be adjudicated, rests with another level of management. In this way, employee fraud is a form of social control by management (Tucker, 1989). The more frequent sanction is that of dismissal (Henry, 1978; Hollinger

& Clark, 1983a). With most cases of employee fraud resolved in a civil proceeding (Henry, 1978; Hollinger & Clark, 1983a), employee fraud is tried within the company and out of public view. In my research, management alone administers sanctions, without the assistance of elected employees or managers. To some extent, the formalized industrial regulations that govern Canadian labour relations affords employees a certain level of procedural protection. The dismissed person may also seek redress in a civil court.

In spite of these protections in civil and criminal court, some forms of injustice may not be illegal. There may be little to protect an employee from dismissal or a criminal charge even though a co-worker may engage in a similar act and not receive either sanction.

## **VI. CONCLUSION**

### **A. Perceptions of Internal Audit Departments' Employee-Fraud-Control Policy: A Review of Findings**

#### **1. Reporting Hierarchy for the Internal Audit Department**

The internal audit manager has regular access to a Vice-President to discuss administrative issues and has direct access to the President, Chief Executive Officer (CEO), or Chief Financial Officer (CFO) to discuss employee fraud.

#### **2. Internal Auditors' Knowledge of Employee Fraud**

Approximately 65% of internal auditors have a professional designation granted by an accounting or auditing

association. Most of an auditor's education about employee fraud comes from attending professional conferences and reading professional literature. The CFEA plays an influential role in the education of internal auditors through conferences and professional literature.

### **3. Organizational Responsibilities for Employee-Fraud Control**

Corporate responsibility for the deterrence, prevention, detection, and investigation of employee fraud is widely dispersed throughout the corporation, but the internal audit department is the dominant player. This relative dominance may be related to the absence of an investigation unit and a data security department in several companies. In a few companies, a single person oversees employee-fraud control, usually an internal audit department manager. The only control employees have over the control of employee fraud is in their decision whether or not to report a case of fraud.

The internal audit departments' role in the detection of employee fraud may be due to management's expectation that the internal audit profession has the expertise to detect fraud. Also, this role may be a result of the line managers' inability or reluctance to perform this function. It was found that most audit managers perceive their department as having at least a secondary role in the deterrence of fraud, contrary to the guidelines of the IIA. Also, some internal audit departments hold the primary responsibility for employee-fraud detection. To a lesser extent, internal audit

departments undertake responsibility for the investigation of fraud, usually conducting only the preliminary investigation. When reporting allegations of fraud to senior management, internal audit departments may be unnecessarily exposing their company to future financial harm by not consulting the appropriate legal counsel on the contents of memos and reports.

#### **4. Internal Audit Managers' Definition of Employee Fraud**

When evaluating the seriousness of employee theft and fraud, audit managers consider the following factors as relevant: (a) the intention of the offender, (b) the person or organization directly victimized by the theft or fraud (ie., in descending order of seriousness, frauds and thefts against the company, against co-workers, against clients, and against other companies), and (c) the type of theft or fraud. The data indicate that property deviance is perceived to be more serious than production deviance, and that cash theft is perceived to be more serious than property damage.

#### **5. Deterring and Preventing Employee Fraud**

In the attempt to predict future fraudulent behaviour, companies focus on dispositional factors, whereas their internal audit departments focus more on situational factors. Companies attempt to deter employee fraud by conducting background checks and by administering integrity tests to prospective employees. Internal audit departments attempt to

eliminate fraud by developing secure computer environments and by educating management and employees about internal controls.

Although internal auditors recognize the importance of situational variables, they focus primarily on only one type of situational variable -- the opportunity to commit fraud. The emphasis on opportunities has meant that internal auditors and their companies fail to appreciate the relevance of job dissatisfaction, work-group norms, and external economic factors in the process of predicting fraud. Extant research suggests that internal audit measures will be ineffective until these factors are taken into account.

#### **6. Detecting Employee Fraud**

In detecting employee fraud, internal audit departments use a series of computer-assisted measures. Internal auditors focus primarily on employees who use computer systems to disburse funds. In the case of the sample companies, less than one percent of employees was investigated for fraud in the preceding 12 month period. Most frauds were perpetrated in the operations of disbursements and policy sales. A complete record of allegations is seldom kept.

The majority of employee-fraud allegations arise from employee tips, external sources, and internal audits, with internal auditors claiming that employee tips are the most useful source of allegations. Employee tips are a useful source regardless of a company's reporting policy. Notably few allegations result from management reviews (a fact that



may be related to the absence of mandatory reporting policies for managers). Ironically, the group that makes the most fraud allegations (ie., employees) is the same one that is perceived to be the most threatening to the financial well-being of the company and that is subjected to the greatest levels of surveillance within the company.

To a much lesser extent, internal auditors audit senior management for fraud. The responsibility of evaluating management decisions appears to be left up to the management team itself or the external auditor. For those few internal audit departments that do supervise management decisions, special tests are created.

