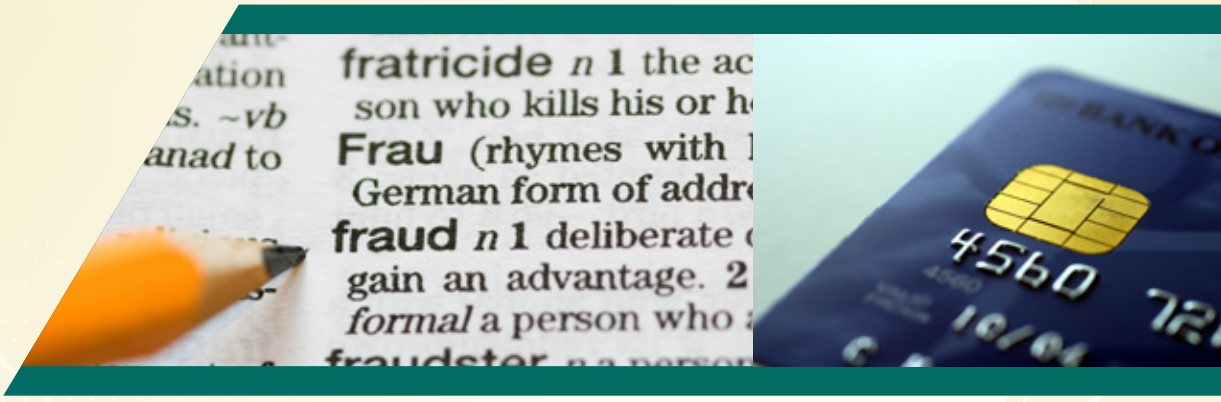
August 2010

GUIDELINES FOR MANAGING THE RISK OF FRAUD IN GOVERNMENT

www.bcauditor.com



OFFICE OF THE
Auditor General
of British Columbia

TABLE OF CONTENTS

The Five Principles Underpinning a Sound Fraud Risk Strategy 2

Principle 1:
Understand your fraud risks 2

Principle 2:
Ensure clear roles and responsibilities 3

Principle 3:
Have appropriately-designed prevention and detection measures 4

Principle 4:
Implement appropriate detective, investigative, disciplinary procedures and monitoring 5

Principle 5:
Regularly communicate fraud management results to stakeholders 8

Common Fraud Indicators 9

Recommended Reading 11

Principle 1: Government should have a well-developed understanding of the fraud risk inherent in its programs

Government, like any organization, needs to have a good understanding of the potential for fraud that exists in its various operations. This entails studying and analyzing its exposures, by size and type, to frauds that could occur. Without having a well-considered and documented understanding of fraud risk, government will be reactive instead of proactive and will not be able to efficiently and effectively mitigate its risk of loss due to fraud.

Fraud occurs in many forms. *Internal fraud* can be committed by employees:

- misappropriating assets – for example, stealing inventory, not recording all sales, setting up fictitious employees on the payroll, setting up false suppliers or shell companies, falsifying expense claims, or using business credit cards inappropriately; or
- making fraudulent statements or claims – for example, falsifying academic or training credentials or "cooking" financial records (such as creating fictitious revenues or concealing expenses).

External fraud can be committed by outside parties such as contractors or suppliers misappropriating an organization's assets. Billing for services not provided and falsifying eligibility for claims are examples of this type of fraud.

Fraud can also occur if an employee colludes with a party outside the organization. This can lead to corruption-related fraud, such as conflict-of-interest schemes and kickbacks.

Establishing a fraud risk register

A fraud risk register provides government with a critical tool for documenting the types and occurrences of fraud risk in its programs and operations.

The register should include the identification of each kind of risk, an assessment of the likelihood of its occurrence, the estimated significance (financial, legal and reputational) of the risk, and suggested responses to managing the risk. Such responses should be based an assessment of the incentives (or pressures) and the opportunities to commit fraud – essentially, where a fraud incident could happen and who might commit it.

The initial risk assessment should consider the inherent risk of fraud in government, absent of any existing controls.

Assessing incentives and opportunities: In assessing *incentives* that might compel individuals to commit fraud, one element to consider is the pressure on employees to achieve performance goals. For example, understanding bonuses and other performance-based pay within government, and the basis on which these are calculated, can help identify areas where a fraud incentive might exist.

In assessing *opportunities* that might give someone reason or temptation enough to commit fraud, it is important to think like a potential fraudster. Ask: Where are controls weak? How could controls be circumvented? How could the fraud be concealed?

