index

background ............................................................................................................. 4
what is fraud? ........................................................................................................... 5
antifraud regime: prevention and timely detection ............................................. 6
key elements of an antifraud regime ..................................................................... 7
  1. governance - oversight by the audit committee and board ...................... 7
  2. fraud risk assessment .................................................................................... 7
  3. code of business conduct and ethics ............................................................. 8
  4. incident reporting mechanisms ................................................................... 9
  5. investigative protocol .................................................................................... 10
  6. remediation protocol ................................................................................... 10
  7. hiring and promotion policies and procedures ....................................... 11
  8. management evaluation and testing ........................................................... 11
summary and conclusion ..................................................................................... 13
end notes .................................................................................................................. 14
political and legislative context

In 2002, the United States Congress passed the Sarbanes-Oxley Act \(^1\) (the Act) designed to restore shareholder confidence in publicly traded securities following a series of highly publicized corporate scandals. In response to the Act, the Ontario government introduced Bill 198, Keeping the Promise for a Strong Economy (Budget Measures), 2002 (Bill 198) \(^2\) which received Royal Assent on December 9, 2002. Bill 198 expanded the powers of the Ontario Securities Commission (OSC) and made it easier for investors to initiate legal action against companies that issue false or misleading statements. Since the enactment of Bill 198, efforts have focused on strengthening enforcement, improving financial reporting and disclosure, enhancing the quality of the audit process and strengthening corporate governance and management accountability, resulting in the following:

- Auditor reforms through the creation of the Canadian Public Accountability Board \(^3\)
- Modifications to civil liability in Ontario \(^4\) and through the Canadian Securities Administrators (CSA) \(^5\)
- Modifications to the audit committee requirements through Multilateral Instrument 52-110 (MI 52-110) Audit Committees
- The issuance of Multilateral Instrument 52-109 (MI 52-109)—Certification of Disclosure in Issuers’ Annual and Interim Filings, which is similar to Section 302 of the Act
- National Policy 58-201 (NP 58-201) Corporate Governance Guidelines, which provides guidance on corporate governance practices

Responsibility for managing the company and preparing financial statements has traditionally rested with management and the board of directors. The changes to Canadian regulations makes it abundantly clear, if there was ever any doubt, that these individuals are also responsible for establishing, validating and monitoring effective internal controls to prevent fraudulent financial reporting—and to detect it on a timely basis if it does occur.
what is fraud?

Fraud is a broad concept that generally refers to any intentional act by one or more individuals, involving the use of deception to secure an unfair or unlawful gain. The primary factor that distinguishes fraud from error is whether the underlying action that results in the misstatement of financial statements is intentional or unintentional. Financial fraud typically falls into five broad categories:

- Fraudulent financial reporting—deliberate accounting misstatements, accounting manipulation, the creation of fictitious transactions and records and/or intentionally inaccurate or incomplete disclosures with the intention of misleading users of the financial information
- Asset misappropriation—straightforward theft of cash, securities, inventory or fixed assets, the circumvention of company controls and procedures (i.e. procurement and payroll fraud), the theft of business secrets or other intellectual property and the diversion of revenues, asset stripping and other breaches of fiduciary duty
- Unauthorized receipts and expenditures—an umbrella term for engaging in corrupt business practices to influence the awarding of business opportunities, or subverting government objectives
- Disclosure fraud—intentionally providing inaccurate or incomplete information (not just limited to the financial statements)
- Aiding and abetting—facilitating the misconduct of others, i.e. entering into structured financial transactions designed to assist the client or business partner in manipulating its financial statements
The CSA has proposed to expand management’s certifications under the existing MI 52-109 to require the CEO and CFO to certify the following in their annual certificates:

- They have evaluated the effectiveness of the issuer’s internal control over financial reporting as of the end of the financial year; and that
- Based on their evaluation, they have caused the issuer to disclose in its annual MD&A their conclusions about the effectiveness of internal control over financial reporting as of the end of the financial year.

