AUDIT OFFICE OF GUYANA

FORENSIC MANUAL

OFFICE OF THE AUDITOR GENERAL OF CANADA

Wrongdoing and Fraud Audit Guidance

February 2005

Ce document est également disponible en français.

Table of Contents

Audit Guidance for Wrongdoing and Fraud

Introduction

About this Audit Guidance

This audit guidance has been developed to

- raise auditors' awareness of wrongdoing and fraud in government operations and programs,
- assist auditors in identifying possible incidents of wrongdoing and fraud while undertaking their various audits,
- explain red flags that may indicate wrongdoing and fraud, and
- suggest actions to take when auditors suspect wrongdoing and fraud.

Whether conducting attest audits, special examinations, or performance audits, auditors have a responsibility to be aware of the indicators and the risks of wrongdoing and fraud in order to detect and report. Given the hidden nature of wrongdoing and fraud, and the inherent limitations of an audit, the Office of the Auditor General (OAG or the Office) recognizes that some risk remains that wrongdoing and fraud will not be detected.

This audit guidance sets out the Office's audit policy, procedures, and standards as they relate to wrongdoing and fraud.

This guidance information will help OAG auditors to identify wrongdoing and fraud when conducting audits. It provides tools and assistance to assess the risks of wrongdoing and fraud, and encourages appropriate action (see "Office of the Auditor General—Audit Policy on Wrongdoing and Fraud" on page 113) when auditors suspect wrongdoing or fraud.

This audit guidance is designed to be user-friendly and offers search capability and direct links to specific topics. Readers are encouraged to peruse the information and seek out areas of interest.

As further guidance, ten checklists are provided that can assist the auditor to assess an entity's vulnerability to wrongdoing and fraud and to help identify indicators of wrongdoing and fraud.

Background

What is Wrongdoing?

This audit guidance refers to wrongdoing as improper conduct or inappropriate activities such as

- abusing or exceeding authority,

- conflicts of interest,
- gross administrative abuse,
- improper contract or contribution awards,
- intentional non-compliance with authorities,
- misuse of funds or assets, and
- unethical behaviour.

Wrongdoing does not include matters that are solely issues of economy, efficiency and effectiveness, nor solely matters of the environment and sustainable development.

What is Fraud?

This audit guidance refers to fraud as one or more intentional acts to deceive for the purpose of obtaining some unjust advantage. This would include serious wrongdoing such as

- breach of trust,
- collusive awarding of grants and contributions,
- collusive bidding or awarding on contracts,
- deceit, and
- dishonest acts,
- false representation,
- fraudulent concealment,
- illegal acts of a similar nature,
- intentional misstatements,
- irregularities,
- kickbacks,
- secret commissions, and
- theft.

Only a court of law can conclusively determine if a fraud has occurred.

See Part 2, section on "Definitions and Characteristics of Wrongdoing and Fraud" on page 28 for further information.

In Canada, as in other countries, wrongdoing and fraud occurs in the business world as well as in government operations. Incidents of wrongdoing and fraud may have serious financial implications or may result in loss of public confidence in government.

Legislative auditors play an important role in detecting wrongdoing and fraud in government operations.

Whether conducting attest audits, special examinations, or performance audits, the auditor has a responsibility to be aware of the indicators of potential wrongdoing and fraud, to take appropriate actions when concerns and suspicions arise, and to report these concerns and suspicions of possible wrongdoing and fraud to the entity principal. The extent of the auditor's responsibility will vary depending on the type of audit undertaken and the reasonableness of detecting the wrongdoing and fraud during that specific audit. Given the hidden nature of wrongdoing and fraud, and the inherent limitations of an audit, the OAG recognizes that some risk remains that wrongdoing and fraud will not be detected.

All auditors should undertake their audits with appropriate professional skepticism and an awareness that wrongdoing and fraud does take place. They should have sufficient knowledge to be able to identify the indicators or red flags of wrongdoing and fraud. The OAG expects its auditors to act with reasonableness and prudence when irregularities, errors, questionable circumstances, or suspicions of possible wrongdoing and fraud come to their attention.

Auditors should

- exercise due diligence in dealing with matters brought to their attention or concerns raised during the audit;
- remain objective when reviewing matters that appear to be wrongdoing and fraud;
- avoid drawing quick conclusions; and
- use caution and discretion when examining any matters that appear to be wrongdoing and fraud.

When auditors suspect wrongdoing or fraud, they should discuss their concerns and suspicions with the entity principal.

The "Office of the Auditor General—Audit Policy on Wrongdoing and Fraud" on page 113 provides more guidance to auditors.

Part 1: Authorities and Mandate

Canadian and International Auditing Standards

Canadian and international accounting and auditing bodies have set auditing standards and guidelines. These standards inform auditors about their responsibility to consider wrongdoing and fraud when they undertake audits. A review of the standards and guidelines issued by different organizations has shown that there are many similarities. The following information gives a general description of each organization's applicable standards and guidelines as they relate to wrongdoing and fraud.

- **Canadian Institute of Chartered Accountants (CICA)—CICA Handbook: Assurance Standards**

  Section 5135: The auditor's responsibility to consider fraud and error, and misstatements arising there from, in an audit of financial statements and other financial information.

- **Institute of Internal Auditors (IIA)—International Standards for the Professional Practice of Internal Auditing**

  Proficiency Standard 1210.A2: Identification of Indicators of Fraud

- **International Federation of Accountants (IFA)—International Auditing and Assurance Standards**

  ISA 240: The Auditor's Responsibility to Consider Fraud in an Audit of Financial Statements

- **International Organization of Supreme Audit Institutions (INTOSAI)—Auditing Standards** - Auditing standards cited, which include references to wrongdoing and fraud.

For more on these standards, see "Additional Information on Canadian and International Auditing Standards" on page 21.

The OAG's Mandate Concerning Wrongdoing and Fraud

The OAG's mandate is to audit government operations and to provide information to Parliament to assist it in holding the government to account for the stewardship of public funds. OAG audits may also identify weaknesses in internal controls, which are reported to entity management and which may prevent wrongdoing and fraud from occurring.

Under the authority of the *Auditor General Act*, the *Financial Administration Act* and other specific legislation, the Auditor General audits about 70 federal government departments; about 40 Crown corporations; 10 departmental corporations; the governments of Nunavut, the Yukon, and the Northwest Territories; some 15 territorial agencies; and about 60 other entities. The Auditor General may also conduct special audits at the request of federal ministers and Parliamentary committees.

For more on OAG authorizing legislation, see "Additional Information on OAG Authorizing Legislation" on page 24.

The OAG audit policy on wrongdoing and fraud has been adopted to ensure that the Office exercises due diligence in its audits to address wrongdoing and fraud, and that it appropriately deals with those issues that are brought to its attention. Whether conducting attest audits, special examinations or performance audits, the policy applies.

OAG Audit Policy on Wrongdoing and Fraud

This policy sets out general expectations for auditors of the Office of the Auditor General. The principles and practices are in addition to any professional auditing and assurance standards to which the OAG adheres. Due to the inherent limitations of an audit, the OAG recognizes that some risk remains that wrongdoing and fraud will not be detected.

General

1) Auditors should carry out their audits with an attitude of professional skepticism, recognizing that wrongdoing and fraud could exist.

2) During all audit stages, auditors should be aware of the indicators and the risks of wrongdoing and fraud within the entities being audited and in areas or subject matters under audit in order to detect wrongdoing and fraud.

3) While conducting an audit, auditors should give proper consideration and take the necessary actions to appropriately deal with identified indicators and risks of wrongdoing and fraud. Auditors should document any facts and observations that confirm or dispel the concerns raised.

4) Auditors have a responsibility to be open and responsive to receiving disclosures or complaints of wrongdoing and fraud from management and employees of the entity and from other persons. The OAG will protect the identity of whistleblowers and complainants (within the limitations of the law) and will handle allegations or suspicions of wrongdoing and fraud with extreme care and confidentiality.

Attest Audits

5) As part of the process of obtaining sufficient knowledge of the entity's business, auditors should review management's assessment of the risk of wrongdoing and fraud, and how management responded to those risks. Auditors should also review how those charged with governance have discharged their oversight role in ensuring the adequacy of systems and practices to manage the risks of wrongdoing and fraud. During this process, auditors should make enquiries of management, the audit committee, and others concerning their knowledge of any actual, suspected, or alleged wrongdoing and fraud.

Reporting

6) Auditors shall report to the entity Principal any suspicions of wrongdoing and fraud including any allegations received. Auditors shall also advise the entity Principal of wrongdoing and fraud that the entity identified but failed to take sufficient and appropriate action. The entity Principal shall take the necessary actions required to appropriately deal with the wrongdoing and fraud issues raised. The entity Principal shall report to the entity's assistant auditor general and the Principal of the Forensic Audit Section when reasonable suspicions cannot be dispelled or where the entity has mishandled an identified instance of wrongdoing and fraud.

7) When auditors identify significant risks of wrongdoing and fraud in the entity's programs and operations, they should be brought to the attention of:

- the entity Principal and the assistant auditor general;
- the Principal of the Forensic Audit Section;
- entity management, and those charged with oversight;
- Parliament, if appropriate.

8) When the OAG has concluded after receiving an opinion from legal services that it has reasonable grounds to believe that significant wrongdoing or fraud has occurred, it shall report those matters to:

- senior officials of the entity;
- the audit committee or equivalent;
- central government agencies and Parliament, when appropriate; and
- the appropriate police authorities, when required.

Auditors' Responsibilities Concerning Wrongdoing and Fraud

Whether conducting attest audits, special examinations, or performance audits, auditors are responsible for

- being aware of the indicators and the risks in order to detect wrongdoing and fraud,
- taking appropriate actions when allegations are received or suspicions arise, and
- reporting suspicions, risks and findings of wrongdoing or fraud.

The extent of the auditor's' responsibility to detect wrongdoing and fraud will vary depending on the type of audit undertaken and the reasonableness of detecting the specific wrongdoing and fraud. Given the hidden nature of wrongdoing and fraud and the inherent limitations of an audit, it is impossible to provide assurance that wrongdoing and fraud will be detected.

When planning audits, auditors should assess the entity's risk factors for wrongdoing and fraud. The OAG has adopted risk-based entity audit planning (One-Pass Planning) as the basis for determining priority audit work. Using One-Pass Planning, entity teams determine entity risk areas, including the risks of wrongdoing and fraud, based on an analysis of:

- external challenges,
- opportunities and risks, and
- internal factors that must be managed well to achieve the entity's objectives.

Checklist 1 Preliminary Risk Assessment of Entity for Possible Wrongdoing and Fraud may be useful for assessing the risks of wrongdoing and fraud and to implement any required modifications to the audit procedures.

The risk factors identified in this checklist are red flags that do not necessarily indicate the existence of wrongdoing or fraud. Auditors should exercise their professional judgment when considering the risk factors identified, either individually or in combination with other factors. Subsequently, they must consider whether specific controls or circumstances such as management and board oversight will mitigate or eliminate that risk.

When auditors identify indicators or red flags of possible wrongdoing and fraud, or they suspect possible wrongdoing or fraud, they should perform additional work to confirm or dispel these concerns. If the concerns cannot be easily dispelled, auditors should advise their Principal immediately. Auditors should also advise the entity Principal when an entity has failed to take sufficient and appropriate action to deal with wrongdoing and fraud. Disclosures and complaints about wrongdoing and fraud that come to the attention of auditors should also be referred to the entity Principal.

The entity Principal is required to take the necessary action to deal with the matters raised. When suspicions cannot be easily dispelled, or the entity has mishandled possible cases of wrongdoing and fraud, the entity Principal shall report the matter to the responsible assistant auditor general and to the Principal of the Forensic Audit Section.

In addition to the responsibilities outlined above, attest auditors have additional responsibilities. For example, attest auditors are responsible for ensuring that deputy ministers, senior management, and senior financial officers (who all sign letters of representation for section 6 audits) understand the representations with respect to fraud.

Also, attest auditors need to identify and evaluate

- matters that increase the risk of a material misstatement in the financial statements resulting from fraud or error (management's influence over the control environment, industry conditions, operating characteristics and financial stability);
- circumstances that increase the susceptibility that the financial statements are materially misstated; and
- evidence obtained including the auditor's knowledge from previous audits about the reliability of management representations.

Attest auditors should refer to the CICA Handbook, Section 5135, "The Auditor's Responsibility to Consider Fraud and Error in an Audit of Financial Statements and Other Financial Information".

Auditors' Conduct

Auditors must conduct their audits with appropriate professional skepticism and with sufficient knowledge to be able to identify the indicators of possible wrongdoing and fraud. Professional skepticism involves being aware of circumstances or evidence that contradicts or questions the reliability of representations made by entity officials or the documentary evidence obtained. An attitude of professional scepticism is necessary throughout the audit process to reduce the risk of overlooking suspicious circumstances, red flags, and of over-generalizing when drawing conclusions. Nevertheless, auditors should remain objective and avoid drawing quick conclusions. Caution and discretion are needed when examining matters that appear to be wrongdoing and fraud. Auditors must act with reasonableness and with prudence when irregularities, errors, and questionable circumstances come to their attention.

Responsibilities of Government Entities Concerning Wrongdoing and Fraud

The *Financial Administration Act* and Treasury Board policies outline the responsibilities of government departments, agencies, and some Crown corporations to prevent, detect, and report fraud or losses due to wrongdoing and illegal activity. Management, including management review groups such as audit committees, is responsible for insuring mechanisms are in place to prevent and detect wrongdoing and fraud. Crown corporation responsibilities vary depending on what bases and conditions under which a Crown corporation was created.

Not all entities are subject to Treasury Board rules. Treasury Board policies generally apply to departments, agencies, and other entities of the Public Service where the Treasury Board is the employer. Some entities may have special authorities set out in enabling legislation that allows applications or rules other than those of the Treasury Board. Auditors should be familiar with the policies relevant to their auditees.

As well, the Privy Council Office has issued a document called *Guidance for Deputy Ministers*, concerning their accountability and responsibilities, *Governing Responsibly: A Guide for Ministers and Ministers of State* and a *Guidebook for Heads of Agencies*, which covers, among other things, standards of conduct. Also, a Conflict of Interest and Post-Employment Code for Public Office Holders was issued by directive. This code applies to ministers, parliamentary secretaries, ministerial exempt staff, and Governor in Council appointees.

Criminal Code Sections Relating to Fraud

Auditors should recognize and report wrongdoing and fraud offences listed under the *Criminal Code of Canada*. Criminal activity relating to fraud falls under the following sections of the *Criminal Code*:

- section 121: Fraud Against the Government;
- section 332: Misappropriation of Money Held Under Direction;
- section 341: Fraudulent Concealment;
- section 361: False Pretences;
- section 380: Fraud;
- section 397: Falsification of Books and Documents;
- section 418: Supplying Defective Stores to Her Majesty;
- section 426: Secret Commissions; and
- section 465: Conspiracy.

See "Appendix 2—Offences under the Criminal Code, Financial Administration Act and Competition Act" on page 121 for a description of each of these Criminal Code sections.

Offence Under the Financial Administration Act

Section 80 of the *Financial Administration Act* (FAA) requires every person who collects, manages, or disburses public money, and who knows about a violation of the Act, associated regulations, or any revenue loss or fraud against the Crown, is to report their findings in writing to a superior officer. Employees who do not report their findings could be found guilty of an indictable offence and are liable upon conviction to a fine not exceeding $5,000 and to imprisonment for a term not exceeding five years.

Relevant Treasury Board Policies

Treasury Board policies that are most relevant to wrongdoing and fraud are

- Values and Ethics Code for the Public Service,
- Policy on Internal Disclosure of Information Concerning Wrongdoing in the Workplace,
- Risk Management Policy;
- Policy on Losses of Money and Offences and Other Illegal Acts Against the Crown.

See "Appendix 4—Weblinks" on page 129.

Values and Ethics Code for the Public Service

A new Values and Ethics Code for the Public Service came into effect in September 2003. It sets out Public Service values and ethics as well as conflict of interest and post-employment measures. This Code is a policy of the Government of Canada. It applies to all public servants in departments, agencies, and other public institutions listed in Part 1, Schedule 1 of the *Public Service Staff Relations Act*. Other public service institutions not covered by the Code are expected to respect its spirit and adopt similar provisions for their organizations. Public servants who do not comply with the Code are subject to disciplinary action including termination of employment.

Public Service values include maintaining political neutrality, making decisions in the public interest, and acting at all times in a manner that will bear the closest public scrutiny.

Conflict of Interest measures are intended to maintain public confidence in the impartiality and objectivity of the Public Service. The measures provide rules of conduct to help minimize the possibility of conflicts between the private interests and the public service duties of public servants. Public servants are required to arrange their private affairs so as to prevent real or perceived conflicts from arising. Public servants are not allowed to accept transfers of economic benefit or to provide preferential treatment to entities or persons.

Post-Employment Measures are intended to minimize the possibility of conflicts of interest between new employment and the most recent responsibilities of federal public servants. Specific measures are set out for those leaving executive positions. For example, for one year after leaving federal employment, former federal public servants in executive positions may not represent or accept employment with entities with which they or their subordinates had significant interaction.

Policy on Internal Disclosure of Information Concerning Wrongdoing in the Workplace

The objective of this policy is to allow employees to bring forward information concerning wrongdoing and to ensure that these employees are treated fairly and protected from reprisal when they are, in good faith, disclosing a wrongdoing. A wrongdoing defined in this policy may be a violation of any law or regulation, misuse of public funds or assets, gross mismanagement, or a substantial and specific danger to the life, health, and safety of Canadians or the environment.

Deputy Heads are responsible for:

- putting in place internal procedures that allow employees to feel confident when disclosing wrongdoings. These procedures must ensure that the disclosures are addressed in an appropriate and timely fashion, and that employees are treated fairly and protected from reprisal;
- designating a senior officer to receive and handle the disclosures. Managers must promote a culture of open communication and protect employees from reprisals.

Employees are expected to follow internal procedures to disclose wrongdoing and to respect the reputations of others.

The Public Service Integrity Office was set up as a result of this policy. The mandate of the Public Service Integrity Officer is to

- assist employees who believe that their issues cannot be disclosed within their own department, or
- assist employees who have disclosed their issues in good faith through the appropriate departmental mechanisms but believe that their disclosure was not appropriately addressed.

Risk Management Policy

The objective of this policy is to safeguard government property and interests, and to safeguard employees' interests when they are conducting government operations. This policy requires entities to identify the potential perils to which they are exposed, assess their risks, and implement cost-effective prevention and control measures. This policy covers all perils which include wrongdoing and fraud, and that threaten government operations and assets.

Entities must investigate incidents, assess the damage, and determine potential legal liability. They must report the loss of assets in the public accounts and to the appropriate law enforcement agencies. As part of a management feedback system, entities must maintain a database for reported incidents. This requirement should enable them to establish improved measures to prevent the reoccurrence of such incidents.

Policy on Losses of Money and Offences and Other Illegal Acts Against the Crown

This policy requires departments and agencies to prevent or minimize losses, and pay special attention to areas of significant risk and exposure such as procurement contracts, grants and contributions, and all major Crown projects. It also covers the reporting of losses due to fraud and other illegal activities.

All losses of money and any allegations of offences and illegal acts must be fully investigated. Losses must be recovered whenever possible. Suspected offences must be reported to the responsible law enforcement agency. Departments and agencies must also:

- implement measures to prevent future occurrences of losses and offences,
- take disciplinary action where circumstances warrant,
- report the losses in the public accounts, and
- appoint a coordinator, who reports to the deputy head or the departmental executive committee and serves as the single point of contact for reporting incidents and coordinating the subsequent action.

Offences involving government employees that do not require an immediate response from a law enforcement authority may be referred to departmental legal services. Legal services can provide an opinion on the seriousness of the incident before further action is taken. Otherwise, all losses of money and suspected cases of fraud or illegal acts must be reported to law enforcement authorities.

Conflict of Interest and Post-Employment Code for Public Office Holders

The Conflict of Interest and Post-Employment Code for public office holders apply to:

- Ministers of the Crown;
- Ministers of State;
- Ministerial exempt staff;
- Governor in Council appointees; and
- Full time ministerial appointees designated as public office holders.

The Code is designed to enhance public confidence in the integrity of public office holders and government decision-making process. It states that public office holders shall arrange their private affairs in a manner that will prevent real, potential, or apparent conflicts of interest.

The code requires every public office holder to conform to a number of principles. Public office holders:

- shall act with honesty and uphold the highest ethical standards so that public confidence and trust in the integrity, objectivity, and impartiality of government are conserved and enhanced;
- have an obligation to perform their official duties and arrange their private affairs in a manner that will bear the closest public scrutiny—an obligation that is not fully discharged by simply acting within the law;
- fulfill their official duties and responsibilities, and make decisions in the public interest and with regard to the merits of each case;
- shall not have private interests, other than those permitted pursuant to the Code, that would be affected particularly or significantly by government actions in which they participate;
- on appointment to office, and thereafter, shall arrange their private affairs in a manner that will prevent real, potential, or apparent conflicts of interest from arising. If such a conflict does arise between the private interests of a public office holder and the official duties and responsibilities of that public office holder, the conflict shall be resolved in favour of the public interest;
- shall not solicit or accept transfers of economic benefit, other than incidental gifts, customary hospitality, or other benefits of nominal value, unless the transfer is pursuant to an enforceable contract or property right of the public office holder;
- shall not step out of their official roles to assist private entities or persons in their dealing with government where this would result in preferential treatment of any person;
- shall not knowingly take advantage of, or benefit from, information that is obtained in the course of their official duties and responsibilities, and that is not generally available to the public; and
- shall not directly or indirectly use or allow the use of government property of any kind, including property leased to the government, for anything other than officially approved activities.