#### **7. Internal Audit Departments' Investigation and Follow-up Procedures**

Internal audit departments maintain a high level of involvement in both civil and criminal investigations, particularly in companies without a separate investigation unit. The investigatory responsibility for employee fraud is shared among various departments. Police seldom conduct the initial criminal investigation; their services are more frequently used later in an investigation. Forensic accountants are seldom used by companies.

Internal audit staff regularly conduct a preliminary investigation into suspicious transactions using a variety of company records and interviews. The final decision to prosecute or dismiss a case, however, rests with another level

of management. The internal audit department usually prepares a written report for the President or CFO.

#### **8. Role of Private Security Industry in the Control of Employee Fraud**

The private security industry is growing rapidly, but this growth has not dramatically affected the structure of most internal audit departments in the insurance industry. For example, there was only one internal auditor with a CFE designation, and only a few internal audit departments have a separate investigation unit within the department. Perks, such as "time theft," have not yet been defined as behaviour deserving of dismissal or of a criminal charge. Detection measures are only moderately intrusive, and employee-fraud investigations are conducted by internal auditors who probably have limited investigative training or experience. However, these findings should not be interpreted as meaning that the influence of the private security industry has been minimal or is not increasing. At this point, however, internal audit departments seem most influenced by the private security industry through its contribution to the professional literature and internal audit conferences.

#### **9. Distribution of Sanctions Across Companies**

There is evidence that some employee-fraud perpetrators in the Canadian insurance industry are more likely than others to be dismissed or to come to the attention of the criminal justice system. Dissimilar sanctions for similar acts across

companies may result from differences in the definitions about what acts should be sanctioned, in the detection measures used, in the relative competence of an auditor to detect and investigate a case of fraud, and in the criteria used by management to decide whether a case should proceed as a civil or criminal matter.

#### B. Implications of the Research

My research raises at least three issues about the control of employee fraud in general. These issues could serve as a basis for future research on the control of employee fraud.

First, explanations of the cause of theft focus more on the role of situational factors because of their strong influence on theft (Litton, 1990). My research indicates that internal auditors focus on situational factors when trying to control employee fraud. More specifically, they focus on only one type of situational factor: the opportunity to commit fraud. Three reasons may account for why other situational factors are largely ignored: (a) they are better addressed by another department in the organization; (b) they are too expensive to deal with; or (c) they are perceived, albeit incorrectly, to be of little importance or as not having much effect.

Second, in general, police and other control agencies focus their attention on the activities of marginalized or relatively less powerful groups (Williams & MacShane, 1988).

My research suggests the same. The inconsistency in the controllers' scrutiny of managers and employees appears to be best explained by the controllers' relationship to the management team, a relatively more powerful group. This differential treatment exists even though extant research suggests that managers steal more money than employees.

Third, the growth of the private security industry in Canada, as discussed by Sewell (1985), has at least two parallels in the Canadian insurance industry. First, the purview of policing is expanding. However, this takes on an interesting pattern. Instead of devoting resources to the training and education of specialized fraud investigators, insurance companies attempt to utilize the services of "part-time police." Internal auditors and employees are recruited to facilitate social control over other company employees. Consequently, the amount of surveillance during the course of business increases dramatically, along with the number of social control agents.

A second similarity found between the private security industry and the insurance industry is the increased use of sophisticated detection and investigation techniques. Technological innovations, such as security software programs, are making detection methods more effective. By using computers, internal audit departments can analyze thousands of transactions in a short period of time, all without the subjects' knowledge. Again, this results in more effective, covert surveillance.

In sum, the purpose of my research has been to provide a comprehensive review of the internal audit departments' role in the definition, deterrence, prevention, detection, and investigation of employee fraud in the Canadian insurance industry. Hopefully, this exploratory research will be supplemented with more detailed analyses of the policies and procedures used to control employee fraud and the intra- and inter-organizational influences that shape them. Also, a self-report study or participant-observation research could be used to determine the rate of employee fraud that exists within the insurance industry.