Included in the definition of “internal control over financial reporting” is the requirement to “provide reasonable assurance regarding the prevention or timely detection of unauthorized acquisition, use or disposition of the issuer’s assets that could have a material effect on the annual financial statements or interim financial statements.” Although the Ontario Government and the Ontario Securities Commission have not yet delineated what constitutes an effective antifraud program and controls, PricewaterhouseCoopers has identified the key elements of an effective antifraud program based on the core principles shared by the new regulations and standards: prevention and timely detection of fraud.
The key elements outlined below are based on best practice in the industry and each company will have to determine the extent to which each area is appropriate for their particular organization. It is essential that management and audit committees are aware of what they should be doing to build an organization-wide commitment to anti-fraud best practice processes and controls. In practice, this means that management and audit committees should reassess the completeness and accuracy of the information that they exchange, discussing whether it is sufficiently comprehensive and objective to serve the corporate decision-making process which it is intended to support. They should also have this discussion with their external auditors.

1. governance—oversight by the audit committee and board

The organization’s board of directors and audit committee significantly influence the control environment and “tone at the top”. The board, in its fiduciary role, is responsible for overseeing the internal controls over financial reporting established by management and the process by which management satisfies itself that they are working effectively. The board is also responsible for the identification of risks related to the issuer’s business and ensuring that management implements appropriate systems to address these risks. Included in these risks, is the risk of financial fraud by management and employees.

It is critical that the audit committee and the board of directors systematically and periodically review the internal controls over financial reporting established by management and that such responsibilities for oversight are reflected in their charters. Oversight should extend to:

- Management’s antifraud programs and controls including the fraud risk assessment process
- Incident reporting mechanisms for employees to report concerns
- Receipt and review of periodic reports describing the nature, status and eventual disposition of alleged or suspected fraud and misconduct reported
- An internal audit plan as applicable, that addresses fraud risk and a mechanism to ensure that the internal audit can express any concerns about management’s commitment to appropriate internal controls or to report suspicions or allegations of fraud
- Involvement of other experts—legal, accounting and other professional advisers—as needed to investigate any alleged or suspected wrongdoing brought to their attention

2. fraud risk assessment

The fraud risk assessment is a critical step in addressing fraud risks within an organization and, as such, should be an area of significant focus for management. It is performed company wide, at an entity level and for significant business units and significant accounts. An entity needs to be aware of and deal with the fraud risks that it faces. It expands upon the traditional risk assessment and is a critical step in addressing fraud risks within an organization. A fraud risk assessment:

- Is scheme and scenario based (absent any controls) rather than based on control risk or inherent risk
- Is performed on a comprehensive and recurring basis rather than in an informal or haphazard manner
- Considers the various ways that fraud and misconduct can occur within and against the company
- Considers vulnerability to management override and potential schemes to circumvent existing
control activities, which may require additional compensating control activities

- Considers vulnerability of the entity to fraud and its potential impact on financial reporting
- Includes the potential for fraudulent financial reporting, misappropriation of assets, unauthorized receipts and expenditures, disclosure fraud and aiding and abetting
- Considers the risk of fraud by senior management or the board of directors (persons of influence)
- Considers incentives and pressures on management to commit fraud
- Considers past allegations and actual incidents of fraud and misconduct
- Considers fraud and misconduct in the industry
- Considers past significant control violations, which may have led to fraud and misconduct
- Evaluates and prioritizes the fraud risks
- Evaluates whether mitigating controls exist and are effective

Organizations need to reach their own conclusions with respect to the cost of controlling a risk compared to the benefits of mitigating or eliminating that risk. An organization should, however, have a documented process that assesses, identifies and evaluates fraud risk.

The audit committee and the board of directors, in performing their fiduciary duties, are responsible for considering their own knowledge of the company's underlying performance, the types of fraud prevalent in the sector and the risk of financial fraud by management, and ensuring that controls or mitigating actions have been taken to prevent and detect fraud.