The Role of the OAG Forensic Audit Section

This section includes

- Responsibilities of the Forensic Audit Section
- Forensic Accounting
- General Procedures for the Forensic Audit Section

Responsibilities for the Forensic Audit Section

The responsibilities of this Office's Forensic Audit Section include the following:

- auditing matters of wrongdoing and fraud;
- conducting forensic audits and investigations;
- providing assistance and guidance to entity teams on matters of wrongdoing and fraud;
- developing methodology and providing training to audit staff;
- taking appropriate action to allegations of wrongdoing and fraud received from public servants, the general public, and the business community;
- examining transactions to ensure prudence and probity in the use of public funds or assets;
- reviewing revenues and expenditures such as contracts, and grants and contributions to assess the risk of potential losses or to determine actual losses;
- conducting vulnerability assessments of government programs and activities for susceptibility to wrongdoing and fraud;
- examining the application of government policies and procedures designed to prevent, detect, and report wrongdoing and fraud; and
- reporting to Parliament on matters of significance.

Forensic audits and investigations are undertaken to ensure that the required level of due diligence is observed. The OAG recognizes that the successful conduct of a review of matters concerning suspected wrongdoing and fraud requires special skills and warrants extensive examination or investigations relative to the seriousness of the matter.

The section's workload comes from entity team referrals of matters identified during their audits and from allegations and complaints received from public servants, the public, and the business community. The Forensic Audit Section reports on these matters usually in the form of management letters, audit notes, and special reports. It also refers matters to police authorities.

Forensic Accounting

"Forensic" describes something that is used in or suitable to courts of law or public debate. Forensic accounting is a discipline that deals with the relationship and application of financial facts to legal issues and legal problems. Forensic accounting involves gathering evidence following accepted professional standards and procedures so that forensic accountants can give oral and documentary evidence in court that will be accepted by a court of law and will withstand cross-examination.

Forensic Auditing

Forensic auditing is the terminology used by the Office which describes audits undertaken by the Forensic Audit Section. Forensic auditing comprises investigations, auditing and forensic accounting. It requires combining the three disciplines in conducting the forensic audit. Forensic audits are undertaken with the assumption that the matter may end in civil or criminal proceedings.

General Procedures for the Forensic Audit Section

The Forensic Audit Team determines which cases it will take on, based on the following criteria:

- relevance,
- significance,
- credibility,
- legal implications,
- materiality,
- auditability, and
- necessity of forensic expertise.

Assessing cases against these criteria ensure that the section's resources are directed to the areas of greatest need.

The Forensic Audit Section reviews the examinations and findings of matters referred to its attention. Forensic auditors sometimes accompany entity teams on their audits to examine areas where there are suspicions of wrongdoing and fraud. After an initial assessment of the allegations and the information received, the Forensic auditor determines the appropriate action to be taken. For example, a preliminary review , a forensic audit, or an investigation may be undertaken. The matter may be referred to the entity team or the internal audit or security division of a department, agency, or Crown corporation.

The objectives of a forensic audit and investigation are to

- obtain sufficient evidence to either support or refute the allegations;
- identify any weaknesses in the policies, procedures, and controls that provided an opportunity for the wrongdoing or fraud to occur.
- take appropriate actions on the audit findings, including reporting.

Information about suspected wrongdoing and fraud is strictly controlled to protect the confidentiality and privacy of all persons involved, that is, the informants/ complainants and the persons accused of alleged wrongdoing or fraud. Controlling information also minimizes impediments and safeguards the integrity of the review. The OAG is bound by the *Privacy Act* to protect the identity of informants/complainants.

Additional Information on Canadian and International Auditing Standards

Canadian Institute of Chartered Accountants (CICA)—CICA Handbook: Assurance Standards

Section 5135: Auditor's Responsibility to Consider Fraud and Error in an Audit of Financial Statements and Other Financial Information

The Institute's handbook discusses the auditor's' responsibility to consider fraud. The Institute has revised its standards several times to be consistent with international auditing standards.

The Institute's handbook states that a financial audit is designed to provide reasonable assurance that financial statements as a whole are free from material misstatements whether caused by fraud or error. The Institute standard requires that, when planning and performing audit procedures and evaluating and reporting the results, the auditor should consider the risk of misstatements that are the result of fraud and error) .

In planning an audit, the auditor and other members of the audit team should discuss the susceptibility of the entity's financial statements to material misstatement because of fraud and error. The auditor should ask the entity management to provide its assessment of the risk that its financial statements may be materially misstated as a result of fraud. The entity management should also provide information on and the internal controls it has put in place to address such risk. The auditor should determine whether entity management is aware of any known or suspected fraud that has affected the entity.

When assessing inherent risk and control risk in accordance with materiality and audit risk , the auditor should consider how the financial statements might be materially misstated as a result of fraud or error. If fraud risk factors are identified, auditors should design substantive procedures to perform to reduce the risk to an appropriate low level.

If the audit finds indications that financial statements could contain a material misstatement due to fraud or error, the auditor should perform additional procedures to determine whether a material misstatement does in fact exist. If it does, the auditor should determine whether the possibility of fraud is indicated. If so, the auditor should consider the implications of the misstatement in relation to other aspects of the audit, particularly the reliability of management representations.

The auditor should obtain written representation from management acknowledging that it has disclosed to the auditor all significant facts relating to any fraud or suspected fraud, and that the unadjusted errors accumulated by the auditors are immaterial, both individually and as a whole.

When the auditor identifies a misstatement that leads to a suspicion of fraud, the auditor should consider communicating with management, the audit committee or, in some cases, regulatory and enforcement authorities.

Auditors need to maintain appropriate skepticism and an awareness of the risk of fraud. They should not fail to address any such risk they identify.

The Institute of Internal Auditors (IIA)—Standards for the Professional Practice of Internal Auditing

Section 1210.A2: Identification of Fraud, Responsibility for Fraud Detection

The IIA states that internal auditors should be able to recognize fraud indicators but that they are not expected to be experts in detecting and investigating fraud. Auditors are responsible for helping to deter fraud by examining internal controls for adequacy and effectiveness commensurate with the level of potential exposure to risk in the organization's operations.

Internal auditors who suspect wrongdoing will inform the appropriate authorities in the organization. When fraud is detected, internal auditors will determine the knowledge, qualifications, skills, and other competencies required of internal auditors or specialists to ensure that the necessary level of technical expertise is used to conduct an effective fraud investigation.

Once a fraud investigation has concluded, internal auditors should determine whether controls should be strengthened or new ones introduced to reduce future vulnerability. The auditors should prepare a written report for management that includes all observations, conclusions, recommendations, and any corrective actions taken. The chief audit executive is responsible for immediately reporting cases of significant fraud to senior management and the board of directors.

International Federation of Accountants (IFA)—International Standards on Auditing

ISA 240: The Auditor's Responsibility to Consider Fraud and Error in an Audit of Financial Statements

The IFA audit standard require that the auditor plan and perform an audit with an attitude of professional skepticism, recognizing that circumstances may exist that cause the financial statements to be materially misstated. The standard requires that in planning an audit, the auditor and other members of the audit team should discuss the entity's susceptibility to fraud and error that could cause material misstatements in the financial statements. The auditor should supplement his/her knowledge of the entity's business by asking the entity management for its own assessment of its risk of fraud and the system it has in place to prevent and detect it.

During the assessment process, the auditor should document any identified fraud risk factors and how the entity has responded to them. If the auditor identifies fraud risk factors that indicates that additional audit procedures are required, the auditor should document the presence of the risk factors and the auditor's procedures performed in response to them.

International Organization of Supreme Audit Institutions (INTOSAI)— Auditing Standards

General auditing standards cited, which include references to wrongdoing and fraud

The INTOSAI auditing standards cite the need for auditors to be alert to any situations, control weaknesses, inadequacies in record keeping, errors, and unusual transactions or results that could indicate the presence for fraud, improper or unlawful expenditures, unauthorized operations, waste, inefficiency, or lack of probity. Auditors must be entitled to report breaches of the law to the appropriate authorities.

The auditor should design audit steps and procedures to detect errors, irregularities, and illegal acts. If the procedures yield suspicions of any such occurrences, the auditor should extend his/her procedures to confirm or dispel suspicions.

The auditor should ensure that the techniques he/she employed to gather evidence are sufficient to detect errors and irregularities. Errors, deficiencies, and unusual matters should be properly identified, resolved, documented, and then brought to the attention of senior officers of the Supreme Audit institution'.

Auditors are required to report on:

- the entity's compliance with laws and regulations,
- inadequate systems of control,
- significant perceived or potential irregularities,
- inconsistent application of regulations, and
- illegal acts, fraud, and corrupt practices.

The auditors must decide what action is warranted in the case of fraudulent practices or serious irregularities.

Additional Information on OAG Authorizing Legislation

Auditor General Act—

The Auditor General's duties and responsibilities in auditing departments are set out in the *Auditor General Act*. Numerous sections of the Act (specifically, sections 5, 6, 7, 8, 10, 11, and 12) provide authority to examine and report on instances of wrongdoing and fraud. {link to these sections]

The following descriptions are condensed versions of sections of the *Auditor General Act*.

Section 5 states that the Auditor General shall make such examinations and inquiries as considered necessary to enable the Auditor General to report as required by the Act.

Section 6 states that the Auditor General shall examine the required financial statements and express an opinion on whether they present information fairly and in accordance with the accounting policies of the government.

Section 7 states that the Auditor General shall report to the House of Commons on anything that the Auditor General considers to be of significance and of a nature that should be brought to the attention of the House, including cases where

- accounts have not been faithfully and properly maintained, or public money has not been fully accounted for or paid;
- essential records have not been maintained or the rules and procedures applied have been insufficient:
  - to safeguard and control public property;
  - to secure an effective check on the assessment, collection and proper allocation of the revenue; and
  - to ensure that expenditures have been made only as authorized;
- money has been expended for purposes other than those for which it was appropriated.

Section 8 states that the Auditor General may make a special report on any matter of pressing importance or urgency that should not be deferred until the presentation of his next report.

Section 10 states that whenever it appears to the Auditor General that any public money has been improperly retained by any person, the circumstances of the case must be reported.

Section 11 states that the Auditor General may inquire into and report on any matter relating to the financial affairs of Canada, or to public property, or inquire into and report on any person or organization that has received financial aid from the Government of Canada or in respect of which financial aid is sought.

Section 12 states that the Auditor General may advise appropriate officers and employees in the Public Service of matters discovered in the auditor's examinations.

Financial Administration Act—

The *Financial Administration Act* sets out the mandate of the auditor of Crown corporations and provides for reporting by the auditor.

The Act stipulates that the auditor shall prepare a report that expresses an opinion on the following

- whether the financial statements are presented fairly in accordance with generally accepted accounting principles;
- whether quantitative information is accurate in all material respects;
- whether the transactions of the corporation and its subsidiaries are in accordance with this part of the Act, the regulations, and the charter and by-laws of the corporation or its subsidiary.

The auditor shall call attention to any other matter falling within the scope of his examination that, in his/her opinion, should be brought to the attention of Parliament.

An auditor shall conduct whatever examinations are necessary to enable him/her to prepare a report under this section.

Crown Corporations

Part 10 of the *Financial Administration Act* sets out the accountability framework for Crown corporations. Treasury Board policies may apply to certain Crown corporations. However, at the request of Treasury Board most Crown corporations have agreed to refer cases of wrongdoing and fraud to the Royal Canadian Mounted Police (RCMP). In addition, the Conflict of Interest and Post-Employment Code for Public Office Holders policy applies to full and part-time Governor in Council appointments in Crown corporations.

Part 2: Assessing Risk and Detecting Wrongdoing and Fraud

Introduction

Legislative auditors play an important role in furthering the detection of wrongdoing and fraud in government operations and identifying the risks. This part of the audit guidance helps auditors:

- do risk assessments for wrongdoing and fraud, and
- incorporate wrongdoing and fraud detection techniques into their auditing practices.

The extent of auditors' responsibility to detect wrongdoing and fraud is set out in the OAG policy on wrongdoing and fraud and section 5135 of the CICA Handbook. Whether conducting attest audits, special examinations, or performance audits, the auditor is responsible for detecting wrongdoing and fraud, taking appropriate actions when suspicions arise, and reporting the matter. The extent of the auditor's responsibility will vary depending on the type of audit undertaken and the reasonableness of detecting the specific wrongdoing and fraud during that audit. Given the hidden nature of wrongdoing and fraud and the inherent limitations of an audit, some risk remains that wrongdoing and fraud will not be detected.

All auditors should undertake their audits with appropriate professional skepticism and awareness that wrongdoing and fraud does take place. They should have sufficient knowledge to be able to identify the indicators or red flags of wrongdoing and fraud. The OAG expects its auditors to act with reasonableness and prudence when irregularities, errors, questionable circumstances, or suspicions of possible wrongdoing and fraud come to their attention. Auditors should

- exercise due diligence in dealing with matters brought to their attention or concerns raised during the audit;
- remain objective when reviewing matters that appear to be wrongdoing and fraud.
- avoid drawing quick conclusions; and
- use caution and discretion when examining any matters that appear to be wrongdoing and fraud.

The detection of wrongdoing and fraud is often a matter of mindset rather than methodology. It involves being aware of when, where, and how it is most likely to occur and it involves understanding people and their motives.

Auditors shall report to the entity Principal any suspicions they have of wrongdoing and fraud, including any allegations that they have received. Auditors should refrain from mentioning their suspicions to the auditee until all oral and documentary evidence has been obtained, the facts have been confirmed, and they have spoken to their Principal and the Principal of the Forensic Audit Section.

Checklists 1 and 2 will assist auditors to assess risks and identify red flags.

Definitions and Characteristics of Wrongdoing and Fraud

This section includes

- Wrongdoing (definition)
- Fraud (definition)
- CICA's Definition of Fraud
- Canadian Legal Definition of Fraud
- Legal Definitions of Wrongdoing
- Characteristics of Wrongdoing and Fraud
  - Elements of Fraud
  - Attributes of Fraud
  - Recorded or Unrecorded Frauds
  - Conflict of Interest
- Management Wrongdoing and Fraud Versus Employee Wrongdoing and Fraud

Wrongdoing

This audit guidance refers to wrongdoing as improper conduct or inappropriate activities such as

- abusing or exceeding authority,
- conflicts of interest,
- gross administrative abuse,
- improper contract or contribution awards,
- intentional non-compliance with authorities,
- misuse of funds or assets, and
- unethical behaviour.

Wrongdoing does not include matters that are solely issues of economy, efficiency and effectiveness, nor solely matters of the environment and sustainable development.

Fraud

This audit guidance refers to fraud as one or more intentional acts to deceive for the purpose of obtaining some unjust advantage. This would include serious wrongdoing such as

- breach of trust,
- collusive awarding of grants and contributions,
- collusive bidding or awarding on contracts,
- deceit, and
- dishonest acts,
- false representation,
- fraudulent concealment,
- illegal acts of a similar nature,
- intentional misstatements,
- irregularities,
- kickbacks,
- secret commissions, and
- theft.

Only a court of law can conclusively determine if a fraud has occurred.

Canadian Institute of Chartered Accountants' Definition of Fraud

The Canadian Institute of Chartered Accountants (CICA) Handbook defines fraud as

> An intentional act by one or more individuals among management, other employees, those charged with governance, or third parties, involving the use of deception to obtain an unjust or illegal advantage. Although fraud is a broad legal concept, the auditor is concerned with fraudulent acts that cause a material misstatement in the financial statements. Fraud involving one or more members of management or those charged with governance is referred to as management fraud; fraud involving only employees of the entity is referred to as employee fraud.

Fraudulent financial reporting may involve:

- deception such as manipulation, falsification, or alteration of accounting records or supporting documents from which the financial statements are prepared;
- misrepresentation in, or intentional omissions from, the financial statements of events, transactions, or other significant information; and

- intentional misapplication of accounting principles relating to amount, classification, manner of presentation, or disclosure.

Canadian Legal Definition of Fraud

The essential or central philosophy underlying the offence of fraud is that "commercial affairs are to be conducted honestly." However, over the years some uncertainty developed as to the elements of the offence. Criminal offences are made up of two parts:

- the *actus reus* or criminal act itself, and
- the *mens rea*, the guilty mind or wrongful intention of the accused.

The *Olan* case from the Supreme Court of Canada (1978) set out the content of the *actus reus* of fraud. The offence has two elements:

1) dishonest act—the dishonest act is established by proof of deceit, falsehood or "other fraudulent means" ("other fraudulent means" includes all other dishonest means that are not in the nature of deceit or lies);

2) and deprivation—deprivation is established by proof of detriment, prejudice or risk of prejudice to the economic interests of the victim, caused by the dishonest act.

The elements of the *actus reus* are judged on the objective facts, considering whether a reasonable person would consider the act to be dishonest. Actual economic loss is not required. Therefore, placing an economic interest at risk is sufficient. Also, the person accused of the offence does not have to profit by the fraud.

In *R. v. Théroux* and *R. v. Zlatic.* (1993), the Supreme Court of Canada discussed the elements making up the offence of fraud. The *actus reus* of the offence of fraud will be established by proof of:

1) the prohibited act, be it an act of deceit, a falsehood or some other fraudulent means; and

2) deprivation caused by the prohibited act, which may consist in actual loss or the placing of the victim's pecuniary interests at risk.

The *mens rea* of fraud is established by proof of:

1) subjective knowledge of the prohibited act; and

2) subjective knowledge that the prohibited act could put the property or economic interests of others at risk.

The question to be answered is whether the accused subjectively appreciated or understood that certain consequences would flow from his/her acts. A belief that what he/she was doing was honest is not a defence to a charge of fraud.

Where the required conduct and knowledge are established, the accused person will be found guilty, whether he/she actually intended the prohibited consequence or was reckless as to whether it would occur.

Definitions of Wrongdoing

There is no Canadian legal definition of wrongdoing but in the *Carswell Canadian Law Dictionary* it refers to a wrong as a deprivation of a right, an injury, or the consequence of the violation or infringement of a right. In *Black's Law Dictionary*, a civil wrong is a violation of non-criminal law, such as a tort, a breach of contract or trust, a breach of statutory duty, or a defect in performing a public duty; or the breach of a legal duty treated as the subject matter of a civil proceeding. In the *Gage Canadian Dictionary* a wrongdoing is the doing of wrong, or bad acts.

Characteristics of Wrongdoing and Fraud

The distinguishing factor between wrongdoing and error is whether the action was intentional or unintentional. Intention is often demonstrated by a series of similar incidents. Wrongdoing and fraudulent activities can be comprised of a series of many small events or transactions that, when taken together, would indicate possible wrongdoing and fraud. Therefore, auditors should not dismiss certain transactions as being insignificant.

Elements of Fraud

There are two main elements of fraud: dishonesty and deprivation.

Within the context of fraud, dishonesty includes

- lies, intentional misstatements, intentionally inducing a person to believe that something that is false is true;
- deception including misleading statements, giving false impressions or representations;
- a dishonest trick; and
- covering up falsehoods or actions taken.

Within the context of fraud, deprivation refers to

- loss,
- an act of taking away,
- removing something from its rightful owner, or
- withholding of something.

Even the risk of loss or withholding is deprivation.

Attributes of Fraud

Motivation, rationalization, and opportunity are the attributes that generally underlie the commission of a fraud. The motivations may include financial problems or feelings of anger or revenge. Perpetrators usually find ways to rationalize their behaviour. For example, they may think that everybody is doing it. A breakdown in controls can provide the opportunity for wrongdoing or fraud.

For more on this topic, see "Additional Information on Attributes of Fraud" on page 41.

Recorded or Unrecorded Frauds

Fraudulent activities may be recorded or unrecorded in the books of the entity. A recorded fraud exists where either paper or electronic evidence remains. Examples include documented evidence of phoney vendors and ghost employees. With unrecorded frauds, there is no record whatsoever of the fraudulent transaction within the entity's books. Examples are secret commissions, bribery, and kickbacks. In these examples, the audit trail is poor and the fraud is difficult to detect because it requires documentary evidence outside of the audit entity, such as third party documents or verbal information from persons knowledgeable of the fraudulent transactions.

Conflict of Interest

A conflict of interest with wrongdoing and fraud may co-exist, although one may occur without the other. For example, both a conflict of interest and a wrongdoing or fraud exist where an official in a position to award contracts, fails to disclose his or her interest in a company and subsequently awards a contract to that company. A key element for fraud is the intentional material misrepresentation.

A conflict of interest may be present without a wrongdoing or fraud existing. For example, an employee may disclose to his/her employer a conflict of interest (e.g. a relationship of self-interest between the employee and a company awarded the contract). The employer may permit the employee to remain in the conflict of interest, therefore no wrongdoing or fraud is present.

In certain circumstances a conflict of interest may lead to charges of breach of trust. For example, a person who uses his or her official position to improve or increase the value of his or her private interests would be in a conflict of interest, and the individual could also be charged with breach of trust.

Management Wrongdoing and Fraud Versus Employee Wrongdoing and Fraud

The risk of an auditor not detecting management wrongdoing and fraud is far greater than the risk of not detecting employee wrongdoing and fraud. Auditors generally assume and expect a high level of honesty and integrity from management. However, management is usually in a position to override internal controls. Auditors should not dismiss the possibility that management is involved in a wrongdoing and fraud.

Assessing the Risks of Wrongdoing and Fraud in an Organization

Assessing risks is a fundamental part of audit planning, both at the strategic planning level (determining what audits should be done) at the audit planning level (determining audit steps necessary for particular audits) and during the audit (determining additional audit steps required as a result of determining new risks or higher level of risks). When conducting risk assessments auditors should consider the entity's risks of wrongdoing and fraud. Checklist 1 will assist auditors in evaluating these risks under the following headings:

Governance. Management is in a position to commit major wrongdoing and fraud if the mechanisms for the management oversight are ineffective.

General Environment. The ethical tone of the organization is set at the top. The risks of wrongdoing and fraud are reduced when management demonstrates and communicates the importance of values and ethical behaviour.

Entity's Financial Condition. Pressure to achieve unrealistic financial results can create a motivation for wrongdoing or fraud in financial reporting.

Internal Controls. Inadequate or ineffective internal controls create opportunities for wrongdoing and fraud.

Inadequate Documentation or Unusual Transactions. Poor supporting documentation for transactions makes transactions difficult to audit. Unusual or complex financial transactions should be questioned.