## LIST OF REFERENCES

- Albrecht, W. S., Howe, K. R., & Romney, M. B. (1984). *Deterring fraud: The internal auditor's perspective*. Altamonte Springs, FL: Institute of Internal Auditors.
- Albrecht, W. S., & Williams, T. L. (1990, August). Understanding reactions to fraud. *Internal Auditor*, 47(4), 45-51.
- Allen, B. (1981). Threat teams: A technique for the detection and prevention of fraud in automated and manual systems. *Computer Security Journal*, 1(1), 1-13.
- American Institute of Certified Public Accountants. (1984). *Report on the study of edp-related fraud in the banking and insurance industries*. New York, NY: Author.
- Anderson, U., & Young, R. A. (1988, Fall). Strategic auditing: A different game. *Internal Auditing*, 4(2), 14-24.
- Baker, D. W., Barrett, M. J., & Radde, L. R. (1976, October). Top-management fraud: Something can be done now! *Internal Auditor*, 33(5), 25-33.
- Baker, M. A., & Westin, A. F. (1987). *Employer perceptions of workplace crime*. Washington, DC: U.S. Bureau of Justice Statistics.
- Becker, R. W. & Costello, T. P. (1991). The reporting and collection of management and employee fraud data: Current practices and developing trends in American business. *Security Journal*, 2(3), 152-171.
- Berghuis, A. C., Paulides, G. (1985). *Abuse of Dutch private companies (BV's): An empirical study*. The Hague, NETH: Research and Documentation Centre, Ministry of Justice.
- Bigus, O. E. (1972). The milkman and his customer. *Urban Life and Culture*, 1, 131-165.
- Bologna, J. (1984). *Corporate fraud: The basics of prevention and detection*. Stoneham, MA: Butterworths.
- Cameron, M. O. (1964). *The booster and the snitch*. London, UK: Collier-Macmillan.
- Carter, R. L. (1974). *Theft in the market*. London, UK: The Institute of Economic Affairs.
- Certified Fraud Examiners Association. (1993). *The Certified Fraud Examiner Program (Promotional packet)*. Austin, TX: Author.

- Chamber of Commerce of the United States. (1974). *A handbook of white collar crime*. Washington, DC: Author.
- Cooper, H. (1989). *Integrative research*. Newbury Park, CA: Sage.
- Cressey, D. R. (1953). *Other people's money: A study of the social psychology of embezzlement*. Glencoe, IL: The Free Press.
- Crocker, O. L., Kukeil, E. A. (1953). Accountants respond to professional misconduct. *Canadian Journal of Criminology*, 25(2), 159-172.
- Collier, P. A., Dixon, R., & Marston, C. L. (1991, August). Computer fraud: Research findings from the UK. *Internal Auditor*, 48(4), 49-52.
- Ditton, J. (1977a). *Computer fraud* (mimeo). London, UK: The Outer Circle Policy Unit.
- Ditton, J. (1977b). Perks, pilferage and the fiddle: The historical structure of invisible wages. *Theory and Society*, 4, 39-71.
- Ditton, J. (1977c). *Part-time crime: An ethnography of fiddling and pilferage*. London, UK: Macmillan Press.
- Ditton, J. (1979). *Contrology: Beyond the new criminology*. London, UK: MacMillan.
- Edlund, B. (1979). Qualified accountants' role concerning economic crime. *Ekonomisk Brottslighet*, 187-203.
- England, K. A. D. (1976). Fiddles in the distributive trades (mimeo). In *Evening Standard* (1976, September 16). Surgical swindles. p. 12.
- Ernst & Young. (1989). *White collar crime: Loss prevention through internal control*. Warren, NJ: Chubb Group of Insurance Companies.
- Franklin, A. P. (1975). *Internal theft in a retail organization: A case study*. Unpublished doctoral dissertation, Ohio State University, Ann Arbor, MI.
- Gardiner, J. A., & Lyman, T. R. (1984). *The fraud control game: State responses to fraud and abuse in AFDC and Medicaid programs*. Bloomington, IN: Indiana University.
- Gill, P. R. (1986, April). Avoiding corporate self-incrimination. *Internal Auditor*, 43(2), 15-18.

- Goldstein, L. M. (1989, June). The auditor as private eye: Using public records as tools for investigating fraud. *Internal Auditor*, 46(3), 18-28.
- Graham, C., & Freely, M. (1990, December 1). Keep your data secure. *Datamation*, 97-100.
- Greenberg, D., Wolf, D., & Pfeister, J. (1986). *Using computers to combat welfare fraud: The operation and effectiveness of wage matching*. New York, NY: Greenwood.
- Grove, H., Lee, P., & Hanbery, G. (1988, Summer). The internal auditor: Key agent for reduction of fraudulent financial reporting. *Internal Auditing*, 12-22.
- Guercio, J. P., Rice, E. B., & Sherman, M. F. (1988, September). Old fashioned fraud by employees is alive and well: Results of a survey of practicing CPAs. *The CPA Journal*, 74-77.
- Gurvich, P. B. (1991). *The blue book of Canadian business Financial Post top 500 Canadian businesses directory*. Toronto, ON: Financial Post.
- Henry, S. (1976). *Stolen goods: The amateur trade*. Unpublished doctoral dissertation, University of Kent, UK.
- Henry, S. (1978). *The hidden economy: The context and control of borderline crime*. London, UK: Martin Robertson.
- Hollinger, R. C. (1991). Neutralizing in the workplace: An empirical analysis of property theft and production deviance. *Deviant Behavior*, 12(2), 169-202.
- Hollinger, R. D., & Clark, J. P. (1983a). *Theft by employees*. Toronto, ON: Lexington Books.
- Hollinger, R. C., & Clark, J. P. (1983b). Deterrence in the workplace: Perceived certainty, perceived severity, and employee theft. *Social Forces*, 62, 398-418.
- Horning, D. (1970). Blue collar theft: Conceptions of property, attitudes toward pilfering, and work group norms in a modern industrial plant. In E. O. Smigel & H. L. Ross (Eds.). *Crimes against bureaucracy* (pp. 46-64). New York, NY: Van Nostrand Reinhold.
- Hylas, R. E., & Ashton, R. H. (1982). Audit detection of financial statement fraud. *The Accounting Review*, 57, 751-765.
- Institute of Internal Auditors. (1968). *Certified Internal Auditor code of ethics*. Altamonte Springs, FL: Author.