Weak controls and a lack of segregation of duties can signal to some individuals a potential opportunity for committing fraud. The ability for senior management to override controls is another area of risk that should be assessed.

Gathering information about past frauds: Opportunities for committing fraud are always changing (consider how communication and information management technologies have changed access to information) and must therefore be constantly watched for. However, understanding the different types of fraud that government has already encountered in the past provides invaluable information for developing effective fraud prevention and detection techniques. This information should be captured as part of the case management system discussed under Principle 4, below.

Given the types of fraud seen in government environments, the following information should be tracked:

- the nature of the fraud;
- the duration and frequency of the fraud;
- the level of complexity or sophistication of the fraud;
- whether the fraud was committed by an employee, by an external party, or by both; and
- whether the fraud was an opportunistic incident or part of a targeted, organized crime?

Assessing frauds by type: A team approach to fraud risk assessment should be used to ensure that all types of potential frauds and all existing controls and possible corrective actions are considered. Financial managers, internal auditors, program staff, risk management staff, legal advisors and human resources staff should all be part of the assessment process to achieve best results.

Estimating the potential significance of various fraud risks: After considering the types of frauds that could be committed, the next step is to estimate the potential significance of each. This is most often done through statistical modelling and in-depth research. Statistical modelling by way of reviewing a sample of transactions for fraud and then extrapolating the results over the entire population is relatively simple. However, several factors may influence the accuracy of estimates:

- The population may not be homogeneous, making a representative sample difficult to extract.
- The available data may not be complete and thus not truly representative of all the fraud threats.
- It may be difficult to classify irregularities detected in the sample as clearly erroneous or fraudulent. Irregularities are not always the result of fraud, but may have occurred through negligence, incompetence or genuine mistake.

An example of *in-depth research* used to estimate risk significance would be applying published fraud statistics of other similar jurisdictions to the particular government operation and then estimating a level of fraud. Alternatively, an external firm could be engaged to conduct fraud penetration and data security testing against government operations.

Establishing appropriate controls for each risk identified: Risks identified should then be "mapped" to existing controls, and new controls should be designed and implemented as necessary to fill in gaps.

Both preventative and detective controls should be in place for risks that involve potential collusion or override by government managers, as controls such as segregation of duties will not likely be sufficient to detect fraud in those cases.

Planning appropriate responses to each risk identified: Responding to each fraud risk will depend on what government's risk tolerance is. A "zero fraud" policy, while theoretically the ideal goal to promote, will not likely be achievable since the cost to address all the fraud risks identified may be too high. Therefore, in risk response planning, it is important to consider what risks are worth covering, and what residual ones are not.

Principle 2: Fraud risk in government should be managed through clear roles and responsibilities

Establishing clear roles and responsibilities for managing fraud risk must begin first with establishing a focused and clearly explained fraud risk management policy. The policy should be part of the organization's operational manual, available to all staff. The requirement to comply with all operational policies – including the organization's fraud risk management policy – should also be included in the standard terms and conditions of employment contracts for all staff.

Developing a comprehensive fraud risk management policy

An organization should ensure that its fraud risk management policy includes:

- a definition of fraud and a description of the organization's attitude to fraud and commitment to investigating and prosecuting fraud;
- an explanation of staff responsibilities in preventing and reporting fraud;
- assurance that reported incidents or suspicious activities will be managed in a professional and confidential manner;
- a summary of the possible consequences of fraudulent behaviour (including disciplinary action, termination of employment or contract, counselling, and legal action to recover fraud losses); and
- a statement about arrangement for protecting "whistleblowers" (individuals who report suspected cases of fraud).

The fraud policy should also require employees and contractors to report suspected fraud immediately to the individual with the designated responsibility, ideally through a hotline. The fraud policy should promote the awareness of this hotline and the fact that protection exists for employees using the service.

Government should ensure that employees at all levels, plus contractors, have acknowledged through an annual sign-off that they have read the fraud risk policy and the organization's code of conduct and are abiding by those policies. The sign-off may also

include an acknowledgement that the employee is not aware of anyone committing fraud against the government. Having a conflict-of-interest policy in place also ensures that employees and contractors must come forward and disclose any potential or actual conflicts of interest they may have in carrying out their work.

Assigning roles and responsibilities

Assigning responsibility and accountability for managing fraud risk is important to ensure that the anti-fraud measures implemented by government can be effectively applied. The fraud risk management policy should assign responsibilities at all levels of staff so that everyone knows who is expected to do what in mitigating the risks.