Red Flags That Help Identify Wrongdoing and Fraud

One of the keys to detecting wrongdoing and fraud is the use of red flags to spot unusual events. Red flags are anomalies that point to symptoms or indicators that are known to be associated with wrongdoing and fraud. Knowledge and awareness of these red flags provides auditors with a significant head-start in detection. Auditors should be aware of red flags, know when to use them, and understand their strengths and limitations.

Auditors should remember that a red flag does not always indicate wrongdoing and fraud. While red flags may be present, wrongdoing and fraud may not be. Auditors should undertake further work and seek explanations for any red flags identified. Auditors should avoid making quick conclusions that wrongdoing or fraud exists, and should avoid trying to easily explain the symptoms away.

A red flag list is rarely all inclusive. The presence of one or more red flags should alert auditors to the possibility of wrongdoing and fraud. The ability to spot and assess red flags increases with experience, judgement, and common sense. However, intuition and hunches are also important. Auditors should be familiar with the red flags associated with the subject matter that is under audit. The more red flags there are, the greater the risk that wrongdoing and fraud have occurred.

Auditors should seek straightforward explanations for red flags. They should not assume that the way wrongdoing and fraud has been carried out is necessarily complex and cleverly concealed; start with the simplest explanations first. If the evidence still warrants, tests can be developed and carried out for more complicated scenarios.

Auditors should note that discrepancies indicated by a red flag might not appear significant in themselves, but that an accumulation of small differences is often indicative of a material wrongdoing or fraud. Where concerns cannot easily be dispelled, they should be referred to the Principal and the Principal of the Forensic Audit Section.

Intelligent information gathering becomes crucial. Auditors must make sure that their focus is not biased by assumptions about people or events or by "inside" information provided by interested parties. The auditor must remain independent and objective, and consider all possible interpretations of events.

In many cases, wrongdoing and fraud come to light because of whistleblowers or complainants within the organization who are aware of what is happening. All disclosures or complaints received on inappropriate activities should be taken seriously and reported to the entity principal and the principal of the Forensic Audit Section. The Forensic Audit Section maintains a list of disclosures and complaints received by the OAG concerning improprieties in government operations. Auditors may request a list of disclosures and complaints received on the entity to be audited. They also have access to a Web site with a list of media articles written on the entity being audited and relating to wrongdoing and fraud. This information should assist them in assessing the risk to wrongdoing and fraud in their entities.

Checklists 1 and 2 will assist auditors to identify red flags for wrongdoing and fraud .

Red Flags for Wrongdoing and Fraud in the Governance, Culture and Control Environment which Assist Auditors in the Risk Assessment of the Entity

The following are red flags related to an organization's environment.

- The organization has weak ethics practices.
- Review and oversight by governing bodies are inadequate.
- Senior managers show disregard for regulatory or legislative authorities or government policies.
- Senior managers receive significant bonuses for achieving performance targets.
- The internal audit function is ineffective.
- Management is dominated by one individual or by a small group of senior executives.

- There is a high rate of staff turnover in key positions.
- Complaints or allegations of inappropriate behaviour have been made by employees, customers, suppliers or the public.
- Managers or employees, particularly those in key control functions, never take vacations.
- There are indicators that certain managers or employees have a lavish lifestyle
- Management tries to influence the scope of the audit or to limit the audit team's access to people and information.
- Internal controls are insufficient or ineffective.
- Internal controls are overridden by management.
- Management monitoring of significant controls is inadequate.
- The organizational structure is complex.
- Record keeping is inadequate.
- There are inadequate safeguards for protecting cash, inventory or other assets.
- Procedures for screening job applicants, particularly for key positions, are inadequate.

For detailed descriptions of these red flags, see "Description of Red Flags for Wrongdoing and Fraud in the governance, culture and control environment which will assist the auditor in the risk assessment of the entity" on page 44.

Checklist 1 will assists auditors in identifying red flags in the governance, culture, and control environment of the entity.

Red Flags for Wrongdoing and Fraud in Transactions and Documents

Auditors should follow-up on any inadequate documentation or odd transactions. The following are red flags that may be encountered in the review of transactions and accounts.

- Documentation is missing.
- Information is provided to the auditor unwillingly or following unreasonable delays.
- There is conflicting evidence.
- Transactions are not appropriately approved and authorized.
- There are transactions that do not comply with program.
- There are signs of alterations or discrepancies in supporting documentation.
- There are unusual or complex transactions.

- Transactions are not processed through the normal accounting procedures.
- Transactions are not recorded in a complete or timely manner.
- There are transactions with non-arm's-length parties.
- There are significant unreconciled amounts in accounts.

For detailed descriptions of these red flags, see "Description of Red Flags for Wrongdoing and Fraud in Transactions and Documents" on page 46.

Checklist 2 will assists auditors in identifying red flags in transactions and documents.

Computer and Internet Wrongdoing and Fraud

Computer wrongdoing and frauds involve using a computer to alter electronic records for improper purposes' for example, making unauthorized changes to a computer program to generate fraudulent transactions or to hide wrongdoing or fraudulent activities. The risk of computer wrongdoing and fraud increases each day. The risk of not detecting computer wrongdoing and fraud is very high due to the lack of traditional paper audit trails. Detecting computer wrongdoing and fraud requires a deeper understanding of technology than the average auditor possesses. Information technology specialists may be required to assist in reviewing computer systems and interpreting computer transactions.

Internet wrongdoing and fraud is a type of computer wrongdoing and fraud that involves using Web sites, e-mail, chat rooms or message boards, or other components of the Internet for improper or illegal acts. The Government of Canada is a potential victim because its Web sites provide portals for wrongdoers and fraudsters to enter government computer systems. The government is at high risk because of its size and the large number of persons who can access its services via the Internet.

With the move to e-government or Government Online, new risks arise, as applications for grants and contributions and other funding arrangements can be received over the Internet. New procedures will need to be put in place to authenticate applicants and applications and provide secure information. The transition period to e-government may create opportunities to commit wrongdoing and fraud because government personnel will be unfamiliar with the new processes.

Types of computer wrongdoing and fraud include

- altering or falsifying computer input transactions to conceal problems such as misappropriation of funds or assets;
- implementing computer program changes for personal gain (e.g. an employee manipulating systems to have payments made to himself/ herself);

- stealing computer data and selling it to third parties;
- direct computer file changes by an employee for his/her benefit;
- transferring funds electronically and subsequently destroying the audit trail; and
- inappropriately accessing computer information that can be used to commit an illegal activity (e.g. a person hacks into a government computer server and views confidential information that will be publicly announced shortly which will impact on share values of certain publicly traded companies and uses this confidential information to make gains on the stock market.

Types of Internet wrongdoing and fraud include

- theft of funds through false Government Online applications;
- identity theft or using such stolen identity through the Internet;
- illegal use of government credit card numbers for purchases on the Internet;
- selling on the Internet, products or services that do not exist;
- stealing data via the Internet for personal benefit or selling it to third parties;
- sabotaging computer systems, including planting viruses and worms by hacking into computer systems via the Internet, which affects network downtime and destroys valuable computer information;
- sending endless SPAM to government Web sites;

Red Flags for Computer and Internet Wrongdoing and Fraud

The following are red flags that may indicate a potential for computer or Internet wrongdoing and fraud.

- The information technology security policy is inadequate.
- There is no enforcement of the technology security policy.
- Funding for information security measures is inadequate.
- There is no designated person or group responsible for computer security.
- Security training for system administrators and other technical service personnel is inadequate.
- Security audits are inadequate.
- Security of physical premises is poor.
- Password security policies for computer or Internet access are inadequate.
- Internal system controls are poor.
- Computer and network duties are not appropriately segregated.

- There are no set procedures and controls for making changes to programs.
- Access to computer files and systems exceeds what is needed to perform job duties.
- Access logs are not reviewed.
- Management does not take responsibility for designing and implementing secure systems.
- The organization fails to produce, review, or resolve exception reports.
- Companies only communicate with the government electronically.
- Companies use free e-mail addresses.

For descriptions of these red flags, see "Description of Red Flags for Computer and Internet Wrongdoing and Fraud " on page 48.

Checklist 3 will assist auditors to identify computer and Internet red flags.

Procedures to Follow When Wrongdoing and Fraud are Suspected

This section includes

- Documentary Evidence
- Oral Evidence
- Data Mining

When wrongdoing and fraud are suspected, sufficient evidence should be gathered to support or dismiss the suspicions. The auditor should obtain different types of evidence from various sources to support further examination, or refer the matter to the OAG Forensic Audit Section. When wrongdoing and fraud are suspected, supporting evidence should be discreetly obtained to facilitate future examinations and investigations.

Forensic Audit Section auditors can assist audit teams to obtain evidence to support or dismiss the suspicions of wrongdoing and fraud. Further, the Forensic Audit Section auditors can undertake a forensic audit to determine the facts surrounding the suspected wrongdoing and fraud and to obtain all documentary and oral evidence required to support its findings. Forensic auditors have the expertise to undertake sensitive, detailed interviews and to obtain critical evidence necessary to defend the findings, which may be used in other proceedings.

Documentary Evidence

Documentary evidence refers to all writings, records and instruments which includes anything that is capable of being read by a person, computer system, or other device. Documentary evidence should be properly identified and copies obtained quickly before the evidence disappears. Original documents may disappear once parties suspect inquiries are being made.

When auditors suspect that a wrongdoing or fraud may have occurred, they should identify the relevant documents and make photocopies of these documents discreetly and as soon as possible. On the back of the photocopies, the auditor should put his signature, the current date, the location of where the original document was located, and the name of the departmental official or employee responsible for the original document. It is important the evidence be properly handled as it may be used in examinations and investigations by the Forensic Audit Section, investigative agencies and the police, and it may be subsequently used in administrative and judicial proceedings.

Oral Evidence

Oral evidence is verbal evidence provided by people with knowledge about transactions, events, circumstances, and about other people. Oral evidence may include information about personal participation in certain events and transactions and the reasons for certain actions. Any verbal statements given to the auditors must be recorded at the first opportunity, in writing, either verbatim or as close as possible to the statements made. Auditor's notes should include the time, date, and location where the interview took place, and the names of the participants. Auditors should keep their rough notes that were taken during the interview.

Data Mining

When wrongdoing and fraud is suspected, it is possible that data mining may be very helpful in identifying red flags in large databases. Data mining refers to using special computer software programs to search for red flags or using your own created database program to search the data for indicators of wrongdoing or fraud. Data mining software programs are designed to search large databases and report on identified items (hits) that may suggest irregularities or fraud. Auditors with the assistance of the OAG forensic audit team and OAG IT specialists can also design data mining programs to identify unusual items (hits). Data mining should identify red flags in large databases and between different databases that would probably never be uncovered otherwise. The auditor analyzes the report of hits for determining if there are concerns raised for possible wrongdoing and fraud. If concerns are raised, the auditor may take additional audit steps or advise his/her Principal of the concerns raised.

A sample of data mining searches is provided in "Appendix 3—Data Mining to Detect Wrongdoing and Fraud" on page 127.

Additional Information on Attributes of Fraud

Motivations for Fraud

The most common motivations for fraud are financial need or gain. People who participate in frauds often complain that they had unbearable financial problems for which there was no legitimate relief. Or, they may feel they deserve more recognition than they have received. Jealousy, revenge, anger, or pride may also motivate them to commit fraud. People who commit fraud frequently believe that they are superior to others, are shrewd enough to confound and confuse their colleagues and superiors, and can commit fraud without being discovered or detected. People may also be motivated to commit fraud for a cause or values that they feel are morally superior to those of others or the government.

Rationalizations for Fraud

Perpetrators of criminal fraud often rationalize their actions with non-criminal justification. This sometimes makes it possible for people who are otherwise honest, to commit fraudulent acts.

Examples of employee rationalizations:

- I was only using the money on a temporary basis and I intended to repay it back.
- I am underpaid for what I do and deserve what I have taken.
- Our bosses are doing it, so what's the big deal.
- I only wanted to make the department look good.
- The government is so big that what I took is nothing.

Here are examples of rationalizations by contractors or recipients of funding.

- Others are doing the same thing.
- The minimal value perks I gave to government employees did not influence them.
- Gifts to government employees were only intended to promote the company.
- I am losing money on this contract.
- I lost money on the last contract.
- I am saving the government money.
- I am providing a worthy and needed service to the public.

Organization factors (e.g. management approach or the organization's philosophy), whether actual or perceived, may provide rationalizations for employees to commit fraud. For example:

- senior managers are feared;

- senior managers are perceived as insensitive, insecure, impulsive, or tightfisted;
- there is evidence of significant hostility or jealousy among the management group;
- performance is judged on short-term results;
- management and/or the organization sets unrealistic goals and objectives;
- those charged with governance pay little attention to internal controls;
- there is poor communication within the organization;
- ethics are ambiguous or management does not support the entity's values and ethics and/or subscribes to inappropriate values and ethics;
- loyalty is negatively affected by the way management treats people;
- management shows it does not trust its employees;
- feedback on performance is unnecessarily critical and negative;
- personnel policies are widely ignored and favouritism is practised;
- pressures for peak performance are so great that people burn out or become disgruntled and feel wronged;
- there are high rates of turnover, grievances, absenteeism; and
- there is actual or perceived inequitable treatment among employees.

Opportunity for Fraud

Auditors should be aware that organizational factors can contribute to fraud. An authoritarian organization may cause both managers and employees to break the rules. The risk of fraud increases when there is a general breakdown in internal controls or when managers (in particular, senior managers) are in a position to override internal controls.

The following are examples that provide opportunities for fraud to occur:

- poor internal control;
- lack of segregation of duties;
- staff shortages in review and approval of general expenditures, contracts, and grants and contribution awards;
- a lack of proper monitoring;
- ineffective internal audit practices;
- an ineffective audit committee;
- lack of policies and procedures for controlling assets;
- insufficient security checks on hiring employees;
- high turnover of staff in financial positions;

- employees not knowledgeable of conflict of interest and code of conduct policies;
- a lack of enforcement of a conflict of interest and code of conduct policies; and
- new government programs and activities.

Description of Red Flags for Wrongdoing and Fraud in the governance, culture and control environment which will assist the auditor in the risk assessment of the entity

- **The organization has weak ethics practices.** Senior management sets a poor example for employees to emulate. The organization does not have a code of ethics or has not communicated its code of ethics to employees.
- **Review and oversight by governing bodies are inadequate.** Senior managers are not held accountable for the exercise of their responsibilities. There is ineffective oversight of management by those charged with governance (e.g. the board of directors or the audit committee). For example, members of the oversight body lack the necessary training and experience.
- **Senior managers show disregard for regulatory or legislative authorities or government policies.** For example, management is reluctant to communicate openly with appropriate third parties such as central agencies, regulators or Members of Parliament. Or, management focuses on "getting the cheques out the door", rather than ensuring that only eligible recipients are paid.
- **Senior managers receive significant bonuses for achieving performance targets.** Managers may be motivated to misstate financial or operating results in order to achieve performance targets linked to their compensation.
- **The internal audit function is ineffective.** The internal audit function is understaffed or lacks qualified and experienced auditors. Or, management fails to take action on control weaknesses identified by internal audit.
- **Management is dominated by one individual or by a small group of senior executives.** Employees feel intimidated by senior management. Employees are told by managers to override internal controls. Employees are reprimanded for questioning the actions of senior managers and rewarded for complying with executive's requests.
- **There is a high rate of staff turnover in key positions.** Employees may leave key positions if they feel unhappy with the ethical tone of the organizations and do not want to compromise their professional ethics. Or, employees may be asked to leave because they are not willing to comply with management's requests to override controls.
- **Complaints or allegations of inappropriate activities have been made by employees, customers, suppliers or the public.** Complaints or allegations received are an indication of problems in an organization; likewise, a lack of complaints or allegations may indicate a climate of intimidation in the organization.

- **Managers or employees never take vacations.** Employees or managers, particularly those in key control functions, do not take their regular vacation leave to ensure that they can continue to cover up irregularities or because they do not want their replacement staff to discover the irregularities. Taking a vacation would give someone else access to systems and records, increasing the risk of detection.
- **There are indicators that certain managers or employees have a lavish lifestyle.** Managers or employees have purchased expensive items which, given their salary, they do not seem to be able to afford.
- **Management tries to influence the scope of the audit or to limit the audit team's access to people and information.** Management does not respect the role of the Office of the Auditor General to conduct audits and report findings. Management suggests that the timing of the audit is inappropriate because of changes underway in the area subject to the audit.
- **Internal controls are insufficient or ineffective.** For example, there is poor segregation of duties, few independent checks of transactions, inadequate controls on computer systems or weaknesses in procedures for authorizing transactions.
- **Internal controls are overridden by management.** When management frequently overrides key internal controls or does not enforce the controls, this may suggest a pattern that indicates possible wrongdoing and fraud.
- **Management monitoring of significant controls is inadequate.** The reports prepared for senior management do not contain sufficient and appropriate information to monitor the effectiveness of control systems and practices. For example, the audit team identifies important issues that senior management was not aware of.
- **The organizational structure is complex.** There are many lines of managerial authority so that it is difficult to determine responsibilities. Or, there are unusual affiliated organizations whose business purposes are unclear. A complex structure may make it easier for a corrupt senior manager to conceal wrongdoing because it makes it difficult to understand what is really happening in the organization.
- **Record keeping is inadequate.** Poor record keeping makes it difficult for auditors to locate documents necessary to reconstruct how transactions were justified and processed. In some cases, it may be more than poor administration; destroying the audit trail may be intentional.
- **There are inadequate safeguards for protecting cash, inventory or other assets.** There is a high risk of theft if assets that can be removed from the organization are not properly secured. Poor internal controls in areas that handle or manage assets can provide opportunities for many kinds of wrongdoing.

- **Procedures for screening job applicants, particularly for key positions, are inadequate.** There are no background checks done to verify the qualifications and experience of applicants for responsible positions. As a result, dishonest individuals may be hired.

Description of Red Flags for Wrongdoing and Fraud in Transactions and Documents

- **Documentation is missing.** Files do not contain key documents. For example, a contribution agreement file does not contain the recipient's application for funding. Or, payment files do not contain evidence that the conditions for the payment have been met.
- **Information is provided to the auditor unwillingly or following unreasonable delays.** Failure to respond to information requests in a timely manner raises suspicions about the integrity of the transaction. Delays could enable the perpetrators to create fictitious documentation to support the requested transactions.
- **There is conflicting evidence.** When supporting documentation conflicts with management or employees' responses to inquiries, the transaction should be considered suspicious.
- **Transactions are not appropriately approved and authorized.** Exceptions are made to the standard approval process. Transactions are missing required approvals or are signed by someone who does not have authority to approve. Payments are made with missing or unauthorized signatures for approvals required under Sections 33 and 34 of the Financial Administration Act. Or, there is evidence that supervisors do not properly review documents before approving them.
- **There are transactions that do not comply with program authorities.** The entity does not comply with statutory regulations or Treasury Board policies. All government expenditures must be authorized by Parliament, either through specific legislation or through appropriation acts. Many government activities also require Treasury Board approval of the terms and conditions under which the program will operate.
- **There are signs of alterations or discrepancies in supporting documentation.** Original documents cannot be located. Only photocopies are available. There is evidence of revisions to documents. Documents are incomplete or the dates on documents do not make sense.
- **There are unusual or complex transactions.** There are transactions that are unusual in terms of their nature, size or complexity, particularly close to the financial yearend. This could indicate efforts to cover up improper transactions so that the financial statements will not raise suspicions.
- **Transactions are not processed through the normal accounting procedures.** Auditors should determine why transactions were processed differently, particularly is there is a pattern of irregularities.
- **Transactions are not recorded in a complete or timely manner.** Transactions that are not completed in a timely manner or are improperly recorded as to classification or accounting period, may indicate irregularities.

- **There are transactions with non-arm's-length parties.** There are indications that payments have been made to organizations or individuals with ties to a government employee. For example, a grant is given to a company owned by the spouse of an employee in the granting department. Or, there are invoices that use post office boxes as addresses or are missing other information to identify the company.
- **There are significant unreconciled amounts in accounts.** There are differences between control accounts and subsidiary accounts. There are significant differences between the physical inventory count and the perpetual inventory account. There are unreconciled amounts in suspense accounts. All significant differences should be investigated.

Description of Red Flags for Computer and Internet Wrongdoing and Fraud

- **The information technology security policy is inadequate.** A typical security policy should include system access controls, system backup and monitoring procedures, intrusion detection, intrusion and incident response procedures, and periodic security audits.
- **There is no enforcement of the security policy. If the security policy is not enforced, employees will realize the opportunity to take advantage of the system and with the right motivation will take advantage of the situation.**
- **Funding for information security measures is inadequate.** Information security is critical for all organizations and should be protected by appropriate resources.
- **There is no designated person or group responsible for computer security.** Organizations should appoint an in-house person who is responsible and accountable for computer and Internet security.
- **Security training for systems administrators and other technical service personnel is inadequate.** Periodic training and reminders of the policies are needed as well as security sensitivity training. Internal experts may be reluctant to admit that they lack the required expertise or knowledge to give the training.
- **Security audits are inadequate.** Security audits should be performed to identify systems at risk and to assess opportunities for systems misuse.
- **Security of physical premises is poor.** Organizations should avoid providing unlimited physical access to computers. It should ensure that users log off when they leave a computer unattended or that automatic processes are in place to log out computers after a set period of inactivity.
- **Password security policies for computer or Internet access are inadequate.** Policies for the appropriate access privileges, through the use of passwords, should be clear and applicable to all employees. Access should be monitored and passwords changed on a regular, scheduled basis and access removed as soon as an employee leaves.
- **Internal system controls are poor.** For those who are aware and understand the weaknesses in the computer systems, poor internal system controls can provide countless opportunities to commit fraud. Auditors finding significant numbers of red flags that indicate system controls are inadequate should be aware that the risk of fraud may be high.
- **Duties are not appropriately segregated.** There are many issues around segregation of duties when operating computer systems. For example, to minimize the risk of abuse system programming must be separate from computer operations . Otherwise, one person who might be in a position to input data could also take advantage by making improper programming changes.