- Institute of Internal Auditors. (1981). *Statement of responsibilities of internal audit*. Altamonte Springs, FL: Author.
- Institute of Internal Auditors. (1985). *Standards for the professional practice of internal auditing: Deterrence, Detection, Investigation, and Reporting of Fraud*. Altamonte Springs, FL: Author.
- Juliani, T. J., Jayewardene, C. H. S., & Talbot, C. K. (1983). Preventing moral men from making immoral decisions. In C. K. Talbot, T. J. Juliani, & C. H. S. Jayewardene (Eds.). *Fraud: Detection and preventive strategies* (pp 1 - 12). Ottawa, ON: Crimcare.
- Kirkendall, D. (1990, Summer). Can auditors polish their sometimes tarnished image? *Government Accountants Journal*, 39(2), 3-8.
- Kramer, W. M. (1989). Internal fraud: Detection, investigation, prosecution and prevention. Part two: Investigation. *The White Paper*, 3(3), 8-10.
- Leech, T. (1990, April). Investigating conflicts of interest. *Internal Auditing Letter*, 3-4.
- Leinicke, L. M., Rexroad, W. M., & Ward, J. D. (1990, August). Computer fraud auditing: It works. *Internal Auditor*, 26-33.
- Litton, R. A. (1990). *Crime and crime prevention for insurance practice*. Aldershot, UK: Avebury.
- Mars, G. (1973). Hotel pilferage: A case study on occupational theft. In M. Warner (Ed.), *The sociology of the workplace* (pp. 200-210). New York, NY: Halsted Press.
- Mars, G., & Mitchell P. (1977). *Room for reform: A case study on industrial relations in the hotel industry*. Bletchley, UK: Open University Press.
- Mautz, R. K., Tiessen, P., & Colson, R. H. (1984). *Internal auditing: Directions and opportunities*. Altamonte Springs, FL: Institute of Internal Auditors.
- McKee, T. E., & Bayes, P. E. (1987, October). Why audit background investigations. *Internal Auditor*, 44(5), 53-56.
- McKenzie, G. (1989, October). The first NRMA/Ernst & Young survey of retail internal audit. *Retail Control*, 57(8), 10-12.

- Meier, M. E., & Rittenber, L. E. (1986, April). Dealing with known corporate wrongdoing. *Internal Auditor*, 43(2), 37-42.
- Murusalu, V. (1991, September 1). Error, fraud and good faith. *CA Magazine*, 58-60.
- Quinney, E. R. (1963). Occupational structure and criminal behaviour: Prescription violators by retail pharmacists. *Social Problems*, 11, 179-185.
- Raab, M. S. (1987). Detecting and preventing financial statement fraud: The roles of the reporting company and the independent auditor. *Yale Law & Policy Review*, 5, 514-535.
- Reinstein, A., & Weirich, T. R. (1988, October). Ethics and fraud: Opening doors for internal auditing. *Internal Auditor*, 45(5), 43-47.
- Richstein, K. J. (1965). Ambulance chasing: A case study of deviation and control within the legal profession. *Social Problems*, 13, 3-17.
- Robin, G. D. (1965). *Employees as offenders: A sociological analysis of occupational crime*. Unpublished doctoral dissertation, University of Pennsylvania, PE.
- Sewell, J. (1985). *Police: Urban policing in Canada*. Toronto, ON: Lorimer.
- Shepard, I. M., & Dustin, R. (1988). *Thieves at work: An employer's guide to combating workplace dishonesty*. Washington, DC: Bureau of National Affairs.
- Sieh, E. W. (1987). Garment workers: Perceptions of inequity and employee theft. *British Journal of Criminology*, 27, 179-190.
- Stover, C. (1981). *Finding and forestalling food stamp fraud: A study of the food stamp enforcement activities of the Office of Inspector General-Investigations*. Washington, DC: United States Department of Agriculture Office of Inspector General.
- Sweeney, L. E. (1976, August). Are internal auditors responsible for fraud detection? *Internal Auditor*, 10-16.
- The internal auditor and fraud. (1990, March). *Internal Auditing Alert*, 10(1), 1-8.
- The National Commission on Fraudulent Financial Reporting. (1987). *Report of the National Commission on Fraudulent Financial Reporting*. New York, NY: Author.