This approach works best if fraud resources are integrated and coordinated within government. In large government organizations and in central government, it may be even more cost-effective to create a specialist unit that can focus exclusively on dealing with fraudulent activities.

Having a central, coordinated function in place for fraud risk management can also help ensure there is a systematic and organized process for the management of fraud risk. This will enable better efficiencies to be achieved in committing resources to fight fraud and also help illuminate any gaps in government's anti-fraud strategy.

Principle 3: Government should have appropriate preventative and deterrence measures in place and regularly monitor their performance

Prevention measures aim to stop frauds from occurring. These measures are the first line of defence against fraudsters, and it is essential that the measures be effective in stopping the majority of fraudulent activity. Frauds that circumvent these preventative and deterrence measures will require subsequent detective measures if they are to be found.

Developing and promoting an anti-fraud culture

Government can deter fraud by influencing the attitude towards it. Employees who view fraud as socially unacceptable or criminal are less likely to commit it than those who might try to justify doing it. Government should set the right tone from the top regarding its intolerance of fraud and make clear that ethical behaviour is expected throughout the organization.

Government can communicate deterrence messages to staff in many ways, for example by:

- *Establishing a robust fraud risk management policy* (as discussed under Principle 2)
- *Publicizing the fact that preventative, deterrence and detective controls are in place* – Effective preventative controls that are in place, working and well known throughout the organization will also serve as strong deterrents because most people are afraid of getting caught. Continuous communication and reinforcement of all controls are important. The message needs to get out to both internal parties (employees) and external parties (suppliers and contractors). Getting the message out to service deliverers that fraud will not be tolerated will also help get the same message out to service users (e.g., benefit claimants).
- *Conducting reference checks and criminal record checks* – Criminal record checks and background checks are important preventative and deterrent measures. The people being hired (employees and contractors) are in a position of trust and authority. A past history of criminal activity is a red flag for fraud. Before conducting criminal record checks, the government organization should consult with its Human Resources department and legal advisors to ensure legislation such as the Human Rights Act is not violated. A policy that encourages criminal record checks for all staff in a position of financial management and trust over public funds is good practice and government should consider requesting this from all such employees and contractors before beginning a business or employment relationship.

  Confirming reference checks and educational history can also uncover fraudulent statements. Any embellished or falsified statements represent increased risk that needs to be considered in the hiring process.
- *Making it known that previously disciplined employees and contractors will be red-flagged in the Human Resources system* to prohibit their obtaining future employment or contract work in government.
- *Including in supplier contracts information about government's fraud policy* – All contractors should be made aware of the fraud policy and required to sign off in the contract that they have read the terms of the policy and will comply with it.
- *Stressing in new employee orientations the organization's anti-fraud culture and fraud risk management program* – Initial orientation about the organization's anti-fraud culture and

ongoing education on the fraud risk management program are important for all employees. This will help reinforce the tone from the top.

- *Running annual fraud awareness training programs* – Fraud awareness training for staff should include defining fraud, explaining the fraud risk management policy, and giving examples of public sector fraud and of red flags that should alert employees to suspicious behaviour. Attendance at these training sessions and at periodic refreshers should be mandatory.
- *Regularly monitoring compliance with internal controls and communicating the findings of that work with all employees* (this is both a preventative and detective measure and is discussed in detail under Principle 4) – The importance a government organization attaches to its Internal Audit department is an indication of its commitment to maintaining internal controls. With respect to fraud risk management, Internal Audit can be involved in fraud investigations, conducting internal control reviews and making recommendations for improvement, monitoring fraud hotlines and providing fraud awareness training sessions.
- *Publicizing internally across the organization information about frauds that have been detected and the disciplinary action taken*
- *Establishing fraud hotline and whistleblower protection* (this is both a preventative and detective measure, and is discussed in detail under Principle 4) – It is important that employees and third parties have a process to report instances of non-compliance with the expected behaviour. A hotline for reporting tips anonymously is a common way. Those who do report fraud (whistleblowers) must also know they will be protected.

Limiting some employee roles and responsibilities

The level of authority granted to initiate and approve transactions should be reasonable for the employee's level of responsibility. This is especially important where fraud controls are few and duties are not well segregated.

In a good fraud risk management program, all fraud prevention and deterrent procedures are documented, along with the respective roles and responsibilities, and these procedures are monitored on a regular basis to ensure they remain effective and the responsibilities assigned to employees remain appropriate.