- **There are no set procedures and controls for making changes to existing programs.** Procedures should be in place to prevent unauthorized changes to programming.
- **Access to computer files and systems exceeds what is needed to perform job duties.** Unlimited access to an organization's computer system can provide opportunities for people to tamper with a range of computer programs or files. Processes need to be in place to change access rights when employees change positions orleave.
- **Access logs are not reviewed.** Employees who have accessed the computer system at unusual times, too frequently, or who have accessed areas that are not related to their job duties could be identified through access log reviews or trail log audits. Not all systems have the capacity to do comprehensive access log reports. Therefore, auditors must look at other methods for reviewing access.
- **Management does not take responsibility for designing and implementing secure systems.** Management must be involved in the development and implementation of new systems to ensure appropriate controls are in place, tested, and are functioning properly.
- **The organization fails to produce, review, or resolve exception reports.** Exception reports identify issues and irregularities that should be resolved by supervisors. Exceptions should be reviewed or followed-up by an appropriate individual in the organization. If not followed-up, these exceptions could lead to inappropriate use of computers.
- **Companies only communicate with the government electronically.** Exclusive electronic communication may indicate that the company does not have a physical presence or that it may be fictitious. The organization should verify the existence of the company by sending correspondence by mail. A red flag should be raised if the company does not respond to mailed correspondence or the correspondence is returned undelivered.
- **Companies use free e-mail addresses.** Free, Web-based, e-mail addresses provided by an Internet Service Provider such as @hotmail.com, @juno.com, @usa.net, and @yahoo.com cannot be easily traced back to the real owner. Fictitious companies may use these free e-mail addresses to hide their true identity when requesting funding from the government.

Part 3: Wrongdoing and Fraud in Contracting

Introduction

This part provides guidance to auditors to help them:

- assess the risks of wrongdoing and fraud related to contracting;
- recognize the red flags or indicators of contract wrongdoing and fraud; and
- identify potential wrongdoing and fraud.

This part should be read in conjunction with the Introduction, Part 1, and Part 2.

When conducting audits, the auditor should maintain an awareness of the possibility of wrongdoing and fraud in contracting practices. The auditor should be knowledgeable of the common types of contract wrongdoing and fraud and should also be aware of the red flags that may indicate possible contract wrongdoing and fraud.

Checklist 4 summarizes red flags for screening contracts.

How Contract Wrongdoing and Fraud May Occur

The following are common methods of perpetrating contract wrongdoing and fraud.

- bribery and kickbacks
- change order abuse
- collusive bidding, price fixing, or bid-rigging
- co-mingling of contracts
- conflict of interest
- defective pricing
- duplicate invoices
- false invoices
- false quality and performance representations
- information disclosure
- local purchase order abuse or split purchases
- phantom contractor
- product substitution

- progress payment abuse (front-end loading or advance payment)
- purchases for personal use
- short bidding time limits
- tailored specifications
- unnecessary purchases

For descriptions, see "Description of How Contract Wrongdoing and Fraud May Occur" on page 61.

Screening Government Contracts

The process of screening contracts involves examining for different things in each of the following three contracting stages:

- Stage 1—contract requirements definition;
- Stage 2—contract acquisition, bidding, and contractor selection; and
- Stage 3—contract administration, performance and evaluation.

One of the keys to identifying wrongdoing and fraud is the ability to spot anomalies. These irregularities should be considered red flags. Cases of wrongdoing and fraud usually exhibit such red flags. Knowledge of these red flags provides auditors with a significant head-start in recognizing potential wrongdoing. Auditors should be aware of red flags, know when to use them, and understand their strengths and limitations.

The section includes

- Reviewing Contracting Documents
- Stage 1—Contract Requirements Definition
  - Red Flags for Contract Requirements Definition
- Stage 2—Contract Acquisition, Bidding, and Selection
  - Red Flags for Contract Acquisition, Bidding, and Selection
  - Anti-Competition Activities in the Bidding Process
    - Red Flags That May Indicate Anti-Competition Activity
  - Wrongdoing and Fraud In Non-Competitive Contracts
    - Red Flags for Non-Competitive Contracts
- Stage 3—Contract Administration, Performance, and Evaluation
  - Red Flags for Contract Administration, Performance, and Evaluation
- Checklist 4 summarizes red flags for screening contracts.

Reviewing Contracting Documents

When screening contracts for wrongdoing and fraud, the auditors should review the following documents, which are usually associated with contracts:

- plans and reports defining requirements and needs,
- work specifications,
- records of conversations between the tendering agency and bidders,
- requests for proposals or other bid solicitation records,
- copies of the tenders,
- copies of the assessments of tenders,
- contract acceptance records,
- the approved contract,
- progress reports,
- receipts and invoices,
- payment schedules and records,
- contract amendments and change orders,
- quality assurance and contractor performance reports, and
- all approval sign-offs required by the *Financial Administration Act.*

Stage 1—Contract Requirements Definition

This stage involves assessing an entity's requirements and justifications for purchasing certain goods and services. Wrongdoing and fraud schemes usually involve misusing administrative discretion by defining contract requirements so that the contract can be directed to a specific contractor. Inadequate needs analysis is usually an indication of administrative deficiency, but in certain cases it is also an indicator of wrongdoing and fraud.

Red Flags for Contract Requirements Definition

- Technical experts are not consulted in drawing up specifications for technical purchases or contracts.
- There is unusual involvement of a senior official.
- There is an inadequate review to determine if goods, services or information to be purchased are already owned.
- The needs analysis is rushed.
- Excessive stock is acquired.

- Information on potential sources of materials is provided to only one bidder.
- The replacement period for goods has been shortened.
- Surplus materiel in good operating condition is being replaced.
- The requirements specifications are narrow.
- A consultant who helped develop contract needs specifications is permitted to bid.
- The needs analysis is product oriented rather than performance oriented.

For descriptions of these red flags, see "Description of Red Flags for Contract Requirements Definition" on page 63.

Checklist 4, Part 1 summarizes red flags for screening stage 1 of the contracting process – requirements definition.

Stage 2—Contract Acquisition, Bidding, and Selection

This stage involves the process of inviting or not inviting bids on prospective contracts. *Government Contract Regulations* set out the conditions under which contracts can be awarded without a competitive process. Further, the selection process can vary substantially depending on the complexity of the contract. Wrongdoing and fraud at this stage may involve collusion between a government employee and a contractor or collusion between contractors bidding on the contracts.

This section includes

- Red Flags for Contract Acquisition, Bidding, and Selection Processes
- Anti-Competition Activities In the Bidding Process
  - Red Flags That May Indicate Anti-Competition Activity
- Wrongdoing and Fraud In Non-Competitive Contracts
  - Red Flags for Non-Competitive Contracts

Red Flags for Contract Acquisition, Bidding, and Selection

- Bid specifications are unclear.
- There is unusual involvement by a senior official.
- The relationship between the contractor and government officials responsible for selecting the contractor is questionable.
- Confidential information is released.
- There are unusual bidding patterns.
- Few bids are submitted.

- Evaluation of contractors is inconsistent in relation to their previous performances.
- The review of bids is rushed.
- Bids are evaluated by one person instead of a panel.
- The contractor gave benefits to government officials.
- Several contracts for the same goods or services are issued sequentially.
- Exceptions are made to the tender deadline.
- Bids are changed after they are submitted.
- Changes are made to the contract specifications after the contract is awarded but before it is signed.
- The request for proposal contains a mistake that invalidates the call for tenders or request for proposal.
- The lowest bidder is not selected.

For descriptions of these red flags, see "Description of Red Flags for Contract Acquisition, Bidding, and Selection" on page 65.

Checklist 4, Part 2 summarizes red flags for screening stage 2 of the contracting process – acquisition, bidding and selection.

Anti-Competition Activities in the Bidding Process

In a competitive process, bid specifications are prepared to provide potential bidders and government selection officials with a common basis for preparing and accepting bids. These specifications provide

- specific criteria about the eligibility of contractors,
- a description of the work to be performed or the type of goods to be delivered, and
- a complete guide about how bids are to be prepared and submitted.

Wrongdoing and fraud in the bidding process may involve collusion among contractors including such anti-competition activities as bid-rigging and price-fixing. The collusion involves informal arrangements or agreements intended to limit competition.

Collusion between bidders is more likely when certain market characteristics exist such as industries where products or services are homogeneous, where there are few sellers, or where competition is based primarily on price. The following are examples of the types of businesses susceptible to anti-competition activities:

- dredging;
- building construction;

- asphalt paving;
- roofing;
- household goods shipping;
- waste disposal; and
- suppliers of electrical equipment, lumber, and fuel.

Examples of common anti-competitive activities include

- **Bid suppression**—one or more contractors agree to refrain from bidding on a contract, or to withdraw a previously submitted bid so that another contractor's bid will be accepted.
- **Complementary bidding**—contractors submit token bids that are too high to be accepted, or that include terms that are unacceptable. Such bids are submitted to give the appearance of competitive bidding.
- **Bid rotation**—contractors take turns submitting the low bid. These bids may follow a cyclical pattern, or may be related to the size of the contract.
- **Market division**—a group of contractors agree to split a particular market and limit competition. Markets may be divided according to government entities, customers, or geographic areas. As a result, contractors will bid only in their designated market and will either not bid or submit only complementary bids when bidding in a market not assigned to them.

Red Flags That May Indicate Anti-Competition Activity

- An analysis of bidders and contract awards indicates patterns.
- Competition is restricted.
- Bids refer to industry-wide pricing practices.
- Correspondence with contractors suggests possible collusion.
- There are unusual withdrawals of tenders.
- Bid details are peculiar or different bids display similarities.
- The successful contractor uses competitors as subcontractors.
- Bids are higher than expected.
- Related companies submit individual bids.
- There are few bidders and only one qualified contractor, because dummy bids are submitted.
- Bids include labour costs that are too high or too low.

For descriptions of these red flags, see "Description of Red Flags That May Indicate Anti-Competition Activity" on page 68.

Checklist 4, Part 2.1 summarizes red flags that may indicate anti-competition activity.

Wrongdoing and Fraud in Non-Competitive Contracts

Government Contract Regulations are based on the belief that competitively awarded contracts will provide the best quality and price. There can be a conflict between competitiveness and efficient, economical acquisition. Therefore, the *Regulations* set out limited conditions under which contracts can be awarded on a sole-source basis without a formal bidding process.

Other mechanisms to reduce the time and effort required to make acquisitions include standing orders and local purchase orders. Standing offers are agreements with suppliers to provide goods and services on demand according to a set of terms and conditions; a contract is struck when a department makes a "call-up" against an offer. Local purchase orders give government departments the authority to purchase goods and services, up to certain dollar values, directly from suppliers rather than using the procurement services of Public Works and Government Services Canada.

These mechanisms are subject to abuse, such as

- bribery and kickbacks,
- conflict of interest,
- local purchase order abuses,
- purchases for personal use, and
- unnecessary purchases.

Red Flags for Non-Competitive Contracts

- A contract is changed from competitive to sole-source.
- The documentation used to justify sole-source contracting is inadequate.
- Contracts are repeatedly awarded to the same contractor.
- Several small contracts are issued sequentially to the same supplier.
- Use of standing offers is unusual.
- Local purchase orders (LPOs) are valued beyond approved dollar limits.

For descriptions of these red flags, see "Description of Red Flags for Non-Competitive Contracts" on page 70.

Checklist 4, Part 2.2 summarizes red flags for screening sole-source contracts.

Stage 3—Contract Administration, Performance, and Evaluation

This stage refers to how contracts are administered and managed to ensure the fulfillment of the contract. The types of wrongdoing and fraud committed in this stage are generally related to the pricing method of the contract. Three common pricing methods are fixed-cost, cost-plus, and cost-per contract.

This section includes

- Fixed-Cost Contracts
  - Red Flags for Fixed-Cost Contracts
- Costs-Plus and Cost-Per Contracts
  - Red Flags for Costs-Plus and Cost-Per Contracts

Fixed-Cost Contracts

Fixed-cost contracts are contracts where the total price payable is set and the contractor must fulfil the contract at the agreed upon price. Wrongdoing and fraud generally involve the contractor trying to deviate from the fixed price of the contract. Fixed-cost contracts are particularly vulnerable to

- change order abuse,
- duplicate payments,
- false representations, and
- product substitution.

Red Flags for Fixed-Cost Contracts

- Changes are made to a contract after it is awarded, resulting in substantially increased charges.
- Change orders are issued without adequate explanation or as a result of circumstances that should have been foreseen.
- A contract is unexpectedly extended.
- A contract has significant cost over-runs.
- Contractor invoices are not reviewed.
- Test certification documentation is inadequate or missing.
- Contractor performance is not verified.
- Inspection reports are inadequate or missing.
- Complaints or disclosures are received about the inferior quality of the goods and services provided.
- Certification under section 34 of the *Financial Administration Act* is missing.

For descriptions of these red flags, see "Description of Red Flags for Fixed-Cost Contracts" on page 71.

Checklist 4, Part 3.1 summarizes red flags for screening fixed-price contracts.

Cost-Plus and Cost-Per Contracts

Cost-plus-a-fee pricing may be necessary where defining requirements is difficult. Cost-per contracts are priced per unit of labour, materials or other measureable unit. Wrongdoing and fraud generally involve situations in which contractors take advantage of the price variable nature of the contract. For example, contractors may

- charge the government for costs that are not allowed in the contract,
- charge the government for costs that are unreasonable, or
- charge the government for costs that cannot be directly or indirectly allocated to the contract.

These types of wrongdoing and fraud are done by concealing or misrepresenting costs as allowable costs, or hiding them in certain accounts that are not closely audited.

The types of wrongdoing and fraud that are most likely to occur in cost-plus and cost-per contracts include

- defective pricing,
- false invoicing,
- front-end loading,
- phantom contracting, and
- unwarranted progress payments.

Red Flags for Cost-Plus and Cost-Per Contracts

- There are inadequate inspections of each phase of the contract..
- Rates charged are higher than those stipulated in the contract.
- Photocopies are submitted to support charges.
- There is evidence of double billing.
- Invoices provide inadequate information to identify the contractor.
- Invoices are questionable.
- Invoices are not certified as paid.
- The contractor's employees or subcontractors do not have the required skills.
- Labour costs appear high.

- Charges for overtime seem unreasonable.
- Quality assurance is weak or does not exist.
- Incomplete cheques are submitted as proof of payment.
- The timing of progress payments does not coincide with plans.
- Claims are made for materials that are not purchased.

For descriptions of these red flags, see "Description of Red Flags for Cost-Plus and Cost-Per Contracts" on page 72.

Checklist 4, Part 3.2 summarizes red flags for screening cost-plus and cost-per contracts.

Description of How Contract Wrongdoing and Fraud May Occur

The following are common methods of perpetrating contract wrongdoing and fraud.

- **Bribery and kickbacks**—a contractor gives a government employee money, gifts, or other favours in order to obtain business or favourable treatment.
- **Change order abuse**—changes are made to the original contract conditions, resulting in a need for more funds than were provided in the original contract. Change orders may be issued throughout the life of the contract to compensate a contractor who initially submitted a low bid. For example, the contractor may be requested to do additional phases of the project that were not part of the original contract.
- **Collusive bidding, price fixing, or bid-rigging**—a group of prospective contractors may make an arrangement to eliminate or limit competition. For example, they may agree that one of them will bid lower than the other contractors. Part IV of the Competition Act, which identifies several offences, including conspiracy to limit competition and bid-rigging, may apply in these situations.
- **Co-mingling of contracts**—a contractor bills for the same work under more than one contract. For example, a one-time demolition service may be billed more than once under separate contracts (e.g. the demolition fee could be invoiced four times under separate contracts for the construction of foundations, walls, ceilings and floors).
- **Conflict of interest**—contracts are awarded to organizations that employ government employees or their families, or to companies in which government employees or their families have an undisclosed financial interest. For example, printing contracts are awarded to the brother-in-law of a government employee.
- **Defective pricing**—a contractor submits inflated invoices that do not comply with the costs/prices specified in the contract.
- **Duplicate invoices**—a contractor submits separately two copies of the same invoice and is subsequently paid twice.
- **False invoices**—a contractor submits invoices for goods that have not been delivered, or the invoice does not reflect the contract terms. For example, the contract sets out a fixed-price but the contractor invoices at a cost-plus.
- **False quality and performance representations**—a contractor makes false representations about the quality of the products to be supplied or qualifications to perform the requested services.
- **Information disclosure**—a government employee releases unauthorized information to a contractor to assist that contractor to win the contract.

- **Local purchase order abuse or split purchases**—the total cost of purchasing goods and services exceeds the local authority limit, or a competitive process is required to provide such goods or services. To bypass these rules, the purchases are split into two or more segments.
- **Phantom contractor**— a contractor submits an invoice from a non-existent company to support fictitious costs contained in a government cost-plus contract.
- **Product substitution**—a contractor fails to deliver the goods or services as specified in the contract. The contractor may substitute an inferior product without informing the government. Typical examples include delivering products manufactured by foreign suppliers when the products are supposed to be produced in Canada, or when tests are not conducted to ensure product quality, as required by the contract.
- **Progress payment abuse: front-end loading or advance payment**—under government contracts, payments are made as work progresses. The payments are based on the costs incurred, the percentage of work completed, or the completion of particular stages of work. Progress payment fraud normally includes falsified certification of the work completed in order to receive payments prior to the work being done. The contractor may inflate the costs of the initial work so that, when the percentage of completion billing method is applied, the contractor would receive higher cash flows relative to the actual work completed. The cost of subsequent contract work would be understated with the anticipation that change orders would be approved for additional compensation.
- **Purchases for personal use**— a government official purchases items for personal use, or makes excess purchases of which some items are diverted for personal use. For example, a government employee, who operates a family advertising business, purchases materials via the government to be subsequently used in a personal advertising business.
- **Short bidding time limits**—the lead-time for responding to a proposal is unusually short so that only bidders with inside knowledge will be able to prepare a proposal on time. There is no compelling reason to justify a markedly reduced response time.
- **Tailored specifications**—a government official establishes unnecessary or highly restrictive product specifications that only one contractor can meet. For example, a contract may specify a type of equipment that only one contractor can provide.
- **Unnecessary purchases**—goods or services that have been previously purchased are purchased again when there is no additional need.

Description of Red Flags for Contract Requirements Definition

- **Technical experts were not consulted in drawing up specifications for technical contracts or purchases.** Needs must be specified in a way that will facilitate the assessment of alternatives. Without adequate technical advice, bid specifications will be unclear, giving more discretion to contracting authorities.
- **There is unusual senior management involvement.** A senior official, who is not usually involved in the contract process, takes a hands-on approach to preparing the needs analysis.
- **There is an inadequate review to determine if goods services or information to be purchased are already owned**. For contracts involving the purchase of proprietary information, trade secrets, or other technical information, there is no indication that attempts were made to determine whether the government already owns that information. For contracts involving the purchase of goods or services, the contracting unit failed to determine if the requisitioned goods or services had already been purchased.
- **The needs analysis is rushed.** The time allocated to conduct the requirements definition stage is minimal when compared with the estimated costs and technical complexity of obtaining the goods or services. Rushed timing may indicate that someone is trying to find a way around the normal contracting process.
- **Excessive stock is acquired**. There is inadequate information on usage patterns or the inventory available substantially exceeds projected usage needs. Large amounts of the same materials are routinely acquired from the same contractors.
- **Information on potential sources of materials is provided to only one bidder**. This may indicate that the needs analysis was prepared with the intention of directing the contract to a specific bidder.
- **The replacement period for goods has been shortened**. Goods are replaced in a much shorter time frame than indicated in manufacturer or entity standards.
- **Surplus materiel in good operating condition is being replaced.** Goods in operating order are declared surplus but are subsequently replaced.
- **The requirements specifications are narrow.** The requirements specifications are precise, rather than generic, without reasonable justification. This reduces or eliminates potential competition.
- **A consultant who helped develop contract needs specifications is permitted to bid**. Statements of work or specifications are developed by, or in consultation with, a contractor who can tailor the requirements to fit his specific product or unique capabilities.

- **The needs analysis is product oriented rather than performance oriented.** Needs assessments describe the product to be acquired rather than justifying the performance needs and specifications. The contract defines a solution rather than a need, and material has already been selected.

Description of Red Flags for Contract Acquisition, Bidding, and Selection

- **Bid specifications are unclear.** When bid specifications are vague, government officials may exercise considerable discretion in selecting a contractor. Unclear bid specifications also enable the contractor to try to recoup losses that would not otherwise be compensated, by falsely classifying the losses as increased costs due to inadequate specifications.
- **There is unusual involvement by a senior official.** Senior government officials take an unusual interest in whether or not a particular contractor is awarded a contract. For example, they may request specific details about the contract, or take a hands-on approach during the bidding and selection stage.
- **The relationship between the contractor and government officials responsible for selecting the contractor is questionable.** Here are some examples
  - A government employee has close professional or personal ties with the company or its officials. These ties influence the selection of the contractor.
  - A government official who selected the contractor joins the contractor's company shortly after the contract was awarded.
  - A consulting agency or its employees, engaged to help develop contract requirements, accepts employment with a potential bidder and discusses the requirements definition that they helped develop.
- **Confidential information is released.** Confidential contract information is released in advance, or released selectively, to certain contractors. Or, consultants or companies hired by the government release information to competing contractors prior to the tendering process.
- **There are unusual bidding patterns.** A review of potential contractors may indicate that:
  - certain contractors always bid against each other or, certain contractors never bid against each other;
  - bid prices drop when a new or infrequent bidder submits a bid;
  - a contractor bids substantially higher on certain contracts, although no obvious cost difference can account for the variance;
  - certain qualified contractors never or infrequently bid on federal government contracts;
  - a bid is accepted from a contractor who lacks the necessary skills and experience set out in the bid specifications;
  - a contractor with a history of poor performance is awarded a contract;
  - certain contractors are consistently successful in a particular territory; or

  - the same contractor is always the successful bidder when contracting with a particular entity, yet usually is not successful with other agencies.