- Thio, A. (1988). *Deviant behavior*. New York, NY: Harper and Row.
- Tiessen, P., & Barrett, M. J. (1989, Fall). Organizational support for internal audit. *Internal Auditing*, 39-53.
- Tittle, C. R. (1980). *Sanctions and social deviance: The question of deterrence*. New York, NY: Praeger.
- Thompson, M. (1986). Plans for prevention: Winning strategies. *Security World*, 23(3), 48-54.
- Thornhill, W. T. (1990, Summer). When to implement a specialized fraud audit program. *Internal Auditing*, 6(1), 29-35.
- Townsend, D. A. (1989, June). Caveat auditor. *Internal Auditor*, 46(3), 40-41.
- Tucker, J. (1989). Employee theft as social control. *Deviant Behavior*, 10, 319-334.
- United States Department of Justice, Federal Bureau of Investigation. (1987). *Bank crime statistics: Federally insured financial institutions, January 1, 1987 - December 31, 1987*. Washington, DC: Author.
- United States General Accounting Office. (1986). *Fraud hotline: 7 year GAO fraud hotline summary*. Washington, DC: Author.
- Wagner, C. R. (1979). *The CPA and computer fraud*. Lexington, MA: Lexington Press.
- Williams, F. P., & MacShane M. D. (1988). *Criminological theory*. Englewood Cliffs, NJ: Prentice Hall.
- Wilson, P. R., et al. (1985). Medical fraud and abuse: Australia, Canada and the United States. *International Journal of Comparative and Applied Criminal Justice*, 9(2), 25-34.
- Zeitlin, C., & Nelson, D. (1986, December). The use of external reviews. *Internal Auditor*, 27-29.

Cases cited:

- R. v. Olan, Hudson and Hartnett, (1978), 86 D.L.R. (3d) 212.

## APPENDIX 1

## Searches of Printed Abstracts and Indexes

Manual Searches

1. **Criminal Justice Abstracts** 1977-1993. Key words included "Employee Theft," "Embezzlement," "Criminology," "Fraud," "Workplace Crime."
2. **Index to Canadian Legal Periodical Literature** 1961-1993. Key words used "Master and Servant."
3. **Criminal Justice Periodical Index** 1972 - 1993. Key words include "Embezzlement," "Employee Dishonesty," "Employee Fraud," and "Employee Theft."
4. **Dissertations Abstracts** 1861-1993. Key words include "Employee ...", "Fraud," "White Collar Crime," "Workplace Crime." Looked under divisions of "Law and Political Science," and "Sociology."
5. **Personnel Management Abstracts** 1986 - 1992. Key words "Ethics."
6. **Human Resources Abstract** 1981 - 1993. Key word "Embezzlement."
7. **Socialist Review** 1986 - 1988. Key word "Employee Theft."
8. **Internal Auditor Magazine** - 1984 - 1991 Key word "Employee Fraud."

Computer-assisted and On-line Searches

9. **Social Sciences Index** 1989 - 1993. Key words include "Employee Theft," "Industrial Relations," "Supervision of Employees," "Employee Rating," "Employee Behavior," and "Fraud."
10. **Infotrac** 1980 - 1992 (August). Subjects searched include "Employee Theft" and subdivisions of "Research," "Statistics," and "Surveys."
11. **NCJRS** 1972 - 1991. Conducted July 11, 1991. Key words include "Insurance Fraud" and "Embezzlement."
12. **NCJRS** 1972 - 1991. Conducted August 23, 1991. Key words include "Fraud," "Crime," "Embezzlement," "Professional Misconduct," and "Audit."
13. **NCJRS** 1983 - 1993. Conducted August 28, 1993. Key words include "Auditors" and "Fraud."

14. **Simon Fraser University Library** 1992. Subjects searched include "Computer Crime," "Employee Theft," "Employee Fraud," "Internal Audit," and "Fraud."
15. **University of Alberta Library** 1993. Subject searched include "Computer Crime," "Employee Theft," "Employee Fraud," "Internal Audit," and "Fraud."
16. **Canadian Business and Current Affairs** 1985 - 1993. Key words searched include "Employee," "Fraud," and "Audit."
17. **American Business Index** 1985 - 1993. Key words searched include "Fraud," "Employee," "Embezzlement," and "Audit."

## APPENDIX 2

## Questionnaire

**Purpose**

The purpose of this questionnaire is to determine the role of internal audit departments in the deterrence, detection, investigation, and reporting of employee fraud.

**Definition**

For the purpose of this study, "fraud" is defined as those allegations and actual cases where there has been an attempt to use deception to obtain a tangible or non-tangible reward.

**STRUCTURE AND STAFFING**

1. To whom does the internal audit department report to on regular administrative matters?

\_\_\_\_\_ VP Finance  
 \_\_\_\_\_ President  
 \_\_\_\_\_ Board of Directors  
 \_\_\_\_\_ Other \_\_\_\_\_

2. Do you have direct access to the President to discuss cases of employee fraud?

Yes / No

3. What is the total number of professional staff members in your internal audit department?

\_\_\_\_\_ Managers  
 \_\_\_\_\_ Auditing staff  
 \_\_\_\_\_ Support staff  
 \_\_\_\_\_ Secretarial staff

4. Are your auditors part of a union?

Yes / No

- \* If "Yes," has this presented any problems in relation to your fraud control?