Making fraud risk an integral part of new program development

Considering the risk of fraud attacks when developing new programs can reduce later costs for implementing fraud prevention and detection measures. Internal Audit should be consulted early in the development process to assist with the identification of financial risks and the appropriate strategies to mitigate them.

Maintaining a continuous review of existing controls

Even though government may have instilled effective controls when a program was launched, those controls might become ineffective over time. This can result, for example, through fraudsters developing more complex methods of attack or through changes occurring in the business process of the program. Advances in information technology may also mean that new, more cost-effective controls are available to replace original controls.

For this reason, it is critical that organizations continuously and systematically review of controls.

Principle 4: Government should have appropriate detective, investigative and disciplinary procedures in place and regularly monitor their performance

Tackling fraud head-on using proactive methods of detection is good practice. Detective procedures are required to uncover frauds when preventative measures are not in place or are not strong at mitigating the risk. Detecting frauds and prosecuting fraudsters will not only reduce losses to an organization but also deter other potential fraudsters. Fraud detection will also help to identify new threats, or themes, that are developing. Based on these developments, the organization's strategic approach to managing fraud risk can be suitably updated (if necessary).

Important to keep in mind is that these are not intended to *prevent* fraud occurring. The cost-effectiveness of prevention techniques versus detective techniques should be considered when designing fraud controls. It may be more cost-effective to have good detective measures in place versus preventative controls.

Detecting fraud activities

Establishing detection measures: Reconciliations, independent reviews, physical inspections, analysis and audits are all process controls designed in part to detect fraudulent activity. The design of these process controls is best done after first analyzing the types of frauds that could be committed in the government environment.

Two especially good proactive detection measures to analyze financial data are installing fraud hotlines and using computer-assisted techniques.

- *Fraud hotlines:* Fraud hotlines are the most common source of detected frauds, and can be a cost-effective way for staff – and even members of the public – to report suspicious activity.
- *Computer-assisted techniques:* Techniques such as data matching and data mining can also aid in detecting suspicious activity.

  Data matching uses computers to match different data files and scan for abnormalities. For example, matching a series of electronic payment transfers to an approved supplier list can be used to look for suspicious payments.

  Data mining uses computer models to generate patterns, themes or associations that may help identify suspicious activity. For example, sorting an organization's credit card transaction data by payee or transaction day can be used to look for suspicious activity.

  The advantage of data matching and data mining is that a large amount of transaction data can be reviewed and analyzed in a relatively short time. Operators can also easily filter and prioritize data based on pre-determined risk assessments.

  Before undertaking this work, however, government should be aware and take account of any legislation that may limit the collection and use of personal information for purposes of data matching.

Monitoring effectiveness of detection methods: It is important to assess the effectiveness of the detective measures in use through continuous monitoring. Measurement criteria to monitor fraud detection performance in government include:

Guideline for setting up a fraud hotline:

- A single free telephone number should be used. This can be supplemented by an online email submission form or regular mailing address.
- The hotline's existence and number should be well advertised.
- The message should be reinforced that information received through the hotline will be kept confidential and employees will not face any retribution for reporting their suspicions.
- Assigned staff or pre-recorded messages should use standard pre-defined questions when calls are taken to enable the capture of all pertinent information.
- A system should be used to log the calls and monitor their follow-up.
- The call data should be analyzed at regular intervals to allow management to adjust its strategic approach to managing fraud risk (if necessary). Call volume, call type and percentage successful outcomes are all aspects that should be reviewed.
- The fraud-related issues detected through the tips should be communicated to the appropriate authorities according to the organization's established fraud policy.

- number of known frauds committed;
- number and status of fraud allegations that require investigation;
- number of fraud investigations resolved;
- number of whistleblower allegations received through the hotline;
- number of employees who have not had fraud awareness training;
- number of employees in key financial positions who have not had background checks;
- number of employees and suppliers/contractors who have not signed the code of conduct; and
- number of fraud audits performed by Internal Audit.

Investigating and responding to fraudulent activities

Having clear fraud investigation practices and strong sanctions in place are good ways for public sector organizations to show staff, suppliers and the public that government is serious about managing fraud risk. Investigations and sanctions not only deal with newly uncovered (or potential) fraud cases, but may also deter other people from committing fraud in future. As well, government can improve its chances of recovery from fraud losses and minimize its exposure to reputation damage by having sound investigative and disciplinary processes in place.