- **Few bids are submitted.** Few bidders show an interest in a contract. This may indicate that specifications were written so that only certain contractors could compete.
- **Evaluation of contractors is inconsistent in relation to their previous performances.** Contractor capabilities were overrated or underrated when compared to deficiencies reported in previous contract performance evaluations.
- **The review of bids is rushed.** The call for tenders had an unusually short closing date without a reasonable explanation. This may indicate that certain officials exercised discretion to limit the time allowed for contractors to prepare and submit proposals. Only those who may have received advance information have enough time to prepare their bids or proposals.
- **Bids are evaluated by one person instead of a panel.** This could indicate that a contractor was chosen because of his/her connection to the person selecting the contractor, rather than on the merits of his/her bid.
- **The contractor gave benefits to government officials.** Information indicates that the successful contractor provided gifts, parties, meals, or any other benefits to a government official connected with the contract.
- **Several small contracts are issued sequentially to the same supplier.** This may indicate that contracts have been split to keep the contract values low and avoid a competitive process. Officials have more discretion in awarding small contracts. By splitting a large contract into several smaller ones, an official may be able to direct the contract to a specific supplier.
- **Exceptions are made to the tender deadline.** Tenders were opened prior to the deadline. Tenders received after the closing date were not disqualified.
- **Bids are changed after they are submitted.** Information indicates that changes were made to bid documents after they were submitted.
- **Changes are made to the contract specifications after the contract is awarded but before it is signed.** New contract specifications were developed because of a consultation with the successful bidder and were incorporated into the final contract. These specifications result in additional charges, over and above those originally specified in the call for tenders documentation.
- **The request for proposal contains a mistake that invalidates the call for tenders or request for proposal.** If a mistake is found in the bid specification document after the submissions have been evaluated, it may indicate that an official wants to invalidate the competition because the wrong contractor was about to win the bid.

- **The lowest bidder is not selected.** There is no adequate explanation for not accepting the lowest bid when the lowest bid proposal meets all other contract requirements.

Description of Red Flags That May Indicate Anti-Competition Activity

- **An analysis of bidders and contract awards indicates patterns.** The bidders are always the same. No bidder wins consecutive contracts. Certain bidders always win in certain regions of the country.
- **Competition is restricted.** The request for proposal was not published in a newspaper. Rather it was expressed orally to a few contractors, or was announced in obscure publications, or during a holiday period or weekend.
- **Bids refer to industry-wide pricing practices.** Bidders may collude to fix prices. Indicators include a reference in a bid to an industry price list or price agreements, or to association price schedules, industry price schedules, industry-suggested prices, industry-wide prices, market-wide prices or market share.
- **Correspondence with contractors suggests possible collusion.** Letters, notes, or memos by government employees, former employees, or competitors indicate only a particular company sells in a particular area, or that it is not that company's turn to receive a contract.
- **There are unusual withdrawals of tenders.** The lowest bidder withdraws his/her bid after it has been submitted, or a bidder withdraws from the contracting process and the justification for doing so is vague.
- **Bid details are peculiar or different bids display similarities.** A review of the bids reveals certain anomalies. Or, identical amounts, calculations, or spelling errors appear in two or more competing bids.
- **The successful contractor uses competitors as subcontractors.** If the winning contractor uses competing bidders, it may indicate collusion. Auditors should be aware of situations where:
  - a low bidder withdraws from the contracting process but subsequently becomes a subcontractor of a higher bidder,
  - the successful bidder repeatedly subcontracts work to companies that submitted higher bids or to companies that qualified to act as prime contractors but did not submit a bid,
  - a contractor's tender package includes the bids of subcontractors who are actually competing for the main contract, and
  - the successful contractor uses unsuccessful bidders as subcontractors for the same project.
- **Bids are higher than expected.** Final bids are higher than preliminary cost estimates, previous bids by the same firms, published price lists, or comparable bids of other buyers in the same or similar markets.
- **Related companies submit individual bids.** Related companies submit bids for the same contract and do not disclose their relationship.

- **There are few bidders and only one qualified contractor, because dummy bids are submitted.** Only one bidder has submitted a bid that meets the necessary specifications and requirements. Other bids do not respond to the contract's requirements.
- **Bids include labour costs that are too high or too low.** Manipulating labour costs may be one way colluding bidders can rig bids.

Description of Red Flags for Non-Competitive Contracts

- **A contract is changed from competitive to sole-source.** A contract that was initiated using the competitive process is converted into a negotiated contract.
- **The documentation used to justify sole-source contracting is inadequate.** Documentation in the file in support of a non-competitive contract does not justify sole-sourcing. Such situations may also indicate intervention by officials who would not normally be involved in this type of contract.
- **Contracts are repeatedly awarded to the same contractor.** Alternative sources of goods or services are not developed; purchases are repeatedly made from a single source. Or, goods or services are purchased from the same source or contractor over a long period of time without verifying market price changes or other producers of the product or service.
- **Several small contracts are issued sequentially to the same supplier.** Contracts may have been split to by-pass government financial authority, and to avoid several review levels.
- **Use of standing offers is unusual.** Unusual use of standing offers, for example, for large purchases where a competitive process may be justified, could indicate that a supplier is being unduly favoured.
- **Local purchase orders (LPOs) are valued beyond approved dollar limits.** Using local purchase orders to make may small purchases from the same supplier may indicate that a supplier is being unduly favoured. Auditors do not usually audit LPOs because of their low levels of materiality. However, auditors should consider reviewing local purchase orders because as they are not well controlled.

Description of Red Flags for Fixed-Cost Contracts

- **Changes are made to a contract after it is awarded, resulting in substantially increased charges.** The government entity changes the definitions of the required services after the contract has been awarded. This enables the supplier to submit charges for losses, which the contractor blames on government-mandated changes.
- **Change orders are issued without adequate explanation or as a result of circumstances that should have been foreseen.** Change orders are issued that are inadequately justified or that may have been caused by problems that the contractor should have known about. For example, during a demolition contract, hazardous materials are uncovered resulting in more costly requirements to demolish the building. The contractor charges additional costs to the organization that should have been foreseen before awarding the contract.
- **A contract is unexpectedly extended.** An unexpected contract extension is granted allowing the contractor to complete the project beyond the termination date specified in the contract and/or in the requirements definition.
- **A contract has significant cost over-runs.** The amount invoiced by the contractor significantly exceeds the contract amount; the justification provided is questionable. This situation may result from poor bid specifications which enable the contractor to recoup losses that would not otherwise be compensated.
- **Contractor invoices are not reviewed.** The contractor's invoices are not compared to previously submitted invoices or to project schedules to determine whether they have already been paid by the government. Or, invoices are not reviewed to ensure they meet project specifications.
- **Test certification documentation is inadequate or missing.** No original test results or reports appear in the contract file even though they are required by the contract specifications. Or, a test certification by an independent test agency is missing, although it is required.
- **Inspection reports are inadequate or missing.** PWGSC or other government inspections appear inadequate, or inspection reports are incomplete or missing.
- **Complaints or disclosures are received about the inferior quality of the goods and services provided.** Documentation or interviews show that there is concern about the supply of inferior quality goods or services.
- **Certification under section 34 of the *Financial Administration Act* is missing or incorrect.** Section 34 required that an authorized person certify that the work has been performed, the goods supplied or the service rendered in accordance with the contract. There is no section 34 certification in the file or the person signing does not have the authority to sign.

Description of Red Flags for Cost-Plus and Cost-Per Contracts

- **There are inadequate inspections at each stage of the contract.** There is no qualified government inspector on site to confirm that, at each stage of the contract, the work that has been billed was completed.
- **Rates charged are higher than those stipulated in the contract.** The contractor charges higher rates than allowed, or submits charges for services that are not included in the contract or the bid specifications.
- **Photocopies are submitted to support charges.** The contractor submits photocopies of invoices for charges to the government on a cost-plus contract.
- **There is evidence of double billing.** Invoices for the same goods and services are submitted more than once.
- **Invoices provide inadequate information about the contractor.** Contractor or subcontractor invoices lack telephone numbers and/or have only a post office box address.
- **Invoices are questionable.** Information is crossed out or correction fluid has been used on the original document. Products listed on the invoice are only referenced by a number.
- **Invoices are not certified as paid.** The contractor does not certify that third party invoices submitted to the government have been paid.
- **The contractor's employees or subcontractors do not have the required skills.** The contractor uses untrained employees when skilled personnel are required.
- **Labour costs appear high.** Labour costs are most susceptible to misrepresentation because employee labour can be readily shifted to any contract by falsifying time cards. The contractor may charge hours worked on other projects to the contract.
- **Charges for overtime seem unreasonable.** Overtime is charged when it was not incurred, or it is charged at rates significantly higher than those stipulated in the contract.
- **Quality assurance is weak or does not exist.** Examples of weak quality assurance include the following:
  - the entity has minimal or no inspection and quality assurance programs;
  - goods and materials have not been tested as required in the contract specifications;
  - foreign products were provided when domestic products were required;
  - the contracting entity relies entirely on the contractor to ensure that goods and services meet government specifications; or

  - government employees rely on the contractor's word that testing has been carried out, or that tests have met government requirements.
- **Incomplete cheques are submitted as proof of payment.** The contractor submits photocopies of only the front side of a cheque to indicate that the invoices supporting the charge on a cost-plus contract were paid.
- **The timing of progress payment charges do not coincide with plans.** Progress payments do not appear to coincide with the contractor's plans.
- **Claims are made for materials that are not purchased.** Progress payment claims are made for materials that are not supported by a paid invoice.

Part 4: Wrongdoing and Fraud in Grants and Contributions

Introduction

Part 4 covers aspects of wrongdoing and fraud for grants and contributions. It should be read in conjunction with the Introduction and Parts 1 and 2.

Part 4 is intended to help auditors to

- assess the risks of wrongdoing and fraud related to grants and contributions;
- recognize the red flags or indicators of grant and contribution wrongdoing and fraud; and
- identify potential wrongdoing and fraud.

Although the focus of Part 4 is on grants and contributions, auditors should apply these auditing principles to other government funding arrangements that are designed to transfer funds to various entities under specified accountability arrangements or other authorities. Examples include

- alternative funding arrangements,
- collaborative arrangements,
- joint ventures,
- partnerships, and
- special foundations.

This part includes

- How Grant and Contribution Wrongdoing and Fraud May Occur,
- Screening Grants And Contributions,
  - Stage 1—Proposal, Application, and Selection,
  - Stage 2—Establishing the Agreement and Initiating Funding,
  - Stage 3—Reporting and Monitoring Compliance With Terms and Conditions,
  - Stage 4—Post-Agreement Review and Subsequent Events.

How Grant and Contribution Wrongdoing and Fraud May Occur

The following are common types of grant and contribution wrongdoing and fraud.

- bribery and corruption
- conflict of interest
- embezzlement
- false representation
- false claims
- fraudulent concealment
- improper or unusual approval authorities
- false and misleading statements
- misuse of funds or assets
- quality substitution
- questionable or fraudulent performance reporting

For descriptions of these red flags, see "Description of How Grant and Contribution Wrongdoing and Fraud May Occur" on page 82.

Screening Grants and Contributions

One of the keys to identifying wrongdoing and fraud is the ability to spot anomalies. These irregularities should be considered red flags. Cases of wrongdoing and fraud usually exhibit such red flags. Knowledge of these red flags provides auditors with a significant head-start in recognizing potential wrongdoing. Auditors should be aware of red flags, know when to use them, and understand their strengths and limitations.

It is important that auditors understand the normal process for grants and contributions to be able to spot red flags that may indicate wrongdoing and fraud. The grants and contributions process comprises the following four stages:

1) Stage 1—proposal, application, and selection;

2) Stage 2—establishing the agreement and initiating funding;

3) Stage 3—reporting and monitoring compliance with terms and conditions; and

4) Stage 4—post-agreement review and subsequent events.

Initially, auditors should ask the following two questions when screening grants and contributions:

1) Did the department or agency act appropriately when seeking the necessary approvals including, where applicable, Treasury Board approval?

2) Did the department or agency and the recipient organization properly exercise their authority and responsibilities with respect to fulfilling the terms and conditions of the agreement?

Answers to these questions may indicate red flags that may require further investigation.

This section includes

- Assessing the Risk of Wrongdoing and Fraud
- Conflict of Interest
- Reviewing Documentation for Grants and Contributions
- Stage 1—Proposal, Application, and Selection
  - Red Flags for the Proposal, Application, and Selection Stage
- Stage 2—Establishing the Agreement and Initiating Funding
  - Red Flags for Establishing the Agreement and Initiating Funding
- Stage 3—Reporting and Monitoring Compliance With Terms and Conditions
  - Red Flags for Reporting and Monitoring Compliance With Terms and Conditions
- Stage 4—Post-Agreement Reviews and Subsequent Events
  - Red Flags for Post-Agreement Reviews and Subsequent Events

Assessing the Risk of Wrongdoing and Fraud

Given the non-accountable nature of grants, obtaining grant funds fraudulently only requires falsifying documents at the application stage. Because the recipients of grants are subject to limited scrutiny, there is usually little chance of detecting wrongdoing and fraud after the agreement has been established.

In contrast, there is a greater likelihood of detecting wrongdoing and fraud related to contributions because:

- there are more accountability mechanisms built into contribution agreements,
- funding for contributions occurs on a scheduled payment basis, and
- monitoring and audit are standard practices.

When auditing grants and contribution agreements, auditors should assess whether all necessary authorizations have been received. These authorizations are:

- Parliamentary authority to fund the program via government estimates or legislation,
- Treasury Board approval of the terms and conditions of the program, where required,

- appropriate approvals of agreements by authorized departmental or agency officials, and
- approvals of amendments by authorized departmental or agency officials and, if necessary, by the Treasury Board.

Auditors should also assess whether the recipient of funding meets the conditions, both program conditions and financial reporting conditions, established by the Treasury Board and the department.

Conflict of Interest

Auditors should be sensitive to conflict of interest issues. Public servants must comply with the Treasury Board's conflict of interest and post employment measures (Part of the Values and Ethics Code for the Public Service), which include being impartial and objective. This policy does not apply to recipients of government grants and contributions. If a conflict of interest issue arises concerning third party recipients of government grants and contributions, auditors should determine the significance of the conflict and the OAG's authority to look into the matter. If the OAG does not have a mandate to look into the matter, the auditor should determine whether departmental auditors have the authority to audit recipients. If so, the matter should be referred to the departmental auditors for review and action.

Reviewing Documentation for Grants and Contributions

In order to properly screen grants and contribution arrangements for wrongdoing and fraud, the auditor may need to review the following documentation:

- applications for funding including supporting information such as the organization's annual audited financial statements, and annual reports
- feasibility studies, business plans, and/or other related reports;
- records or documents that outline the decision-making process for awarding grants or contributions;
- the signed funding agreement and any supporting documents required by the agreement such as the entity's organizational structure, financial and budgetary reports, and terms and payment schedule;
- agreement amendments;
- sign-offs as required under the *Financial Administration Act*;
- cheque requisition documentation in support of the initial payment;
- an organization's progress reports submitted to justify continued progress payment; ands
- the records showing the final accounting of funds received and used, and the supporting documentation.

Stage 1—Proposal, Application, and Selection

The objective of the first stage is to ensure that those who receive grants or contributions meet the program's eligibility and other assessment criteria. Detecting wrongdoing and fraud at this stage is easier because applicants generally submit a lot of documentation to justify their eligibility for funding. The auditor can review this information to determine whether recipients satisfy the assessment criteria. The auditor should also review the assessments of the applications of non-successful applicants to determine whether the selection process was reasonable.

Red Flags for the Proposal, Application, and Selection Stage

- There is no application for funding in the agreement file.
- Proposals or business plans are vague.
- There may be a conflict of interest between a government employee and an applicant.
- The organization funded has no previous financial history or has a history of limited success.
- Audited financial information on the organization funded is limited or missing.
- An organization regularly receives funding under the program.
- An organization barely meets the eligibility criteria for funding or has little experience in the field.
- An organization's matching funding is misleading or incorrect.
- The viability of the proposal is suspicious because of unsupportable claims.

For descriptions of these red flags, see "Description of Red Flags for the Proposal, Application, and Selection Stage" on page 84.

Checklist 5 summarizes the red flags for the Proposal, Application and Selection Stage.

Stage 2—Establishing the Agreement and Initiating Payments

Once the applications have been reviewed and the funding awarded, the agreement between the government and the recipient is prepared. Although the risk of wrongdoing at this stage is low, there may be indications that the recipient does not intend to comply with the purposes of the agreement

Red Flags for Establishing the Agreement and Initiating Funding

- The agreement is vague.
- Certain terms and conditions unreasonably favour the recipient and broaden the scope for permitted expenditures.

- The name and address on the funding agreement is different than on the initial application for funding.

For descriptions of these red flags, see "Description of Red Flags for Establishing Agreements and Initial Funding" on page 86.

Checklist 5 summarized the red flags for Establishing the Agreement and Initiating Funding.

Stage 3—Reporting and Monitoring Compliance with Terms and Conditions

The objective of Stage 3 is to ensure that funds are used in accordance with the terms and conditions of the agreement. Recipients of funding under contribution agreements submit reports which government departments and agencies use to make decisions about continuing funding.

The risks of wrongdoing and fraudulent reporting are high in Stage 3 because recipients may be motivated to alter documents to hide their inappropriate actions in order to continue to receive funding. The opportunities to identify possible wrongdoing and fraud also increase during Stage 3 because it involves more monitoring of the recipient's performance.

Weaknesses in monitoring activities by departments and agencies can increase their risks of exposure to wrongdoing and fraud. Auditors should review the adequacy of these activities with a view to identifying any significant weaknesses. At a minimum, departments and agencies should be carrying out the monitoring activities specified in the agreement.

Red Flags for Reporting and Monitoring Compliance with Terms and Conditions

- There are complaints from users about the recipient's services.
- Subcontractors or suppliers are not getting paid.
- The department does not adequately monitor contribution agreements.
- Recipient's performance and financial reports seem exaggerated or inconsistent.
- The recipient becomes insolvent or bankrupt shortly after receiving government funding.
- Most of the funding has been spent but the purpose of the agreement is far from achieved.
- The valuation of in-kind matching funding appears to be unreasonable.
- Matching funding provided by third parties is misrepresented.
- Payments are made without sufficient verification that the work has been performed.
- An adverse event has suddenly brought into question the success of the project.

For descriptions of these red flags, see "Description of Red Flags for Reporting and Monitoring Compliance with Terms and Conditions" on page 87.

Checklist 5 summarizes the red flags for Reporting and Monitoring Compliance with Terms and Conditions.

Stage 4—Post-Agreement Reviews and Subsequent Events

Auditors are generally looking at grants and contributions that have been completed. At this stage, the auditor can assess the recipient's overall performance and the department's compliance with authorities

Red Flags for Post-Agreement Reviews and Subsequent Events

- The project described in the final report is different than the one described in the original agreement.
- Specific requirements of the contribution agreement are not met.
- Payments are not approved by the appropriate people.
- Changes to the original agreement are not approved by the appropriate people.
- Treasury Board approval of changes and/or expenditures is not obtained, when required.
- Total actual costs are significantly over budget, under budget, or very near the original budget.
- The final report is significantly delayed or is lacking critical information.
- Repayable portions of contributions are not recovered.
- The final payment is made before all the terms and conditions of the agreement have been met.

For descriptions of these red flags, see "Description of Red Flags for Post-Agreement Reviews and Subsequent Events" on page 89.

Checklist 5 summarizes the red flags for Post-Agreement Reviews and Subsequent Events.

Description of How Grant and Contribution Wrongdoing and Fraud May Occur

- **Bribery and corruption**—giving gifts, money or other rewards to influence an official act. In the context of grants and contributions, a company provides a government employee with season tickets to hockey games in exchange for favourable consideration of its application for funding.
- **Conflict of interest**—having undeclared private interests that could affect, or be perceived to affect, the independence and objectivity of an individual in carrying out official duties. For example, a government official recommends that a contribution be made to the organization which employees his/her spouse without declaring that a potential conflict of interest exists.
- **Embezzlement**—taking money that has been lawfully received and using it, without the knowledge and consent of the provider of the funds, for other purposes. For example, a person uses the grant money that is intended for a particular project and uses it to satisfy their gambling debts.
- **False representation**—knowingly making false or misleading statements to gain an improper advantage. In the context of grants and contributions, this could involve making false statements to mislead the government in order to obtain funding. For example, an applicant misrepresents an organization's history, its financial position, or the viability of the proposed program. Or, a foreign organization claims to be incorporated in Canada and Canadian-owned, and applies for a grant or contribution for which Canadian ownership is a requirement.
- **False claims**—submitting false documents in order to continue receiving periodic contribution payments. For example, a funding recipient materially represents his/her financial position in order to satisfy conditions in the funding agreement.
- **Fraudulent concealment**—knowingly hiding information that is necessary and important to the funding decision. For example, an applicant seeking funding to undertake certain research fails to disclose that it previously received government funding under a different business name to undertake the identical research.
- **Improper or unusual approval authorities**—those approving funding applications do not have the require delegated authority. Or senior officials, who would not normally be involved in the approval process, take a special interest in the approval of the funding application.
- **Misuse of funds or assets**—a recipient of government funds or assets uses them for purposes for which they were not intended. For example, the recipient of a government grant uses the funds for personal purposes or for a project other than the one specified in the agreement.

- **Quality substitution**—the government receives an alternative product or service that is inferior to that specified in the grant or contribution agreement. The substitution is concealed from the government.
- **Questionable or fraudulent performance reporting**—a funding recipient does not submit all the performance information required by the funding agreement Or the quality and completeness of the performance is so poor that there are suspicions about how funds were used. Minimum or no performance information may indicate that government funds were diverted to other unauthorized projects or used for personal benefit.