### 3. code of business conduct and ethics

The term code of business conduct and ethics ("code of conduct") is defined in NP 58-201 Corporate Governance Guidelines as written standards that are reasonably designed to deter wrongdoing and to promote ethical conduct. In particular it recommends the code of conduct address the following:

- **a. conflicts of interest**, including transactions and agreements in respect of which a director or executive officer has a material interest
- **b. protection and proper use of corporate assets and opportunities**
- **c. confidentiality of corporate information**
- **d. fair dealing with the issuer’s security holders, customers, suppliers, competitors and employees**
- **e. compliance with laws, rules and regulations**
- **f. reporting of any illegal or unethical behaviour**

In addition to the items listed above, the code of conduct should articulate what constitutes fraudulent behavior, how accountability for the code is established and the sanctions imposed for noncompliance. The monitoring of compliance with the code should be the responsibility of the board, including the approval of any waivers for directors or executive officers.

NI 58-101 Disclosure of Corporate Governance Practices requires a reporting issuer to disclose whether or not the board has adopted a written code of conduct that applies to the company's directors, officers and employees. Issuers should also disclose the following:

- How compliance with the code of conduct is monitored or if the board does not monitor, whether and how they gain assurance over compliance with the code of conduct
- How a person or company can obtain a copy of the code of conduct
- A cross reference to any material change reports that have been filed which pertain to a violation of the code of conduct by a director or executive officer.

Due to the potential for apparent or actual conflicts of interest, it is recommended that the code of conduct apply internally and externally to anyone who has significant influence over relationships and dealings with suppliers, customers, investors, creditors, insurers, competitors, auditors and so forth.
assessing operating effectiveness

The mere existence of a code of conduct does not evidence its effectiveness. Operating effectiveness is evidenced through the following:

- **Antifraud regime communication plan**—There should be clear communication of antifraud policies and procedures which flows down, up, and across the organization on a periodic basis to all applicable persons. The communication should include: incident reporting mechanisms available, types of violations required to report, availability of the code of conduct to all employees (through employee handbook, policy manual, intranet, etc); behaviour which is acceptable and unacceptable, and strong knowledge sharing regarding fraud risks, control activities, allegations of fraud, and remediation.

- **Annual confirmation**—Employees should evidence their receipt and understanding of the code of conduct on an annual basis. The company should design a process that clearly demonstrates that all employees have signed off and that proper follow up for “non responses” is completed. The results should be summarized and provided to the audit committee and senior management for review.

- **Antifraud regime training and education**—A comprehensive training program should address “tone at the top”, code of conduct, use of incident reporting mechanisms, the individual’s obligation to report actual or suspected violations and the penalties for not reporting. The training program should be completed at the time of hire and periodically thereafter, and records documenting the type of training should be retained.

- **Management and audit committee involvement and oversight**—Both management and the audit committee are required to monitor the code of conduct and document the monitoring as evidence.

4. **incident reporting mechanisms**

Mi 52-110 requires each issuer’s audit committee to establish procedures for:

- Receiving and retaining information about, and treating alleged incidents involving the issuer regarding accounting, internal accounting controls or auditing matters; and
- The confidential, anonymous submission of concerns by employees about questionable accounting or auditing matters.

Companies use a variety of incident reporting mechanisms. Examples include:

- direct reporting to either the audit committee, management or Compliance Officer/Committee
- use of a P.O. Box
- use of websites/e-mails
- use of a 1-800 Ethics Hotline.

Not all incident reporting mechanisms need to be independent of management, anonymous and confidential. However, a company must establish at least one incident reporting mechanism which will provide employees with an anonymous and confidential means to report incidents that operates independent of management. One way to achieve independence is to use an independent third party to provide the intake mechanism. Alternatively, a company may establish a neutral party within the organization, such as a Compliance Officer/Committee who reports directly to the audit committee. The key factors to consider in selecting a mechanism are employee awareness, understanding, acceptance and usage.

Best practice includes the audit committee directly overseeing the incident reporting process. Normally a Compliance Officer/Committee is established to receive, log and vet violations, confirm they have been appropriately investigated, remediated and communicate the results directly to the audit committee. The purpose behind the Compliance Officer/Committee is to have individuals who are independent of the financial reporting process and least likely to be subject to a fraud allegation or oversee those persons subject to a fraud allegation, such as Legal Counsel, Internal Audit and Human Resources. Companies need to ensure that all incidents reported through the various mechanisms find their way to the audit committee.
The key objective of the incident reporting process is employee awareness, understanding and acceptance and the usage of the incident reporting mechanisms through proper training, education and communication. The process should be tested through an examination of the various communications and a sample of alleged incidents. Because a hotline is essentially a passive process that relies on the initiative of individual employees, volume of use may be a strong indicator of effectiveness, providing insight into whether people believe they are encouraged to report an alleged incident. A pulse survey or “walkabout” (corroborating through inquiries of employees and by making calls to customers and vendors) may also provide insight into employees’ views and their willingness to use the hotline.