When a fraud has been detected it should be stopped at the earliest opportunity. Management should determine how the fraud was perpetrated and if any weak controls can be identified. Weak controls may be an indicator that the fraud was not an isolated incident and other similar frauds may be underway.

Centralizing the investigative process: A process for how allegations of fraud and fraud investigations is to be conducted should be clearly laid out by government and followed. The fraud policy should mention who is to conduct or manage the investigation process. A centralized detective and investigative function allows for better control over the fraud risk exposure, and allows for resources to be focused on those risks identified as priority. It also helps ensure that consistent corrective actions and sanctions are applied consistently.

Centralizing the investigative process also enhances the communication process within government in that all the information can then be managed in one place. For this function to operate effectively, there must be an appropriate level of authority and an adequate number of skilled investigators.

Conducting investigations: The investigation team should document and track the steps of the investigation, items collected as evidence, requests for documents and other information, interview meeting notes, conclusions drawn from analysis of evidence, and interviews conducted. A case management system should be used where the allegations of fraud can be logged and monitored. If the allegations are determined to warrant further investigation, a clear, high-quality investigative process should be in place both to mitigate losses and to ensure that appropriate corrective action is taken (for example, improving controls and handing out sanctions such as employment termination or the possible laying of criminal charges).

Actions taken must also be applied consistently and fairly by type of fraud committed and level of employee. The Human Resources department and legal counsel should be consulted early on in the investigative process and before any disciplinary, civil or criminal proceedings. If it is likely that the case will proceed with criminal charges, police should also be involved to ensure sufficient and appropriate evidence and documentation are collected in the case file.

Prioritizing investigations: Investigative work should always be assigned on a risk basis to ensure that the greatest threats receive the highest priority. Likely remediation costs (for example, investigation costs, legal fees) should also be determined so that government can assess the likely cost outlay relative to the determinable fraud loss. In this way, cases that have the greatest possibility of generating positive outcomes can be given the highest priority.

Taking corrective action: In some cases – for example, to mitigate loss and preserve evidence – it may be necessary to take corrective action before the investigation is complete. Those under investigation may need to be suspended or re-assigned while the investigation is ongoing and assets may need to be protected. Management should seek legal advice before taking any actions.

Important to keep in mind as well is that employees may be under an obligation to respond to their employer's questions while they are still employed. Thus, if they are fired before the investigation is complete, this obligation will no longer exist and investigation delays could result.

Possible corrective actions include:

- criminal referral (which may be a legal obligation; legal counsel and senior management should be consulted before the investigation unit pursues this action);
- civil action (government may wish to pursue civil action to recover funds);
- disciplinary action (for example, termination, suspension with or without pay);
- an insurance claim; and
- remediation to the existing business process and internal controls.

Reporting the findings: A report on investigation findings should be prepared by, or submitted to, a central investigations unit. The external auditor should also be notified of all fraudulent activities. The external auditor will also want to conduct an

assessment of whether there is a more serious and pervasive problem rather than relying on management's own assessment. This makes it critical that all known frauds be communicated in a timely manner to the external auditor.

The investigations unit should also keep track of performance measures such as:

- issue resolution time (by category of complexity);
- repeat incidents (to highlight control or business process weaknesses that have not been addressed); and
- value of loss recovered and prevented (this can help demonstrate the value of fraud risk management actions, but the value of the deterrence message should also be considered).

These measures should be reviewed on a regular basis to determine whether the investigative process continues to operate effectively.

Principle 5: Government should have appropriate reporting procedures in place to communicate the results of its fraud risk management activities to its stakeholders

Internal reporting on fraud risk management activities

A reporting mechanism should be in place to enable government departments to report instances of known losses immediately to the individual with the designated responsibility as prescribed in the fraud policy. By having timely information from all departments, that individual will be able to spot trends of losses by type and decide what investigative and corrective actions are required.

Those staff responsible for fraud risk management throughout government should also receive regular, comprehensive reports on fraud risk management activities. This will help them identify trends and move to mitigate losses effectively and efficiently. Such reports reviewed regularly can also illuminate where program or operating procedural changes may be required. If a good case management system is in place in the centralized investigative unit, then this reporting will be easier to complete.

Reporting externally on fraud risk management activities

External reporting about government's efforts to manage fraud risks helps communicate from the top the importance that government places on managing this highly important risk area.

External reporting should address:

- the activities undertaken in the reporting period;
- the results of those and previous activities;
- the corrective actions taken; and
- the sanctions that resulted.