Description of Red Flags for the Proposal, Application, and Selection Stage

- **There is no application for funding in the agreement file.** There is no evidence on file of the recipient's application and justification for funding. There is no evidence of the selection process followed or the selection occurred after the funds had been issued.
- **Proposals or business plans are vague.** Unless the proposal is sufficiently detailed, there is no way of knowing how the funds will be spent.
- **There may be a conflict of interest between a government employee and an applicant.** Generally, conflict of interest is difficult to substantiate. If it appears that a recipient would not normally be eligible for funding or it is not clear how the recipient was selected, the possibility a relationship between the applicant and a government employee should be considered.
- **The organization funded has no previous financial history or has a history of limited success.** When there is little known about an organization's history, the organization may be concealing information that would jeopardize its application for funding.
- **Audited financial information on the organization funded is limited or missing.** The terms and conditions of a funding agreement may require that the recipient pay certain expenses with its own funds. The organization may try to hide its limited liquidity by providing limited financial information. If the assessment of proposals is done properly, the lack of financial information should be questioned.
- **An organization regularly receives funding under the program.** Government officials may become lax in their scrutiny of applications and proposals when an organization repeatedly submits funding applications. As well, the more trust and familiarity that develops between the parties, the greater the need to ensure that substantive documentation is detailed and well scrutinized.
- **An organization barely meets the eligibility criteria for funding or has little experience in the field.** An organization's eligibility may be weak or below the acceptable level. The project is to be carried out by parties that lack the required specialized expertise. The involvement of unusual or inappropriate parties, without adequate justification, should be investigated further.
- **An organization"s matching funding is misleading or incorrect.** An organization may need to match government funding with funding from another source. Organizations may try to overstate their matching funds. Indicators of potentially overstated or non-existent matching funding include the following:

  a) repeated use of donations-in-kind;

b) financial statements that deviate from the norm or are awkwardly presented;

c) the use of amounts receivable from organizations affiliated with the applicant as a main source of matching funding; and

d) matching funding which is provided for a short period by an organization affiliated with the applicant and is withdrawn once the government funds are received.

- **The viability of the proposal is suspicious because of unsupportable claims.** Claims made by the applicant about the project which cannot be supported by documentation should be treated with suspicion.

Description of Red Flags for Establishing Agreements and Initial Funding

- **The agreement is vague.** A vague agreement opens the door to wrongdoing and fraud. Measuring the performance of the recipient will be difficult and the likelihood that the recipient will make expenditures that are not really for the intended purposes increases.
- **Certain terms and conditions unreasonably favour the recipient and broaden the scope for permitted expenditures.** Terms and conditions that deviate from the norm, especially generous provisions for allowable expenditures, should be investigated. Favourable conditions could also indicate bribery or kickbacks.
- **The name or address on the funding agreement is different than on the initial application for funding.** This could indicate that the recipient organization is different than the applicant for funding. Or, the initial name may have been fictitious or the applicant materially misrepresented its circumstances. Corporate registry searches of company names may be required to obtain incorporation documents or general information on businesses.

Description of Red Flags for Reporting and Monitoring Compliance with Terms and Conditions

- **There are complaints from users about the recipient's services.** Repeated complaints about the quality of the service provided by the recipient could indicate that funding is being used for other purposes. Financial information may not show any indicators of this occurring. Third party independent verification may be necessary to confirm such abuse.
- **Subcontractors or suppliers are not getting paid.** Subcontractors or suppliers are complaining to the department that they have not been paid or notification is received that the funding recipient is being sued by sub-trades for work performed on the project.
- **The department does not adequately monitor contribution agreements.** The funding agreement gives the department the right to audit the recipient but this right is never used. Financial statements submitted by recipients are not audited by third parties as required.
- **Recipient's performance and financial reports seem exaggerated or inconsistent.** For the recipient to continue to receive funding, performance and financial reports must demonstrate that work has been done. If a recipient is experiencing difficulties, there is a high risk that performance reports may be falsified to ensure that funding continues. If a recipient claims ineligible expenses, there is a strong likelihood that financial reports will be overstated and performance reports may be exaggerated to correlate with the expenditures. Inconsistent reported results may also indicate that the work is not progressing well and the reports have been falsified.
- **The recipient becomes insolvent or bankrupt shortly after receiving government funding.** The recipient declares bankruptcy and the government funding goes toward paying off creditors. This may indicate that there was never an intention to fulfill the purposes of the funding agreement but that the real purpose was to divert the funds to pay off creditors.
- **Most of the funding has been spent but the purpose of the agreement is far from achieved.** When a recipient has gone through most of the funding provided and yet the purpose of the agreement is far from being achieved, it may be that funds are being misappropriated. Diverting funds for personal use is tempting when large sums are available. It may involve funnelling funds to affiliated organizations or taking small amounts of cash at regular intervals to avoid detection.
- **The valuation of in-kind matching funding appears to be unreasonable.** Sometimes, when a contribution agreement requires recipients to match federal funding with funding from other sources, the matching funding may take the form of contributions of goods or

services. If the valuation of these goods or services seems high, it may have been overstated to justify that the recipient's contribution matches the government funding. In-kind contribution valuation cannot easily be verified .

- **Matching funding provided by third parties is misrepresented.** A recipient overstates matching funding provided by third parties or reports matching funding from third parties that was never provided.
- **Payments are made without sufficient verification that the work has been performed.** Normally, after the initial payment specified in the agreement, contributions are paid as reimbursements of costs or expenses incurred by the recipient. Any payments without evidence that the recipient has incurred the expense should be questioned.
- **An adverse event has suddenly brought into question the success of the project.** Information previously submitted by the recipient may have concealed the situation from the government so that funding for the project would continue.

Description of Red Flags for Post-Agreement Reviews and Subsequent Events

- **The project described in the final report is different than the one described in the original agreement.** Auditors should determine whether changes have been made to the original agreement and, if so, why the changes were made and whether the proper approvals were obtained. The final project may look reasonable but any significant departure from the terms of the original agreement may indicate misuse of funds.
- **Specific requirements of the contribution agreement are not met.** For example, all sources of funding are not disclosed to the department, or the recipient's financial statements are not audited as required.
- **Payments are not approved by the appropriate people.** Auditors should investigate any payments that have not received proper authorizations. Even if expenditures are within budget and appear reasonable, this does not eliminate the requirement that they be authorized.
- **Changes to the original agreement are not approved by the appropriate people.** Generally, amendments to agreements require the approval of the original parties to the agreement. Auditors should follow up on any changes made to agreements that are not properly authorized.
- **Treasury Board approval of changes and/or expenditures is not obtained, when required.** Transactions that exceed predetermined thresholds require Treasury Board approval. If Treasury Board is not given the opportunity to review a transaction, it could indicate that someone wanted to avoid scrutiny.
- **Total actual costs are significantly over budget, under budget, or very near the original budget.** Some cost overruns or shortfalls can be expected, but significant budget variations may indicate improper activities. Overruns could indicate that ineligible expenditures have been claimed. Under budget results may indicate that inferior or insufficient goods or services were provided. A project that is near budget may also raise suspicions. It may be that the project was under budget but additional, non-allowable expenditures or personal items were charged to the project to use up the funding. To determine the reasonableness of expenditures, auditors may need to seek the advice of specialists.
- **The final report is significantly delayed or is lacking critical information.** As the final payment is contingent upon receiving the final report, recipients normally want to ensure it is submitted as promptly as possible. A late submission may indicate extra time was needed to develop a report that would be acceptable. Auditors should review the final report for completeness and compliance with the terms and conditions of the agreement.

- **Repayable portions of contributions are not recovered.** Some contributions (for example, where the objective is investment in economic development) may include provisions for the repayment of a portion of the contribution. In such cases, the auditor should ensure that such repayments are recovered.
- **The final payment is made before all the terms and conditions of the agreement have been met.** The final payment of grants and contributions should only be made after all required information has been received and approvals have been provided to release the balance of funds.

Part 5: Wrongdoing and Fraud in Non-Tax Revenue

Introduction

This part provides guidance to auditors to help them:

- assess the risks and identify potential wrongdoing and fraud related to non-tax revenues;
- recognize many of the red flags or indicators of wrongdoing and fraud for non-tax revenues;
- follow the appropriate steps and actions when they suspect contract wrongdoing and fraud.

This part should be read in conjunction with the Introduction, Part 1 and Part 2.

In addition to taxes, the government earns revenues from its investments, including consolidated Crown corporations and other government business enterprises, from foreign exchange transactions, from the disposal of surplus assets and from fees charged for products or services, rights or privileges or access to government-owned resources.

This guidance discusses the types of wrongdoing and fraud and the red flags associated with non-tax revenue from the disposal of surplus assets and the sale of government goods or services, including rights, privileges and access to resources.

In 1997, the government introduced a policy of charging user fees for a wide variety of government services where private parties derive a benefit from the service. These benefits include products, services, rights or privileges, and access to or use of government-owned resources. These revenues include such things as

- inspection services fees,
- fees for use of federal testing facilities,
- drug evaluation fees,
- passport fees,
- consular service fees,
- import and export licences,
- spectrum communication fees,
- commercial fishing licences,
- mineral rights,
- patent fees, and

- copyright fees.

The Treasury Board External Charging Policy provides information on how these fees are to be determined.

Wrongdoing and fraud involving non-tax revenues can easily go undetected in government entities because entities and auditors focus on expenditures and tend to monitor and control expenditures rather than monitor and control non-tax revenues.

This part includes

- How Non-Tax Revenue Wrongdoing and Fraud May Occur
- Screening Non-Tax Revenues
  - Reviewing Documentation for Non-Tax Revenues
  - Red Flags for Non-Tax Revenues

How Non-Tax Revenue Wrongdoing and Fraud May Occur

- accounts receivable write-offs
- appropriation of unusual sources of revenue
- bribery or kickbacks
- collusive bidding, price-fixing
- conflict of interest
- disposal of assets for personal gain
- false disclosure
- information theft
- theft of accounts receivable
- unrecorded or under-recorded sales

For descriptions, see "Description of How Non-Tax Revenue Wrongdoing and Fraud Occurs" on page 95.

Screening Non-Tax Revenues

One of the keys to detecting wrongdoing and fraud is the ability to spot anomalies. These irregularities should be considered red flags. Cases of wrongdoing and fraud usually exhibit such red flags. Knowledge of these red flags provides auditors with a significant head-start in recognizing potential wrongdoing. Auditors should be aware of red flags and indicators, know when to use them, and understand their strengths and limitations.

The screening of non-tax revenues for red flags associated with wrongdoing and fraud is done in the course of regular audit work. Auditors should be aware of an entity's risk factors for this type of wrongdoing and fraud. Increased review and testing of the non-tax revenues should be undertaken where the risks of wrongdoing and fraud are high.

This section includes

- Reviewing Documentation for Non-Tax Revenues
- Red Flags for Non-Tax Revenues

Reviewing Documentation for Non-Tax Revenues

To screen non-tax revenue for wrongdoing and fraud, auditors should review the following:

- invoices related to the sale of goods or services,
- contracts for leases of Crown lands,
- agreements for the issuance of rights and privileges,
- agreements for the use of Crown-owned intellectual property,
- contracts for the disposal of surplus Crown assets,
- accounts receivable aging
- accounts receivable write-offs and credit memos, and
- bank reconciliations for all specified purpose accounts.

Red Flags for Non-Tax Revenues

- Appropriate approvals are not obtained.
- There is unusual involvement by senior officials.
- The arm's length relationship is questionable.
- There are unusual trends in revenues.
- Revenues don't compare with provincial revenues.
- Few bids are received for rights to use Crown lands.
- Crown assets are sold as surplus and replaced soon afterward with similar new assets
- The lead time for disposing of surplus Crown assets is very short.
- There is little or no advertising of the disposal of Crown assets.
- Surplus Crown assets are resold by the purchaser within a short period of time.

- Fee charges are less than fair market value.
- Receivable postings do not match deposits.
- There is poor segregation of duties for accounts receivable.
- Accounts that are not in arrears are sent to a collection agency.
- The accounts receivable ledger does not reconcile with the control account.
- There is poor collection of receivables.
- There are unexpected changes in accounts receivable.
- Write-offs of accounts receivable are not properly approved.
- There are unusual write-offs of accounts receivable.

For descriptions of these red flags, see "Description of Red Flags for Non-Tax Revenues" on page 97.

For more information about these red flags for non-tax revenues, see Checklist 6.

Description of How Non-Tax Revenue Wrongdoing and Fraud Occurs

- **Accounts receivable write-offs**—an employee writes off as uncollectible, accounts receivable that are not really in arrears or will likely be collected. This is done to conceal the theft of accounts receivable payments or the future theft of payments. Third parties may also conspire with government employees to write off their outstanding receivables in exchange for a percentage of the write-off.
- **Appropriation of unusual sources of revenue**—manufacturers or wholesalers sometimes issue discounts or rebates for large purchases or volume purchases. These discounts or rebates are usually issued annually, as a separate cheque. As a large purchaser, the government may qualify for a discount or rebate. A government employee does not record the amounts received in the accounting system and steals the cheques. These amounts can be easily stolen and hard to detect as there is no record of the amounts ever being receivable.
- **Bribery or kickbacks**—an individual gives a government employee money or gifts in order to receive preferential treatment. For example, an individual gives money to a government employee to obtain surplus Crown assets at a low price.
- **Collusive bidding, price-fixing**—prospective buyers of government goods or rights to exploit publicly-owned resources reach an agreement among themselves, the effect of which is to eliminate or limit competitive bidding.
- **Conflict of interest**—a government employee has an undisclosed personal interest that may affect, or be perceived to affect, his/her independence and objectivity in carrying out his/her job responsibilities. In the context of non-tax revenues, a government official sells goods or services to a company that employs his/her spouse at lower prices or on more favourable terms than those that could have been negotiated with another company.
- **Disposal of assets for personal gain**—a government employee with a personal interest in government assets could identify those assets as surplus goods even though they still have a government purpose. The sole reason the employee identifies those assets as surplus is to purchase them for personal benefit.
- **False disclosure**—an organization makes false disclosures to the government to maximize its profits. For example, an organization could obtain the right to use Crown lands in return for paying set fees on the lumber or minerals removed. The organization submits false information on the quantity and quality of the resources to minimize the fees it must pay. Or, an organization obtains the right to use Crown-owned intellectual property in return for paying the government a percentage of future earnings from its commercial application. The organization submits false information concerning the revenues earned from its commercial application.

- **Information theft**—a government employee releases information to a third party without charge when the information should have been sold.
- **Theft of accounts receivable**—an employee steals a payment received. Or an employee enters only part of the payment received in the accounting records and pockets the difference. To avoid being detected, the employee posts B's payment to A's account, C's payment to B's account, etc. This process, called lapping, requires continuous manipulation and monitoring of many accounts and transactions.
- **Unrecorded or under-recorded sales**—an employee sells government goods or services to an outside party and immediately steals the payment without creating any record of the sale. Or, an employee sells government assets, which are subsequently forgotten or recorded as stolen items. An employee can also record part of the payment by showing a lower amount on the government copy of the invoice than on the third party's invoice. When payment is subsequently received, the employee can steal the difference.

Description of Red Flags for Non-Tax Revenues

- **Appropriate approvals are not obtained.** Transactions are approved by departmental employees who do not have the required authority.
- **There is unusual involvement by senior officials.** Particular attention should be given to transactions where senior officers, who are not normally involved in such transactions, are actively involved.
- **The arm's length relationship is questionable.** Any indicators of a relationship between a government employee and an organization doing business with the government should be questioned. An example of a questionable relationship is one where a consultant who identified surplus Crown assets also bids to buy some of those assets.
- **There are unusual trends in revenues.** Revenues generated by the government entity are flat or do not reflect the overall strength of the economy, with no corresponding reason. Revenues from the licence of Crown-owned intellectual property for commercial application are falling without explanation.
- **Revenues don't compare with provincial revenues.** Revenues generated from fees for the removal of lumber or minerals from federal Crown lands do not correspond with fees paid to provinces for the use of similar lands in the same vicinity.
- **Few bids are received for rights to use Crown lands.** Companies may have colluded to divide up the country into regions. To keep prices low, companies only bid in their own region.
- **Crown assets are sold as surplus and replaced soon afterward with similar new assets.** A government employee may have declared the assets in order to purchase them for personal benefit.
- **The lead time for disposing of surplus Crown assets is very short.** If the period for bidding on surplus Crown assets is very short, with no apparent justification, it may indicate that only bidders with inside knowledge will be able to submit a bid.
- **There is little or no advertising of the disposal of Crown assets.** Limited advertising is done to dispose of large or unique surplus Crown assets, such as lands or buildings or large pieces of equipment.
- **Surplus Crown assets are resold by the purchaser within a short period of time.** If the purchaser can resell the assets at a substantially higher price, the government did not receive fair market value.
- **Fees charged are less than fair market value.** Government fees for goods and services are priced significantly lower than fair market value, or are below government posted prices at other locations in the country.
- **Receivable postings do not match deposits.** If credits to receivable accounts do not match deposits, this could indicate theft of payments received.

- **There is poor segregation of duties for accounts receivable.** Logging of payments received and recording payments in the accounts receivable ledger should be assigned to different employees. Where one employee is responsible for both functions, additional supervision of the employee may be required.
- **Accounts that are not in arrears are sent to a collection agency**. A government employee may be in collusion with a collection agency. For example, an account that can reasonably be expected to pay, is sent to a collection agency in return for a kickback from the collection agency.
- **The accounts receivable ledger does not reconcile with the control account.** When ledgers do not reconcile with other controls, it may indicate that entries have not been recorded, or that funds have been misappropriated.
- **There is poor collection of receivables.** An organization that has a history of poor collection on its accounts receivable may have an employee who is stealing payments and subsequently writing-off the accounts receivable.
- **There are unexpected changes in accounts receivable.** If previously good accounts now have amounts overdue or if the total amount of overdue accounts receivable is unusually high, an employee may have misappropriated payments.
- **Write-offs of accounts receivable are not properly approved**. An employee, who does not have the proper authority, writes off accounts receivables, or the required two approvals for write-offs have not been obtained. Writing-off accounts receivable is a means of concealing theft of payments.
- **There are unusual write-offs of accounts receivable.** Accounts that appear to have been good accounts are written off. This may suggest funds have been misappropriated.

Part 6: Wrongdoing and Fraud in Other Vulnerable Areas

Introduction

Part 6 discusses aspects of wrongdoing and fraud in other vulnerable areas. It should be read in conjunction with the Introduction and Parts 1 and 2.

Part 6 covers specific areas in government operations where wrongdoing and fraud may also take place and which were not previously discussed in other parts. The other vulnerable areas where wrongdoing and fraud can occur are

- acquisition cards/credit cards,
- expense accounts,
- payroll and personnel, and
- asset management.

One of the keys to detecting wrongdoing and fraud is the ability to spot anomalies. These irregularities should be considered red flags. Cases of wrongdoing and fraud usually exhibit such red flags. Knowledge of these red flags provides auditors with a significant head-start in recognizing potential wrongdoing. Auditors should be aware of red flags and indicators, know when to use them, and understand their strengths and limitations.

The part includes

- Acquisition Cards/Credit Cards
  - How Acquisition Card/Credit Card Wrongdoing and Fraud May Occur
  - Screening Acquisition Cards/Credit Cards for Wrongdoing and Fraud
  - Red Flags for Acquisition Card/Credit Card Wrongdoing and Fraud
- Expense Accounts
  - How Expense Account Wrongdoing and Fraud May Occur
  - Screening Expense Accounts for Wrongdoing and Fraud
  - Red Flags For Expense Account Wrongdoing and Fraud
- Payroll and Personnel Wrongdoing and Fraud
  - How Payroll and Personnel Wrongdoing and Fraud May Occur
  - Screening Payroll and Personnel Files for Wrongdoing and Fraud
  - Red Flags for Payroll and Personnel Wrongdoing and Fraud

- Theft of Assets
  - How Asset Theft May Occur
  - Red Flags for Fixed Assets Theft

Acquisition Cards/Credit Cards

How Acquisition Card/Credit Card Wrongdoing and Fraud May Occur

Acquisition card/credit card frauds occur when the cards or their credit numbers are used to purchase goods or services for non-government purposes or for unauthorized uses. This kind of fraud also includes card use as a means to appropriate funds directly from the government. The risk of acquisition card fraud is high because:

- it is an easy way to make purchases,
- there is a large number of government credit card holders,
- government credit cards are accepted by millions of merchants, and
- purchase slips or monthly statements are inconsistently reviewed by cardholders, finance personnel, or auditors.

The following are some types of acquisition card/credit card fraud. Click on each item to read a description.

- personal purchases
- unauthorized billings
- unauthorized charges by retailers, wholesalers, and contractors

For descriptions, see "Description of How Acquisition Card/Credit Card Wrongdoing and Fraud May Occur" on page 105.

Screening Acquisition Cards/Credit Cards for Wrongdoing and Fraud

To screen acquisition card/credit card purchases for wrongdoing and fraud, auditors should review the following documentation:

- acquisition card statements,
- acquisition card purchase flimsies,
- merchant invoices,
- hospitality and travel expense claims,
- vacation and other leave records, and
- government and entity acquisition card policies.

Red Flags for Acquisition Cards/Credit Cards Wrongdoing and Fraud

- Multiple purchases are made at the same vendor or on the same day.
- Purchases are made with an odd business vendor or it is unusual to use credit cards with a particular vendor.
- Receipts to support statement transactions are incomplete or non-existent .
- Monthly acquisition card statements are not reviewed by auditors.
- Cardholders make purchases on weekends, during their vacation time, or on special leave.
- The cardholder has personal financial difficulties.

For descriptions of these red flags, see "Description of Red Flags for Acquisition Card/Credit Card Wrongdoing and Fraud" on page 106.

Checklist 7 summarizes the red flags for acquisition card/credit card wrongdoing and fraud.

Expense Accounts

Expense account or expense claim wrongdoing and fraud normally involve reimbursing overstated, fictitious, or duplicate expenses. The risk of expense account and expense claim wrongdoing and fraud is high because clerks who manage the claims do not feel comfortable challenging expense reports and claims, particularly those submitted by senior officials. Even though there are very detailed Treasury Board guidelines on claimable employee expenses, expense accounts are easily and frequently abused.