5. Investigative protocol

A company should develop a standardized process for responding to allegations or suspicions of fraud. It should not wait until fraud is detected to develop an investigative process. Management, the audit committee and the board of directors should take appropriate actions to address any incidents of suspected, alleged or actual fraud that is material, as well as fraud of any magnitude involving senior management.

The results of all investigations should be communicated to the audit committee. Management should not be involved in this decision making process in order to maintain independence in the process. Management can, however, be involved in the investigative decisions and investigation itself, albeit under the direction of the Compliance Officer/Committee (and audit committee). The audit committee should be informed on a timely basis and in some situations, where incidents involve senior management, should be actively involved in the decision making process.

An investigative protocol should be created which addresses how items are reported to the audit committee and provides guidance to companies in addressing the following issues which should be considered when reviewing an incident:

- Objectives
- Source of allegations
- Target response time
- Feedback to whistleblower
- Documentation standards
- Type of reporting
- Monitoring
- Investigative style
- Loss of crucial evidence vs. loss of opportunity to gather facts
- Legal liability
- Rights of accused
- Requirement for external expertise (lawyers, investigators and forensic accountants)

The investigation protocol will also assist the issuer in preparing the disclosure related to violations of the code of conduct by a director or executive officer. The material change reports under National Instrument 51-102 Continuous Disclosure, requires issuers to disclose the details of the departure including the date of departure, party(ies) involved, whether the board has sanctioned the departure(s) and the supporting reasons behind the decision, and any measures it has taken to remedy or address the issue.

6. Remediation protocol

In order to demonstrate to employees and stakeholders in the business that unethical behaviour will not be tolerated, a company should develop a remediation protocol which generally involves:

- Taking disciplinary and legal action against wrongdoers
- Recovering/restoring losses and other damages
- Learning from an incident to improve controls and prevent recurrence
- Communication to the audit committee and the independent auditor explaining (i) why the controls failed, and (ii) what action has been taken to prevent a recurrence
The PricewaterhouseCoopers Global Economic Crime Survey found that there was a significant difference between the way companies responded to senior management discovered to be involved in fraud and the way they dealt with other staff members. Fraudsters within senior management were reported not only to have been dismissed less frequently than other grades of staff, but also to have been subject to criminal charges less frequently (34%). Consistency in dealing with fraud when detected, whether by internal reprimand or criminal prosecution is of primary importance, no matter what the staff level. Signs of favouritism in responding to incidents may lead to a rapid drop in staff morale and the possibility of further associated problems.

7. hiring and promotion policies and procedures

Establishing standards for hiring and promotions ("Intelligence Screening") demonstrates a company's commitment to competent and trustworthy people, reduces liability and ensures that standards are applied uniformly and in compliance with laws and regulations.

The first step toward effective Intelligence Screening is to assess the risks and responsibilities associated with each category of employee in order to design a background research profile. Depending on the risk profile created, Intelligence Screening should cover all or a select few of the following areas:

- criminal checks
- civil checks
- reference checks
- academic qualifications
- previous employment
- credit checks

A decision grid which lays out the organization's response to the background investigation is also recommended. The grid should include a course of action for various behaviours reported in consideration of the organization's tolerance for such reported behaviours. This will ensure consistency and reduce the risk to the organization when an employee or applicant disputes the findings. Legal counsel should be involved in the development of the decision grid in order to ensure compliance with local laws and regulations.