Yes / No

5. How many of your internal audit staff have one or more of the following designations?

Accounting

\_\_\_\_\_ CPA  
 \_\_\_\_\_ CA  
 \_\_\_\_\_ CMA

\_\_\_\_\_ CGA  
 Auditing \_\_\_\_\_ CIA  
 \_\_\_\_\_ CISA  
 Other \_\_\_\_\_

6. How many of your auditors who engage in EDP auditing have:

\_\_\_\_\_ An accounting designation  
 \_\_\_\_\_ A business degree  
 \_\_\_\_\_ A computer science degree  
 \_\_\_\_\_ A computer science certificate  
 \_\_\_\_\_ Other

**RESPONSIBILITIES RE: EMPLOYEE FRAUD ALLEGATIONS**

7. Does your organization have a committee established to deal with allegations of employee fraud?

Yes / No

\* If "Yes", who is represented on this committee?

\_\_\_\_\_ Internal Audit  
 \_\_\_\_\_ Investigation Unit  
 \_\_\_\_\_ Corporate Law  
 \_\_\_\_\_ Labour Relations  
 \_\_\_\_\_ Human Relations  
 \_\_\_\_\_ Other \_\_\_\_\_

\* If "Yes", what is its mandate?

\_\_\_\_\_

\_\_\_\_\_

8. If there is no such committee, to whom are allegations of employee fraud most often reported?

\_\_\_\_\_ Line Management  
 \_\_\_\_\_ Investigation Unit  
 \_\_\_\_\_ Internal Audit  
 \_\_\_\_\_ Human Resources  
 \_\_\_\_\_ Other \_\_\_\_\_

9. Within your organization, is there an individual whose primary responsibility is in relation to employee fraud and theft? If "yes," who is this person?

Yes / No \_\_\_\_\_

10. Does the corporation have an employee fraud "log book" (ie., a centralized record of all investigations presently undertaken against an employee)?

Yes / No

11. Do you have anyone within your Investigation Unit/Corporate Security department who conducts "fraud audits" (ie., use financial records for the purpose of detecting fraud)?

Yes / No

12. Do you have anyone within your Investigation Unit/Corporate Security department who conducts "EDP audits" (ie., do they assist in identifying areas where audit trails should be created)?

Yes / No

13. Which of the following departments are involved in ensuring that there are adequate controls to deter employee fraud?

Line Management  
 Internal Audit  
 Corporate Security/Investigation Unit  
 Human Resources  
 Data Security  
 Corporate Control/Controller  
 Other \_\_\_\_\_

14. Which of the following departments are involved with the detection of employee fraud?

Line Management  
 Internal Audit  
 Corporate Security/Investigation Unit  
 Human Resources  
 Data Security  
 Corporate Control/Controller  
 Other \_\_\_\_\_

15. If the act is deemed to be a civil or employee performance matter, who has the responsibility for investigating an allegation of employee misconduct?

Manager within the Department  
 Internal Audit  
 Corporate Security/Investigation Unit  
 Human Resources  
 Other \_\_\_\_\_

16. If the act is deemed to be a criminal matter, who has the responsibility of investigating an allegation of employee fraud?

Manager within the Department  
 Internal Audit  
 Corporate Security/Investigation Unit  
 Human Resources



Other \_\_\_\_\_

**PRIORITIES AND METHODS OF INTERNAL AUDIT**

17. For which of the following **UNAUTHORIZED** acts would an employee be fired or criminally charged by your corporation? If there is no corporate policy, please answer on the basis of what you would recommend.

Assume that the person in question has no prior history of illegal activity and that it is believed that the activity occurred only once.

If the action taken is dependant upon the monetary value, please indicate the approximate level at which firing or criminal charges would be recommended.

- \_\_\_\_\_ Failure to report a theft of employer's property
- \_\_\_\_\_ To the benefit of the corporation, alter corporate records for purpose of tax evasion
- \_\_\_\_\_ Shortchange or overcharge customers
- \_\_\_\_\_ Corporate "perks" designated only for employee use were used for relatives or friends
- \_\_\_\_\_ Take money or gifts from business clients
- \_\_\_\_\_ Reading restricted data sources for interest
- \_\_\_\_\_ Use of corporate information for personal business
- \_\_\_\_\_ Making a copy of organization's retail software program for personal use
- \_\_\_\_\_ Theft of company time
- \_\_\_\_\_ Working while under influence of alcohol or drugs for one day
- \_\_\_\_\_ Unauthorized use of office equipment
- \_\_\_\_\_ Unauthorized use of company vehicles
- \_\_\_\_\_ Travel expenses exaggerated
- \_\_\_\_\_ Not reporting travel bonus points
- \_\_\_\_\_ Intentional damage of company equipment
- \_\_\_\_\_ Removal of office supplies
- \_\_\_\_\_ Take property of co-workers
- \_\_\_\_\_ Borrow money from corporation without approval
- \_\_\_\_\_ Put in a fraudulent claim or loan
- \_\_\_\_\_ Theft of corporate cash