How Expense Account Wrongdoing and Fraud May Occur

The following are some examples of expense account abuses and frauds.

- Personal expenses are submitted as business expenditures.
- Expenses are submitted twice.
- A claim for expenses that someone else paid for is submitted for reimbursement.
- A false claim for automobile kilometre charges is submitted.
- An invoice is submitted for an item that was returned for a refund.

For descriptions, see "Description of How Expense Account Wrongdoing and Fraud May Occur" on page 107.

Screening Expense Accounts for Wrongdoing and Fraud

To screen expense accounts or claims for wrongdoing or fraud, auditors should review the following documentation:

- the expense account or claim,
- hospitality expenses,
- entity acquisition card monthly statements,
- time cards or travel itineraries,
- vacation leave and other types of leave, and
- travel and hospitality policies.

Red Flags for Expense Account Wrongdoing and Fraud

- Expense receipts are missing.
- Detailed expense receipts are missing.
- Photocopied receipts or invoices are submitted.
- The date on a receipt is old or missing.
- An employee submits an expense report even though he or she has an entity credit card.
- Receipts do not match the employee's travel, plans, work schedule, or time sheets.
- The purpose of the expense is not indicated.
- Entity credit card statements are not checked against expense reports.
- The expense report review process is inadequate.
- A T4A is not issued for taxable benefits.
- Code of Conduct or ethics policies are weak, do not exist, or are not enforced.

For descriptions of these red flags, see "Description of Red Flags for Expense Account Wrongdoing and Fraud" on page 108.

Checklist 8 summarizes the red flags for expense account wrongdoing and fraud.

Payroll and Personnel Wrongdoing and Fraud

Payroll and personnel wrongdoing and fraud involve interfering with the cash disbursements and payables cycles so that the organization unknowingly makes a fraudulent payroll disbursement. Organizations that have poor controls over payroll functions are susceptible to this kind of fraud.

How Payroll and Personnel Wrongdoing and Fraud May Occur

The following are common types of payroll and personnel fraud.

- overtime abuse
- overpayment

- annual leave cash out
- severance pay
- ghost employees
- terminated employees are not deleted from the payroll system
- employment insurance fraud
- staffing and classification abuse

For descriptions, see "Description of How Payroll and Personnel Wrongdoing and Fraud May Occur" on page 109.

Screening Payroll and Personnel Files for Wrongdoing and Fraud

To screen payroll accounts for wrongdoing and fraud, auditors typically use computer assisted techniques, such as data mining. Data mining refers to using special computer software programs to search for red flags. Data mining software programs are designed to search large databases and report on identified items (hits) that may suggest irregularities or fraud. Auditors can use data mining software to identify red flags in large databases and between different databases that would probably never be uncovered otherwise. The auditor analyzes the report of hits for possible wrongdoing and fraud.

A sample of data mining searches is provided in "Appendix 3—Data Mining to Detect Wrongdoing and Fraud" on page 127.

Red Flags for Payroll and Personnel Wrongdoing and Fraud

- There is poor internal control of payroll and personnel functions.
- Senior officials or employees cash-out vacation leave on a regular basis.
- There is a high proportion of reclassifications upward or other unusual trends in staffing actions
- There are duplicate or illegitimate social insurance numbers.
- There are duplicate addresses or deposit accounts.
- Payroll amounts are missing basic deductions.
- Notices are received from CRA that payroll taxes are delinquent.
- There are a high number of manually prepared cheques.

For descriptions of these red flags, see "Description of Red Flags For Payroll and Personnel Wrongdoing and Fraud" on page 110.

Checklist 9 summarizes red flags for payroll and personnel wrongdoing and fraud.

Theft of Assets

The risk of theft increases when an organization has assets that can easily be removed from its premises. The risk is high when an organization lacks a proper system of counting, tagging and identifying assets. In some cases, employees may create false documentation or tamper with inventory records to conceal missing assets. Outside third parties may be accomplices in the theft.

How Assets Theft May Occur

The types of assets theft include:

- **Employees take assets for personal use**—an employee misappropriates an organization's assets for his/her personal use without attempting to conceal the theft in the organizations books. Or, an employee sells assets for cash without recording the disposal.
- **Assets are sold at less than fair market value**—assets are sold or disposed of at less than fair market value to someone related to an employee. Or, asset disposal may be recorded at a value less than what was received, and the employee misappropriates the difference.
- **Asset requisitions and other documents are used to move assets to another location to facilitate theft**—an employee overstates the amount of supplies and materials needed for a project and takes the excess. Or, false shipping documents are used to ship assets to the employee or to an accomplice.
- **Purchasing and receiving functions are manipulated**—an employee receiving goods on behalf of the organization falsifies incoming shipments and takes part of the shipment.

Red Flags for Assets Theft

- There is poor segregation of duties in asset management.
- The assets are not well monitored.
- Assets are delivered to questionable addresses.
- Write-offs of assets or sales are not well-controlled.
- Proper authorizations and valuations are not obtained for disposal of assets.

For descriptions of these red flags, see "Description of Red Flags for Assets Theft" on page 111.

Checklist 10 summarizes the red flags for asset management.

Description of How Acquisition Card/Credit Card Wrongdoing and Fraud May Occur

- **Personal purchases**—a government employee cardholder purchases goods or services for personal use on their government credit card, without authority to do so, and allows the department or agency to pay for these goods or services without reimbursing the employer. This fraud can go undetected if the goods and services appear to be normal government purchases such as computers, automobile fuel, and travel and hospitality expenses.
- **Unauthorized billings**—an individual who, intentionally and without the cardholder's knowledge, permits the billing of personal or non-government items on a government credit card and does not reimburse the government for these purchases. This fraud is often undetected if the government cardholder does not verify all charges on the credit card statement before authorizing the payment of the outstanding balance.
- **Unauthorized charges by retailers, wholesalers, and contractors**—in this kind of fraud, businesses will process charges against government credit cards for goods and services that were never authorized or never provided. This kind of fraud also includes inflating charges on government credit cards that do not reflect the agreed upon amount for the goods and services provided. This fraud goes undetected if the government cardholder does not verify all charges on the government credit card statement against invoices or purchase orders and permits the outstanding credit card balance to be paid.

Description of Red Flags for Acquisition Card/Credit Card Wrongdoing and Fraud

- **Multiple purchases are made at the same vendor or on the same day.** Goods are purchased for personal use, or purchases are split so that the cardholder does not go over his/ her transaction limit. Amounts are kept small to avoid inquiries into the purchases.
- **Purchases are made with an odd business vendor or it is unusual to use credit cards with a particular vendor.** This could indicate that purchases have been made for non-government purposes. For example, credit card purchases at a clothing store, stereo and electronics store, or furniture store would be odd. Also unusual would be a credit card purchase with a contractor who would not normally accept a credit card payment with commercial or government clients.
- **Receipts to support statement transactions are incomplete or non-existent.** Information about what was purchased is vague. This could indicate vendor abuse or purchases made for personal use.
- **Monthly acquisition card statements are not reviewed by auditors.** If card holders do not expect their purchases or monthly statements to be reviewed, the risk of fraud increases.
- **Cardholders make purchases on weekends, during their vacation time, or on special leave.** This could indicate purchases were personal, or that a retail merchant is billing the government for non-government purchases.
- **The cardholder has personal financial difficulties.** The risk of abuse can increase when a cardholder has a poor credit rating, has his or her wages garnisheed, or is involved in bankruptcy proceedings.

Description of How Expense Account Wrongdoing and Fraud May Occur

- **Personal expenses are submitted as business expenditures.** An employee submits personal expenses such as computer accessories, automobile fuel purchases, or personal meals as business expenses.
- **Expenses are submitted twice.** An employee is reimbursed more than once for the same expenses or items that have been purchased and paid for by the entity, and also claimed in an expense report or claim. For example, the government may prepay an expense such as an airline ticket. The ticket is changed and a new ticket is issued for a nominal charge; the employee submits the total charges of the revised airline ticket for reimbursement.
- **A claim for expenses that someone else paid for is submitted for reimbursement.** For example, three government employees share a taxi and all three submit the taxi fare on their expense reports. Or, a meal already paid for under a hospitality expense or conference is subsequently claimed by an employee as part of his/her daily meal allowance.
- **A false claim for automobile kilometre charges is submitted.** An employee submits a claim for automobile kilometres that is higher than the actual kilometres driven.
- **An invoice is submitted for an item that was returned for a refund.** For example, an employee submits a copy of the purchase invoice for a computer accessory, when a refund for the item was subsequently received.

Description of Red Flags for Expense Account Wrongdoing and Fraud

- **Expense receipts are missing.** This may indicate that the expense was not incurred.
- **Detailed expense receipts are missing.** Only a credit card slip is provided, without the corresponding detailed receipt.
- **Photocopied receipts or invoices are submitted**. This may indicate duplicate, altered, or fictitious invoices.
- **The date on a receipt is old or missing**. This may indicate that expenses were previously submitted.
- **An employee submits an expense report even though he or she has an entity credit card.** The entity pays for the employee's credit card expenses and the employee also submits an expense report for the same expenses.
- **Receipts do not match the employee's travel, plans, work schedule, or time sheets.** This may indicate fictitious receipts or personal expenses are being submitted for reimbursement. .
- **The purpose of the expense is not indicated.** This may indicate that the expense was not for business purposes.
- **Entity credit card statements are not checked against expense reports.** Checking statements against reports will highlight items that are claimed in an expense report and that may have already been paid for with an entity's credit card.
- **The expense report review process is inadequate.** If employees are aware of the inadequacy of the expense review process, the risk of fraud may be increased.
- **A T4A is not issued for taxable benefits.** An employee makes a false representation to his entity so that a T4A is not issued. For example, an employee may state that there is no personal use of the government automobile when in fact there is substantial personal use of the government automobile.
- **Code of Conduct or ethics policies are weak, do not exist, or are not enforced.** When senior management does not create, adhere to, or enforce appropriate policies, a poor example is provided to employees and can result in increased risks for wrongdoing and fraud.

Description of How Payroll and Personnel Wrongdoing and Fraud May Occur

- **Overtime abuse**—employees are responsible for approving their own overtime without supervisory oversight. Sometimes supervisors and employees collude in overtime abuse by splitting the overtime payments.
- **Overpayment**—an employee is paid at a higher rate of pay than he/she is entitled to and does not disclose the errors.
- **Annual leave cash out**—an employee cashes out his/her annual leave, even though he/she took leave throughout the year but did not submit leave notices. For example, travel claims may show personal leave being taken before or after business trips.
- **Severance pay**—an employee receives severance pay even though he/she is still working for a department, or is ineligible.
- **Ghost employees**—a fictitious employee is put on a department's payroll, and payments for that employee are deposited into the perpetrator's bank account or the account of one of his/her family members. With electronic payroll deposits, it is more difficult to uncover ghost employees.
- **Terminated employees are not deleted from the payroll system**—Payments continue to be made to terminated or retired employees, those who have resigned, or those who are on medical leave. Payroll payments are deposited into the perpetrator's bank account or the account of one of his/her family members.
- **Employment insurance fraud**—false records of employment are issued to an employee so that he/she can meet the eligibility requirements of the employment insurance program.
- **Staffing and classification abuse**—managers who are behaving inappropriately may gain the cooperation of their staff by reclassifying positions to higher salary levels or changing casual or term positions indeterminate positions.

Description of Red Flags For Payroll and Personnel Wrongdoing and Fraud

- **There is poor internal control of payroll and personnel functions.** Payroll and personnel wrongdoing and fraud require manipulation of the organizations systems. Control weaknesses, such as poor segregation of duties or poor controls on access to payroll systems, invite wrongdoing.
- **Senior officials cash-out vacation leave on a regular basis.** Because often no one questions senior officials' absences from the office, it is easy for unethical senior officials to take personal leave and request a cash-out of leave that has already been taken.
- **There is a high proportion of reclassifications upwards or other unusual trends in staffing actions.** Managers may use staffing actions to reward employees who tolerate inappropriate behaviour by management.
- **There are duplicate or illegitimate social insurance numbers.** When more than one employee uses the same social insurance number or the number is unacceptable, it could indicate ghost employees or employees who do not have income tax taken from their employment income.
- **There are duplicate addresses or deposit accounts.** Ghost employees may be indicated when more than one employee is using the same bank account for their payroll deposits, or when the same address is used for more than one employee.
- **Payroll amounts are missing basic deductions.** Ghost employees will often have no withholding taxes, insurance, or other normal deductions taken from their pay.
- **Notices are received from CRA that payroll taxes are delinquent.** Notices from the Canada Revenue Agency may be an indication that payroll deductions have been borrowed, even for a short period of time, prior to being remitted to the Canada Revenue Agency.
- **There is a high number of manually prepared cheques.** Where a payroll process is automated, manually prepared cheques may indicate fraud.

Description of Red Flags for Assets Theft

- **There is poor segregation of duties in asset management.** Poor segregation of duties provides opportunities to misappropriate assets or proceeds of sales of assets. Requisitions are not approved by someone other than the person making the requisition. Or, an employee responsible for asset disposal receives the proceeds of disposition.
- **The assets are not well monitored.** Inventory is not counted annually. Or, the inventory count is not well-supervised and verified. No one has been assigned responsibility for custody of assets.
- **Assets are delivered to questionable addresses.** The delivery address is different than the billing address on the invoice. Or, shipping documents indicate unusual movement of goods. This could indicate that goods are being moved to facilitate theft.
- **Write-offs of assets or sales are not well-controlled**. Writing-off inventory is one way of removing assets from the books so that their theft can be concealed. Or, the perpetrator of theft may record false sales transaction so that it appears missing goods have been sold.
- **Proper authorizations and valuations are not obtained for disposal of assets.** Authorizing the disposal of assets is one way of concealing their theft. Or the value of an asset for disposal may be significantly understated so that it can be sold to an accomplice of for far less than fair market value.

OAG Audit Policy on Wrongdoing and Fraud

This policy sets out general expectations for auditors of the Office of the Auditor General (OAG). The principles and practices are in addition to any professional auditing and assurance standards to which the OAG adheres. Due to the inherent limitations of an audit, the OAG recognizes that some risk remains that wrongdoing and fraud will not be detected. This policy will be incorporated in all corresponding audit manuals in the course of their next revisions.

General

1) Auditors should carry out their audits with an attitude of professional skepticism, recognizing that wrongdoing and fraud could exist.

2) During all audit stages, auditors should be aware of the indicators and the risks of wrongdoing and fraud within the entities being audited and in the areas or subject matters under audit in order to detect wrongdoing and fraud.

3) While conducting an audit, auditors should give proper consideration and take the necessary actions to appropriately deal with identified indicators and risks of wrongdoing and fraud. Auditors should document any facts and observations that confirm or dispel the concerns raised.

4) Auditors have a responsibility to be open and responsive to receiving disclosures or complaints of wrongdoing and fraud from management and employees of the entity and from other persons. The OAG will protect the identity of whistleblowers and complainants (within the limitations of the law) and will handle allegations or suspicions of wrongdoing and fraud with extreme care and confidentiality.

Attest Audits

5) As part of the process of obtaining sufficient knowledge of the entity's business, auditors should review management's assessment of the risk of wrongdoing and fraud, and how management responded to those risks. Auditors should also review how those charged with governance have discharged their oversight role in ensuring the adequacy of systems and practices to manage the risks of wrongdoing and fraud. During this process, auditors should make enquiries of management, the audit committee, and others concerning their knowledge of any actual, suspected, or alleged wrongdoing and fraud.

Reporting

6) Auditors shall report to the entity principal any suspicions of wrongdoing and fraud including any allegations received. Auditors shall also advise the entity principal of wrongdoing and fraud that the entity identified but failed to take sufficient and appropriate action. The entity principal shall take the necessary actions required to appropriately deal with the wrongdoing and fraud issues raised. The entity principal shall report to the entity's assistant auditor general and the principal of the Forensic Audit Section the inability to dispel reasonable suspicions of wrongdoing and fraud or where the entity has mishandled an identified instance of wrongdoing and fraud.

7) When auditors identify significant risks of wrongdoing and fraud in the entity's programs and operations, these risks should be brought to the attention of:

   - the entity principal and assistant auditor general ;
   - the principal of the Forensic Audit Section;
   - entity management, and those charged with oversight;
   - Parliament, if appropriate.

8) When the OAG has concluded after receiving an opinion from legal services that it has reasonable grounds to believe that significant wrongdoing or fraud has occurred, it shall report those matters to:

   - senior officials of the entity;
   - the audit committee or equivalent;
   - central government agencies and Parliament, when appropriate; and
   - the appropriate police authorities, when required.

Appendix 1—Glossary of Terms

Authorizations

All government expenditures must be authorized by Parliament, either through specific legislation or through appropriation acts. Many government activities also require Treasury Board approval of the terms and conditions under which the program will operate. All requests for payment must have signatures by those authorized to give the approvals required under Sections 33 and 34 of the Financial Administration Act

Bid-Rigging Schemes

Contract and procurement frauds that usually involve collusion between competing organizations during the bidding process. (See also "Price-fixing " on page 118) Bid-rigging also includes situations where the contracting organization puts restrictive conditions in the request for bids so as to unreasonably restrict competition.

Bribery

Giving or taking money or some other valuable item in order to influence a public official (any government employee) in the performance of his/her duties. Official bribery is also called corruption of a public official. Secret commissions refer to the corruption of private individuals for commercial or business advantage.

Conflict of interest

Having distinct and competing interests that may affect, or be perceived to affect, the independence and objectivity of the individual in carrying out his/her official duties.

Collusion

Where two persons or businesses enter into an agreement, usually secret, to defraud or gain an unfair advantage over competitors or the parties with whom they are negotiating.

Corruption

In the public sector, any act in which a public official or employee performs favours in exchange for money or other rewards.

Deception

The act of making someone believe what is false; to mislead purposely.

Due diligence

Using reasonable care and attention sufficient to avoid claims of negligence. In the context of audits, conducting the audit planning and examination work with the skill and attention expected of professional auditors.

Embezzlement

Misappropriating money or assets held in trust. This term applies only to persons who have been lawfully entrusted with the property of another party.

False representations

Stating as a matter of fact something that is known by the person who makes it to be false and is made with the intent that the person who hears it will act upon it.

Forensic Accounting

"Forensic" describes something that is used in or suitable to courts of law or public debate. Forensic accounting is a discipline that deals with the relationship and application of financial facts to legal issues and legal problems. Forensic accounting involves gathering evidence following accepted professional standards and procedures so that forensic accountants can give oral and documentary evidence in court that will be accepted by a court of law and will withstand cross-examination.

Forensic Auditing

Forensic auditing is the terminology used by the Office which describes audits undertaken by the Forensic Audit Section. Forensic auditing comprises investigations, auditing and forensic accounting. It requires combining the three disciplines in conducting the forensic audit. Forensic audits are undertaken with the assumption that the matter may end in civil or criminal proceedings.

Forgery

Creating a false document, altering a document or writing a false signature for the illegal benefit of the person making the forgery.

Fraud

For the purposes of this audit guidance, fraud is referred to as one or more intentional acts to deceive to obtain some unjust advantage. This includes serious wrongdoing such as:

- breach of trust,
- collusive awarding of grants and contributions,
- collusive bidding or awarding on contracts,
- deceit, and
- dishonest acts,
- false representation,
- fraudulent concealment,
- illegal acts of a similar nature,
- intentional misstatements,
- irregularities,
- kickbacks,
- secret commissions, and
- theft.

Only a court of law can conclusively determine if a fraud occurred.

The Canadian Institute of Chartered Accountants Handbook defines fraud as "an intentional act by one or more individuals among management, other employees, those charged with governance, or third parties, involving the use of deception to obtain an unjust or illegal advantage. Although fraud is a broad legal concept, the auditor is concerned with fraudulent acts that cause a material misstatement in the financial statements. Fraud involving one or more members of management or those charged with governance is referred to as management fraud; fraud involving only employees of the entity is referred to as employee fraud."

Fraudulently, for a fraudulent purpose, with intent to defraud.

Intentionally using deceit, trickery or some dishonest means to deprive another of money, property or legal rights. These words appear frequently in the Criminal Code. See "Canadian Legal Definition of Fraud" on page 30.

Fraudulent concealment

Knowingly concealing material information that is necessary and important for another party to know, for example when entering into the agreement or contract.

Kickbacks

Undisclosed payments by outsiders to employees of an organization, usually involving collusion between employees and vendors.

Lapping scheme

This scheme is used by an employee who steals cash or cheques received to cover up the theft. To avoid being detected, the employee posts B's payment to A's account, C's payment to B's account, etc. This process requires continuous manipulation and monitoring of many accounts and transactions

Misappropriation

Intentionally using another's money or property for one's own use or other unauthorized purpose. See also "Theft" on page 119.

Price-fixing

Secret agreements between competing businesses to set prices for their products, preventing real competition and keeping buyers of their products form benefiting from price competition.

Misrepresentation

Giving a false or misleading facts to obtain money, goods or benefits to which one is not entitled.

Red flags

Anomalies that point to symptoms or indicators that are known to be associated with wrongdoing and fraud. One of the keys to detecting wrongdoing and fraud is recognizing red flags.

Secret commissions

Giving or taking money or some other valuable item in order to influence private individuals for commercial or business advantage. In the public sector, trying to influence a public official (any government employee) in the performance of his/her duties is called bribery.

Wrongdoing

For the purposes of this audit guidance, wrongdoing refers to improper conduct and inappropriate activities such as:

- abusing or exceeding authority,

- conflicts of interest,
- gross administrative abuse,
- improper contract or contribution awards,
- intentional non-compliance with authorities,
- misuse of funds or assets, and
- unethical behaviour.

Wrongdoing does not include matters that are solely issues of economy, efficiency, effectiveness or environmental sustainability.

Theft

Taking the money or property of another without the knowledge and consent of the owner

Appendix 2—Offences under the Criminal Code, Financial Administration Act and Competition Act

Criminal Code

PART IV - OFFENCES AGAINST THE ADMINISTRATION OF LAW AND JUSTICE

Corruption and Disobedience

Sections 118 to 127 of the Criminal Code deal generally with corruption and disobedience of court orders. Sections 119 and 120 address bribery of judicial officers, members of Parliament or legislatures, and other officers employed in the administration of criminal law. Both offering a bribe and accepting a bribe are illegal.