The company should consider when the information should be gathered to make an informed decision. The information gathering process can occur during any one or combination of the following:

- Completed at the time of application
- Completed after the first interview
- Completed prior to extending an offer of employment
- Completed prior to hiring (offer conditional upon results)
- Completed prior to or subject to promotion

The company also needs to determine who will conduct the Intelligence Screening process, taking into consideration the following:

- Independence
- Expertise
- Capacity to gather information and access to numerous database sources

Best practice would suggest retroactive background investigations should be performed for all employees within a company to ensure the company is in compliance with a policy being implemented for hiring and promotion. In particular, Intelligence Screening should be performed on individuals being considered for employment or for promotion to certain positions of trust within the organization.

8. management evaluation and testing

As is the case with all internal controls, a company's antifraud controls, programs and policies must be monitored through ongoing and periodic performance assessments. The frequency of separate evaluations or audits necessary for management to have reasonable assurance about the effectiveness of its antifraud controls is a matter of management's judgment.
In making that determination, consideration should be given to the following: the nature and degree of changes occurring in the entity and their associated risks, the competence and experience of the individuals implementing the controls, and the results of ongoing monitoring.

Ongoing monitoring occurs in the course of operations and should be built into the normal, recurring operating activities of an enterprise. Separate evaluations will ordinarily be conducted by the internal audit department or equivalent function. The scope and frequency of separate evaluations will depend primarily on an assessment of fraud risks and the effectiveness of ongoing monitoring procedures. It is essential that the organization’s plan, approach and scope of monitoring activities be documented and reviewed from time to time.
Preventing, detecting, investigating and prosecuting fraud is a constant struggle. Companies must not drop their guard. There are always individuals or groups of individuals who have an incentive and the ability to rationalize committing fraud and the ability to spot an opportunity to circumvent or override controls. Companies that establish effective antifraud programs as described above will meet compliance requirements. More important, however, they will go a long way toward meeting their shareholders’ expectations and helping to restore confidence in the financial markets. Finally, fraud prevention and detection can create cost savings that go directly to the bottom line and promote a culture of honesty, openness and create a positive work environment. Fraud management makes good business sense.

For future information contact:
Steven P. Henderson
steven.p.henderson@ca.pwc.com
416-941-8328

Julie C. Whitmore
julie.c.whitmore@ca.pwc.com
416-941-8286
end notes

2. Bill 198, Keeping the Promise for a Strong Economy Act (Budget Measures), 2002
3. The Canadian Public Accountability Board is a not-for-profit corporation incorporated in early 2003 with the mandate to promote high quality independent audits of reporting issuers. Further information on the Canadian Public Accountability Board can be found at www.cpab-ccrc.ca
4. Bill 198 resulted in several amendments to the Ontario Securities Act including: Section 126.1 - Fraud and Market Manipulation, Section 126.2 – Misleading or untrue statements, Section 130.1 – Liability for Misrepresentation in a Prospectus and Part XXIII – Civil Liability. The full text of the Securities Act can be found at www.e-laws.gov.on.ca/DBLaws/Statutes/English/90s05_e.htm
5. CSA “is a forum for the 13 securities regulators of Canada’s provinces and territories to coordinate and harmonize regulation of the Canadian capital markets.” Further information on CSA can be found at www.csa-acvm.ca
6. Black’s Law Dictionary defines fraud as “An intentional perversion of truth for the purpose of inducing another in reliance upon it to part with some valuable thing belonging to him or to surrender a legal right; a false representation of a matter of fact, whether by words or by conduct, by false or misleading allegations, or by concealment of that which should have been disclosed, which deceives and is intended to deceive another so that he shall act upon it to his legal injury.”
7. Source: “Fraud: Time for straight-talking and constructive action” by Steven P. Henderson and Julie Whitmore, Canadian Treasurer, April/May 2006 issue.
10. National Policy 58-201—Corporate Governance Guidelines, 3.8 (a) to (f)
11. National Policy 58-201—Corporate Governance Guidelines, 3.9
12. National Instrument 58-101—Disclosure of Corporate Governance, 5. Ethical Business Conduct (a) to (c)
13. General Assurance and Auditing Section 5135 the auditor’s responsibility to consider fraud paragraph .033 (a)
14. Multilateral Instrument 52-110 Audit Committees Section 2.3 (7)
15. National Policy 58-201, 3.9