18. In the last 12 months, how many internal investigations have there been into cases of alleged illegal employee activities, either fraud or theft, of which you are aware?
- \_\_\_\_\_

19. In which department(s) did employee fraud occur in the last 12 months?

- \_\_\_\_\_ Finance
- \_\_\_\_\_ Operations - Revenue generating
- \_\_\_\_\_ Operations - Disbursements

- \_\_\_\_\_ Purchasing
  - \_\_\_\_\_ Receivables
  - \_\_\_\_\_ Investments
  - \_\_\_\_\_ Data Administration
  - \_\_\_\_\_ Other \_\_\_\_\_
- 

**Deterrence and Detection**

20. Are your staff and managers presently educated about methods of deterring, detecting and investigating employee fraud? If so, which of the following do you utilize?

- \_\_\_\_\_ Conferences organized by the Institute of Internal Auditors
- \_\_\_\_\_ Conferences organized by the Certified Fraud Examiners
- \_\_\_\_\_ Direct contact with anti-fraud organizations (e.g., Insurance Crime Prevention Bureau, police detachments)
- \_\_\_\_\_ Direct contact with other internal audit departments
- \_\_\_\_\_ In-house discussions
- \_\_\_\_\_ Personal readings
- \_\_\_\_\_ Hiring consultants to research in the area of employee fraud
- \_\_\_\_\_ Other \_\_\_\_\_

21. What are your primary ways of detecting fraud?

- \_\_\_\_\_ Specialized fraud audits
- \_\_\_\_\_ Internal audits
- \_\_\_\_\_ External audits
- \_\_\_\_\_ Unsolicited employee confessions
- \_\_\_\_\_ Tips from employees
- \_\_\_\_\_ Tips from outside the corporation
- \_\_\_\_\_ Management reviews
- \_\_\_\_\_ Other \_\_\_\_\_

22. If you conduct a fraud audit, what are the tests that you use to detect employee fraud?

---



---



---



---

23. In which of the following ways does the Internal Audit department become actively involved in deterring or detecting employee fraud?

If the following is a responsibility of the internal audit department, please identify with an "IA." If the following is not a responsibility of the internal audit department but the activity is carried out by some other department of the Corporation please identify with a "C."

- \_\_\_\_\_ Conduct credit checks or criminal checks of all employees
- \_\_\_\_\_ Administer a psychological test to test integrity (eg., Reid Report)
- \_\_\_\_\_ Develop a corporate "Code of Ethics" or "Standards of Conduct"
- \_\_\_\_\_ Educate employees about the corporation's internal controls and fraud policy other than through the dissemination of the "Code of Ethics" or "Standard of Conduct"
- \_\_\_\_\_ Educate managers about internal controls
- \_\_\_\_\_ Educate managers about the ways to detect employee fraud
- \_\_\_\_\_ Publish internally those cases where one has been found guilty of fraud
- \_\_\_\_\_ Have management sign a yearly statement stating their knowledge of the internal controls and their adherence to these controls
- \_\_\_\_\_ Seek the assistance of line management when developing new tests for detecting employee fraud through an internal audit
- \_\_\_\_\_ Test the strength of a manual system's controls to determine if the controls can be circumvented
- \_\_\_\_\_ Offer consulting services in the area of information systems development
- \_\_\_\_\_ Offer consulting services in the establishment of manual controls within departments
- \_\_\_\_\_ Check for possible areas where employees are involved in a conflict of interest
- \_\_\_\_\_ Conduct surprise audits
- \_\_\_\_\_ Set up a continuous auditing system that produces exception reports
- \_\_\_\_\_ Encourage employees to report serious employee fraud
- \_\_\_\_\_ Receive calls from external sources and follow up on those reports (eg., interviewing informers)
- \_\_\_\_\_ Engage in an on-going verification of the existence of vendors, suppliers. or employees
- \_\_\_\_\_ Use an external forensic accountant or fraud auditor
- \_\_\_\_\_ Other \_\_\_\_\_
-

24. Are your senior managers audited for fraud when it comes to actions against the corporation and actions on behalf of the organization (eg., conflict of interest, bribes, kickbacks, altering corporate records for the purpose of tax evasion, etc.,)? If "yes," in what way is this done?

---



---



---

25. Does your department use any of the following computer assisted audit techniques with the primary or secondary objective being the detection of employee fraud?

\_\_\_\_\_ Running external databases against your own databases to detect suspicious cases of data access

\_\_\_\_\_ Running internal databases against each other to detect suspicious cases of employee activity

\_\_\_\_\_ Exception reports of transactions exceeding a certain monetary amount or security level

\_\_\_\_\_ Programs to review physical inventory on a regular basis

\_\_\_\_\_ Other \_\_\_\_\_

- \* If external databases are used, which are they?