COMMON FRAUD INDICATORS

Managers and staff should be vigilant

to any warning signs that might indicate a fraud is being perpetrated. Potential indications that a person might be involved in fraudulent activity are if he or she:

- seems under stress without a high workload;
- is first to arrive in the morning, last to leave at night;
- is egotistical (e.g., scornful of system controls);
- is a risk-taker or rule-breaker;
- is reluctant to take time off work;
- refuses a promotion;
- exhibits wealth inconsistent with salary;
- exhibits a sudden change of lifestyle;
- is a new staff member who resigns quickly;
- has a cozy relationship with suppliers or contractors;
- is a supplier or contractor who insists on dealing with one particular member of staff;
- is disgruntled at work, a complainer; and is greedy or is known to have genuine financial need.

Internal Audit departments and similar assurance type departments should also be vigilant while performing engagements. Potential indications of an environment in which fraud is possible include:

- unusual employee behaviour (e.g., a supervisor who opens all incoming mail; managers bypassing subordinates; subordinates bypassing managers; an employee who refuses to comply with normal rules and practices, fails to take leave, lives beyond his or her means, regularly puts in long hours working, often expresses job dissatisfaction, or acts secretively or defensively);
- key documents missing (e.g., invoices, contracts);
- inadequate or no segregation of duties;
- absence of controls and audit trails;
- inadequate monitoring to ensure that controls work as intended;
- documentation that is photocopied or lacking essential information;
- missing expenditure vouchers and official records;
- excessive variations to budgets or contracts;
- bank and ledger reconciliations that are not maintained or cannot be balanced;
- excessive movements of cash or transactions between accounts;
- numerous adjustments or exceptions;
- overdue pay or expense advances;
- general ledger that is out of balance;
- duplicate payments;
- ghost employees on the payroll;
- large payments made to individuals;
- crisis management coupled with a pressured business environment;
- lack of established code of ethical conduct;
- lack of senior management oversight;
- unauthorized changes to systems or work practices;
- lack of rotation of duties;
- policies not being followed;
- post office boxes being used as shipping addresses;
- lowest tenders or quotes being passed over with minimal explanation recorded;

- single vendors;
- unclosed but obsolete contracts;
- service needs being described in ways that can be met only by specific contractors;
- service requirements being split up to get under small purchase requirements or to avoid prescribed levels of review or approval;
- vague specifications;
- unclear disqualification of a qualified bidder;
- climate of fear or an unhealthy corporate culture;
- high staff turnover rates in key controlling functions;
- chronic understaffing in key control areas;
- low staff morale/lack of career progression/weak management;
- consistent failures to correct major weaknesses in internal controls;
- management that frequently overrides internal controls;
- an employee reluctant to take leave, or an employee on leave stipulates that work must not be done until he or she returns; and
- lack of use of commonsense controls such as changing passwords frequently, requiring two signatures on cheques or restricting access to sensitive areas.

It is important to note that anyone exhibiting one or more of these behaviours does not guarantee that a fraud is being perpetrated; however they can indicate a higher fraud risk is present and that the related internal controls should be examined and remediated as needed.

RECOMMENDED READING

- Association of Certified Fraud Examiners (ACFE), *2008 Report to the Nation on Occupational Fraud and Abuse*, 2008.
- Institute of Internal Auditors (IIA), The American Institute of Certified Public Accountants (AICPA), Association of Certified Fraud Examiners (ACFE), *Managing the Business Risk of Fraud: A Practical Guide,* 2009.
- *The Institute of Internal Auditors* (IIA), *Fraud Prevention and Detection in an Automated World*, 2009.
- Institute of Internal Auditors (IIA), *Internal Audit and Fraud,* 2009.
- Canadian Institute of Chartered Accountants(CICA), *Canadian Auditing Standard 240 -The Auditor's Responsibilities Relating to Fraud in an Audit of Financial Statements*, 2010.
- HM Treasury, National Audit Office, *Tackling External Fraud,* 2008.
- HM Treasury, *Managing the Risk of Fraud: A Guide for Managers,* 2003.
- Audit Scotland, Audit Commission, *National Fraud Initiative 2008/09: Handbook Scotland,* 2009.
- The Audit Office of New South Wales, *Fraud Control: Developing an Effective Strategy.*
- The Audit Office of New South Wales, *Fraud Control Current Progress and Future Directions: Guidance on Better Practice,* 2005.
- KPMG, *Profile of a Canadian Fraudster: Survey Report 2009,* 2009.