---



---

- \* If exception reports are produced, what variables have you identified as "suspicious" or as a "red flag?"

---



---



---

26. How does your department attempt to protect the organization's data?

\_\_\_\_\_ Become involved with the early development of computer systems

\_\_\_\_\_ Regularly audit the computer systems to look for security weakness

\_\_\_\_\_ Evaluate exception reports outlining data security violations

\_\_\_\_\_ Have dial up "front-ends" or "traps"

\_\_\_\_\_ Other \_\_\_\_\_

**Investigation**

27. When an auditor does make the choice to investigate an error or suspicious transaction, what activity is expected of the auditor?
- \_\_\_\_\_ Identify perpetrator(s)  
 \_\_\_\_\_ Determine how irregularity or suspicious transaction was perpetrated  
 \_\_\_\_\_ Document extent of loss  
 \_\_\_\_\_ Determine whether the perpetrator(s) was at premises when incident occurred  
 \_\_\_\_\_ Secure all relevant evidence  
 \_\_\_\_\_ Expand the sample and look for evidence of additional impropriety by the perpetrator(s)  
 \_\_\_\_\_ Other \_\_\_\_\_
28. What sources of evidence are reviewed during a fraud investigation?
- \_\_\_\_\_ Pre-employment records  
 \_\_\_\_\_ Performance records  
 \_\_\_\_\_ Payroll files  
 \_\_\_\_\_ Travel expense files  
 \_\_\_\_\_ Insurance claim or loan files  
 \_\_\_\_\_ Credit reports  
 \_\_\_\_\_ Information from suspect's managers  
 \_\_\_\_\_ Information from an interview with the suspect  
 \_\_\_\_\_ Other \_\_\_\_\_
29. After the auditor's investigation, how is the information used once it is collected?
- \_\_\_\_\_ Suspend perpetrator from his/her job  
 \_\_\_\_\_ Stop payments due to the perpetrator  
 \_\_\_\_\_ Request that assets of the perpetrator be frozen  
 \_\_\_\_\_ Turn over the case to your investigation department  
 \_\_\_\_\_ Turn over the case to outside police  
 \_\_\_\_\_ Other \_\_\_\_\_
30. Do you test for compliance with a standardized process among your auditors when it comes to identifying irregularities in an audit and the auditor's thoroughness in investigating that irregularity?

Yes / No

**Reporting**

31. When an investigation into employee fraud is carried out outside of the regular audit, is any type of report issued?
- Yes / No
32. If "yes", who issues the report?

\_\_\_\_\_ Line Management  
 \_\_\_\_\_ Internal Audit  
 \_\_\_\_\_ Investigation Unit  
 \_\_\_\_\_ Corporate Law  
 \_\_\_\_\_ Human Resources  
 \_\_\_\_\_ Other \_\_\_\_\_

33. If "yes", who are the recipients of the report?

\_\_\_\_\_ President  
 \_\_\_\_\_ Board of Directors  
 \_\_\_\_\_ Audit Committee  
 \_\_\_\_\_ Vice-President Finance  
 \_\_\_\_\_ Department Manager  
 \_\_\_\_\_ External Auditors  
 \_\_\_\_\_ Other \_\_\_\_\_

34. If "yes", which of the following are discussed in the report?

\_\_\_\_\_ Identification of the area of breakdown in controls  
 \_\_\_\_\_ Suggested alternatives in rectifying the problem  
 \_\_\_\_\_ Suggested possible recommendations as to how to deal with the offending party  
 \_\_\_\_\_ Other \_\_\_\_\_

35. Is there a follow-up to determine if appropriate changes to procedures or policies have been undertaken to ensure a similar fraud is unlikely to reoccur? If so, who is responsible for the follow-up?

Yes / No \_\_\_\_\_

### **NATURE OF BUSINESS**

In order to be able to group the responses by size of corporation, we would appreciate if you would supply the following information. Approximate numbers would be adequate.

36. How many people are employed by your company?

\_\_\_\_\_

37. For 1990, what were your revenues, premiums, and deposits?

\_\_\_\_\_

38. How can your corporation's computer environment be best described?

- \_\_\_\_\_ highly computerized environment
- \_\_\_\_\_ on-line real time  
\_\_\_\_\_ batch update
- \_\_\_\_\_ computer-assisted environment
- \_\_\_\_\_ mainframe  
\_\_\_\_\_ micro  
\_\_\_\_\_ both mainframe and micro
- \_\_\_\_\_ manual environment with limited computer system

**COMMENTS:**

39. Do you have any thoughts or ideas that you would like to share concerning the role of the internal audit department in the future with respect to employee fraud?

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

40. Are there any approaches or techniques that you have tried but found to be ineffectual in the deterrence, detection, investigation, or reporting of employee fraud?

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

Would you allow the above information to be used for preparing a M.A. (Criminology) thesis? The thesis will be written without revealing the identity of any corporation.

Yes / No

Would you like a summary of the questionnaire results?

Yes / No