Frauds on the Government

Section 121 of the Criminal Code prohibits a broad range of activities that can be described generally as frauds upon the government.

Government officials may not demand, accept or agree to accept any loan, reward, advantage or benefit, directly or indirectly, for themselves or any member of their family, without the written consent of their department head. It is also an offence for those having dealings with the government to give or offer to give an employee, government official, members of the official's family or a third party accepting on behalf of the official, any benefit or advantage in connection with any matter of business with the government unless the official has obtained written permission from the department head that they have dealings with. Section 121 also makes it an offence to give anything of value with the intent to influence in any way the result of an election.

Breach of Trust by a Public Officer

Section 122 makes it illegal for any official to commit fraud or breach of trust in connection with his or her duties as an official of the government, whether or not the fraud or breach of trust would be considered an offence if it were committed by an individual not employed by the government.

Selling or Purchasing Office

Section 124 makes it illegal to agree to sell or purchase a public office, to arrange the resignation from such office, or to arrange the appointment of a person to such office. No sale has to take place; the agreement to carry out one side of the transaction establishes the criminal liability.

Influencing or Negotiating Appointments or Dealing in Offices

Section 125 prohibits attempts to influence or negotiate appointments to or resignations from public offices by offering a direct or indirect reward, advantage, or benefit. Criminal liability applies to both the person offering and the person accepting the benefit.

Disobeying a Statute

Section 126 makes it illegal to contravene any federal Act by wilfully doing anything prohibited by the Act or failing to do anything required to be done by the Act. The section can be applied to a wide variety of situations covered by statute for which there are no specific penalties for violations.

Disobeying an Order of the Court

Section 127 makes it illegal to disobey an order of a court or other person or body established by legislation to give orders, if there is no other penalty specified for such disobedience. Orders to pay money are not included in this section.

Perjury—Criminal Code Section 131

Section 131 makes it illegal for anyone to make a false statement when that person is permitted, authorized, or required by law to make a statement by affidavit, by solemn declaration or deposition, or orally under oath, to a person authorized by law to take such an affidavit, declaration, or oath. The offence requires proof of several elements, including that the statement made must be false and that the accused must have known it was false. There must also be an intent to mislead. The offence may be committed by making a false statement in judicial proceedings or outside judicial proceedings.

PART IX - OFFENCES AGAINST RIGHTS OF PROPERTY

This Part describes many different forms of theft. It applies to offences committed against the government, in that it prohibits intentional and unauthorized taking or use of government property or records. It also prohibits receiving or concealing such property or records.

It should be noted, however, that these sections do not make it an offence to take "information" or "knowledge," no matter what the value of that information or knowledge may be. This means that conveying information verbally would not be classified as an offence. The distinguishing feature is that the theft is of an object or tangible thing. The only exception is that, if the information taken is deemed secret within the meaning of the *Official Secrets Act*, an offence under that Act may apply.

Theft

Section 322 describes and defines the general offence of theft. Section 330 describes the kind of theft committed by a person who is receives anything that requires him/her to account for or pay it to another person, and fraudulently fails to do so.

Misappropriation of Money Held Under Direction

Section 332 applies to any person who receives money or valuable security for the sale of real or personal property with direction that the money be applied to a specific purpose and fraudulently fails to do so.

Destroying Documents

Section 340 makes it illegal for a person to destroy, cancel, conceal or obliterate official documents for a fraudulent purpose.

Fraudulent Concealment

Section 341 describes the offence of fraudulent concealment. Every person who takes, obtains, removes, or conceals anything for a fraudulent purpose commits the offence.

False Pretence

Section 361 makes it an offence to make a false representation of a matter of fact, either present or past, orally or otherwise, where the representation is known by the person who makes it to be false, and where the representation is made with a fraudulent intent to induce the person to whom it is made to act upon it. It is not necessary to prove that the person to whom the statement was made was harmed by the false statement, or that a financial loss occurred, but only that the false statement was acted upon.

Section 362 sets out in detail the specific applications of false statements and false pretences that can be offences. These include obtaining credit or anything that can be stolen by false pretence or fraud.

Forgery and Offences Resembling Forgery

Every person who makes a false document, knowing it to be false, with the intent that it should be used by another person , believing it to be genuine, commits the offence of forgery. Making a false document includes altering a genuine document by adding material, changing the date, or erasing, obliterating or removing any part of it. Once the false document has been made the offence is complete, even if its maker does not intend any particular person should use or act on it as genuine.

Section 367 sets out the punishment for forgery. Section 368 makes it illegal to utter or use a forged document, with knowledge that the document is forged.

Section 374 applies to anyone who prepares a document in the name of or on behalf of another person without lawful authority and with intent to defraud commits the offence of drawing a document without authority. A person who knowingly makes use of such a document also commits the offence.

Section 375 applies to anyone who obtains anything by the use of a legal document such as a contract, knowing it is a forged document.

Section 378 makes it illegal for a person legally authorized to issue certified copies of or extracts from records or documents to do so falsely. It also prohibits unauthorized persons from fraudulently issuing documents as certified.

PART X - FRAUDULENT TRANSACTIONS RELATING TO CONTRACTS AND TRADE

Fraud

Section 380 makes it illegal for anyone to obtain property, money, or valuable security by deceit, falsehood, or other fraudulent means. To "defraud" someone is to deprive a person dishonestly of something which is his/hers or of something to which he/she is or might but for the fraud, be entitled.

Section 381 makes it an offence to use the mails to deliver letters or circulars that either describe schemes intended to deceive the public or that are to be used for the purpose of obtaining money under false pretences.

Falsification of Books and Documents

Section 397 makes it illegal to destroy, mutilate, alter, falsify, or omit any material, particularly in any record or document, with intent to defraud.

Section 398 applies to anyone who, with intent to deceive, falsifies an employment record by any means, including the punching of a time clock. This is a summary conviction offence, less serious than an indictable offence in terms of potential fines and/or imprisonment.

Under Section 399, an offence is committed when a person entrusted with public revenues knowingly makes a false statement of any sum or balance of money entrusted to or controlled by him/her.

Supplying Defective Stores to Her Majesty

Although rarely used in criminal proceedings, Section 418 makes it an offence to:

- sell or deliver defective stores (or goods) to the government or a government agent; and
- commit fraud in connection with the sale, lease, manufacture, or delivery of any stores to the government or a government agent.

In addition, this section holds directors, officers, agents, and employees of corporations accountable for the commission of these offences if they knowingly take part in the offence, or if they know or have reason to suspect that an offence is being committed or is about to be committed and do not inform an appropriate government official of this fact or suspicion. This provision therefore places the responsibility on every officer or employee of a corporation to inform the government about fraudulent activity that is either known or suspected to be occurring.

Secret Commissions

Offences under Section 426 of the Criminal Code include payments, advantages, or benefits of any kind that are made in return for actual or perceived advantages, benefits, or preferential treatment. In order for an act to be an offence under this section, it is not necessary that the secret commission actually be delivered but only that it be offered or demanded.

Conspiracy

Under Section 465, it is an offence for two or more persons to make any agreement to:

- defraud the government; or
- violate any federal law or regulation when at least one act is taken in furtherance of the agreement.

PART XXIII - SENTENCING

Under Section 750(3), any person convicted under sections 121, 124, or 418, of bribery, or other frauds against the government, shall not be permitted to legally contract with the government again, nor shall they be able to receive a benefit under a contract with the government, unless and until a pardon is issued.

Financial Administration Act

Section 80 of the *Financial Administration Act* (FAA) makes it a crime for any official or employee of the government who is working in any office connected with the collection, management, or disbursement of public money to commit or be involved in fraud, conspiracy to defraud, bribery, or false entries.

In most cases a government official or contractor who has committed an offence under this section of the FAA will also have committed a Criminal Code offence. Criminal Code offences are prosecuted by a provincial Crown attorney, whereas FAA offences are prosecuted by a Crown counsel appointed by the federal Attorney General. A government employee convicted under the Criminal Code would lose his or her employment and also receive a criminal record.

Competition Act

The *Competition Act* prohibits schemes such as collusive bidding, price-fixing, bid-rigging, and bid rotation. It applies equally to situations involving government-private sector contracts and non-government contracts. Investigations under this Act would normally be carried out by investigators from the Competition Bureau and would be prosecuted by the federal Attorney General.

Section 47 of the Act defines bid-rigging to mean agreements or arrangements among two or more competitors not to submit bids or to submit bids arrived at by an agreement or arrangement that the parties do not bring to the attention of the tendering agency.

Conviction under Criminal Code and Restrictions on Contracting with the Government—Criminal Code, Section 750

Section 750 of the Criminal Code provides that a person who holds an office under the Crown or public employment at the time he or she is convicted of an indictable (i.e. a more serious offence in terms of fines and imprisonment) offence and sentenced to two or more years' imprisonment, loses the office or the employment. Moreover, such a person is incapable of holding any office or other public employment until they have undergone the punishment imposed or received a pardon. They are also incapable of being elected or sitting as a member of Parliament or a legislature.

As discussed above, a person convicted of certain crimes of corruption or fraud against the Crown (sections 121, 124 or 418 of the Criminal Code) is disqualified from ever contracting with (directly or indirectly) or being employed by the Crown again, unless the Governor in Council grants a restoration of capacity.

Appendix 3—Data Mining to Detect Wrongdoing and Fraud

Data mining may be very helpful it identifying red flags in large databases. Data mining refers to using special computer software programs to search for red flags. Data mining software programs are designed to search large databases and report on identified items (hits) that may suggest irregularities or fraud. Auditors can use data mining software to identify red flags in large databases and between different databases that would probably never be uncovered otherwise. The auditor analyzes the report of hits for possible wrongdoing and fraud.

Computer programs can be designed to search or mine data and report on exceptions that may suggest wrongdoing and fraud. This appendix provides samples of data mining searches.

Payroll and Personnel

Payroll and personnel data mining may involve searching for:

- contract payments sent to the same addresses as employees;
- large payments made to employees;
- employee payments that differ from paycheque to paycheque;
- employee overtime patterns (and analyzing them);
- employee payroll payments that have no withholding taxes, employment insurance deductions, or other basic deductions;
- employees who have the same address;
- employees who have the same social insurance number;
- invalid social insurance numbers;
- employees who have the same bank account number; and
- matches of active payroll files with disability insurance, pension, or worker's compensation files.

Disbursements

Data mining of disbursements may involve searching for:

- duplicate payments (by same amount, supplier, dates);
- unusual payments to employees that are not made through normal payroll;

- payments made to a supplier who has the same address or phone number as an employee or another supplier;
- payments mailed to a post office box address;
- suppliers where employees are family members;
- contractors who were unsuccessful bidders but who are now subcontractors;
- supplier payments that were initiated or paid outside the usual system;
- disbursements in which no GST was charged;
- discovering sequentially numbered supplier/contractor invoices, which could indicate a phantom supplier; and
- transactions that are slightly below authority approval thresholds.

Revenue and Accounts Receivable

Data mining of revenue and accounts receivable may involve searching for:

- all write-offs, voids, refunds, and other credit receivable adjustments (and analyzing trends, similarities, or anomalies).

OTHER

Other types of data mining may involve:

- searching for duplicate addresses and phone numbers in different databases;
- identifying transactions that are odd as to time, frequency, places or amounts;
- identifying negative balances and transactions; and
- listing all manual payments.

Appendix 4—Weblinks

Institute of Internal Auditors, International Standards for the Professional Practice of Internal Auditing

http://www.theiia.org/iia/index.cfm?doc_id=1499

Financial Administration Act, Part X, Crown Corporations

http://laws.justice.gc.ca/en/f-11/58948.html

Criminal Code

http://laws.justice.gc.ca/en/C-46/index.html

Treasury Board Policies

Values and Ethics Code for the Public Service

http://publiservice.tbs-sct.gc.ca/pubs_pol/hrpubs/TB_851/vec-cve_e.asp

Policy on the Internal Disclosure of Information Concerning Wrongdoing in the Workplace

http://publiservice.tbs-sct.gc.ca/pubs_pol/hrpubs/TB_851/idicww-diicaft_e.asp

List of Senior Officers: Policy on the Internal Disclosure of Wrongdoing in the Workplace

http://publiservice.hrma-agrh.gc.ca/veo-bve/network_lists/agents_sup/list_seniors_idp_e.asp

Policy on Losses of Money and Offences and Other Illegal Acts Against the Crown

http://www.tbs-sct.gc.ca/Pubs_pol/dcgpubs/TBM_142/4-7_e.asp

Risk Management Policy

http://www.tbs-sct.gc.ca/Pubs_pol/dcgpubs/RiskManagement/riskmanagpol_e.asp

Checklist 1—Risk Assessment of the Entity for Wrongdoing and Fraud

For "Yes" answers, auditors should:

- determine the reasons for the Yes answer,
- assess the significance of any Yes answers, and
- assess the implication of several Yes answers and how they relate.

The auditor should consider undertaking additional work to clarify or resolve these warning signs or red flags.

Auditors can amend the questions or add questions as appropriate to reflect the uniqueness of the entity.

QUESTIONS	YES	NO	COMMENTS
1)Governance			
a) Is there inadequate review and oversight by governing bodies (e.g. Treasury Board, Public Service Commission)?			
b) Is there ineffective oversight of the entity by the audit committee? For example, is the audit committee financially illiterate, not well trained or inexperienced in the financial reporting process? Is the audit committee unable to influence the prevention and detection of financial fraud?			
c) Is there a lack of oversight of management by the board of directors, who are charged with governance?			
d) Is there a significant turnover of management, audit committee members, or members of the board?			
e) Is management unethical?			
f) Do you have reasons to be suspicious of management's integrity?			
g) Is there evidence that may indicate breaches of the organization's code of conduct or ethics policy?			
h) Does the organization have weak ethics practices?			
i) Does management show disregard for regulatory, legislative authorities or government policies?			
j) Does management communicate inappropriate values and ethics?			
k) Is management dominated by one individual or a small group without compensating controls such as effective oversight by those charged with governance?			

QUESTIONS	YES	NO	COMMENTS
2) Management Culture and General Environment a) Is a significant portion of management's compensation represented by bonuses or other incentives, the value of which is based financial results or operating results on achieving aggressive targets? b) Is management's compensation based on achieving aggressive targets? c) Does senior management frequently override internal controls? d) Does management fail to adequately correct internal control weaknesses in a timely manner? e) Does management inappropriately monitor significant controls? f) Does management use ineffective accounting and information technology? g) Is the internal audit function ineffective? h) Is the entity understaffed? i) Is there a high turnover in key financial positions? j) If the organization is decentralized, does management have insufficient oversight over the regions? k) Is there inadequate supervision or inadequate monitoring of remote locations? l) Is management reluctant to openly communicate with appropriate third parties, including regulators, members of Parliament, or the media? m) Is the senior full-time financial officer not involved in all key program decisions that affect the organisation's expenditures? n) Does management avoid control because of pressure to minimize public complaints (i.e. desire for service quality and avoidance of political complaints)? For example, does management focus on getting "the cheque out the door" rather than ensuring only eligible recipients get paid? o) Is it difficult to determine who is controlling the organization? p) Have any disclosures or complaints been received on inappropriate activities or behaviours?			
3) Entity's Financial Condition a) Is the organizational structure complex? For example, are there numerous or unusual legal entities, managerial lines of authority, or contractual arrangements? b) Are there any related party transactions that indicate business is not being done in the usual way? c) Are there any related party transactions that are not audited, or			

QUESTIONS	YES	NO	COMMENTS
that are audited by another auditor? d) Are there any unusual or complex transactions, especially close to year end, that pose difficult questions concerning substance over form? e) Are there any adverse consequences for significant pending transactions (e.g. a business combination or contract award)?			
4) Internal Controls a) Are internal controls insufficient and ineffective? b) Is there a lack of appropriate security screening of all employees before they are hired? (eg. key financial or managerial positions should have higher levels of security clearance) c) Is a record keeping system for assets inadequate or non-existent, such that assets are susceptible to misappropriation? d) Is there inappropriate segregation of duties or insufficient independent checks? e) Is there an inappropriate system in place to authorize and approve transactions? f) Are the physical safeguards that are in place insufficient for protecting cash, investments, inventory, or fixed assets? g) Is there a lack of mandatory vacations for all employees, especially those who perform key control functions. h) Have any transactions not been approved according to sections 33 and 34 of the *Financial Administration Act*? i) Are any transactions non-compliant with the appropriate authorities? j) Are transactions processed using unusual accounting procedures? k) Are records inadequate and incomplete? l) Are inadequate internal controls in place for computer processing? For example, is there a lot of processing errors or delays in processing results and reports? m) Is management reluctant to pursue over-payments or excessive write-offs for such accounts?			
5) Entity Co-operation Analysis or Unusual Observations a) Is the relationship between management and the OAG strained? b) Do auditors face unreasonable demands or constraints regarding the completion of the audit or the issuance of the auditor's report? c) Do auditors have restricted access to people and information, or are they limited in communicating effectively with those in			

QUESTIONS	YES	NO	COMMENTS
charge of corporate governance? d) Does management try to influence the scope of the auditors' work? e) Did the audit team identify important issues known by the entity but withheld from the auditors? f) Did management or any employees respond to your inquiries with conflicting or unsatisfactory evidence? g) Did you feel information was provided unwillingly or only after a significant delay? h) Is there evidence of payments to a company that a government employee has an interest (e.g. payments for contracts, grants, contributions)? i) Is there evidence that the organization was doing business with countries identified by international agencies as being prone to illegal or fraudulent activities? j) Is there evidence that management or employees are living a lavish lifestyle? k) Are there any tips or complaints identified by that organization's management, employees, customers, suppliers, or the public that wrongdoing or fraud are taking place?			
6. Other Questions			

Completed by:_____ Date:_____

Reviewed by:_____ Date:_____

Checklist 2—Risk Assessment for Possible Wrongdoing And Fraud in Transactions and Documents

For "Yes" answers, auditors should:

- determine the reasons for the Yes answer,
- assess the significance of any Yes answers, and
- assess the implication of several Yes answers and how they relate.

The auditor should consider undertaking additional work to clarify or resolve these warning signs or red flags.

Auditors can amend the questions or add questions as appropriate to reflect the uniqueness of the entity or the transactions and documents being examined.

QUESTIONS	YES	NO	COMMENTS
1) Access and questionable conduct a) Are there constraints by the entity that may impact on the sufficient review of transactions and documents by the auditor? b) Are auditors restricted to proper access to people or information, or limited in their ability to communicate effectively with respect to the transactions or documents? c) Did management or any employees respond to your inquiries with conflicting or unsatisfactory evidence? d) Did you feel information was provided unwillingly or only after a significant delay? e) Were there disclosures or complaints to the auditor from entity management, employees, customers or suppliers or the general public about wrongdoing and fraud with respect to specific transactions? f) Is there evidence, either observed by the auditors or documented, that management or the employees had breached its code of conduct or code of ethics?			
2) Entity's Financial Condition a) Are the organization's assets, liabilities, revenues, or expenses based on estimates that involve subjective judgments or uncertainties? For example, the ultimate collectibility of receivables, the timing of revenue recognition, the realizability of financial instruments based on subjective valuation of collateral or difficult to assess repayment sources, significant deferral of costs. b) Were there any significant related party transactions that			

QUESTIONS	YES	NO	COMMENTS
indicate business was not done in the usual way? c) Were there related party transactions that were not audited, or that were audited by another auditor? d) Were there any unusual or complex transactions, especially close to year end, that pose difficult questions concerning form over substance? e) Were there any bank account, subsidiary, or branch operations in other jurisdictions for which there appears to be no clear business justification? f) Are there unusual legal entities, managerial lines of authority, or contractual arrangements that do not appear to have a business purpose? g) Are there any adverse consequences for pending transactions (e.g. a business combination or contract award) if poor financial results are reported? h) Is the organization creating a financial reserve by large allowances?			
3) Record Keeping and Compliance a) Is there an inadequate record keeping system or no system for tracking assets that are susceptible to misappropriation? b) Is there an inappropriate system in place to authorize and approve transactions? c) Are the physical safeguards that are in place insufficient for protecting cash, investments, inventory, or fixed assets? d) Have any transactions not been approved according to sections 33 and 34 of the *Financial Administration Act* ? e) Have any transactions not obtained appropriate authorities? f) Are any transactions not in compliance with Treasury Board policies? g) Are transactions processed using unusual accounting procedures? h) Are records inadequate and incomplete? i) Is management reluctant to pursue over-payments or excessive write-offs ?			
4) Inadequate Documentation or Odd Transactions a) Is documentation missing or is the auditor unable to obtain original documents? b) Is there evidence of alterations and discrepancies in supporting documentation?			

QUESTIONS	YES	NO	COMMENTS
c) Is there conflicting evidence? d) Is there unusual evidence, such as handwritten alterations on documentation, or handwritten documentation that is usually electronically printed? e) Is there evidence of incorrect or revised versions of key documents? f) Is there evidence of incomplete, untimely or improperly recorded transactions? g) Are there any transactions that do not make sense? h) Is there evidence of unauthorized transactions or other adjustments? i) Is there evidence of payments to a company which a government employee has an interest in? (e.g. payments for contracts, grants, contributions? j) Are there unsupported transactions? k) Is there a significant number of figures in any accounts that are difficult to audit? l) Is there aggressive application of accounting principles? m) Are there unusual transactions in terms of their nature, volume or complexity, and did those transactions occur close to the year end? n) Is there evidence that transactions were not recorded? o) Is there evidence of significant, unreconciled differences between control accounts and subsidiary records, or between a physical count and the related account balance that were not properly investigated or corrected? p) Is there evidence of fewer confirmed responses than expected, or significant differences revealed by confirmed responses? q) Is there evidence of unreconciled suspense accounts? r) Are there any long, outstanding account receivable balances?			
5) Other Questions			

Completed by: :_____ Date:_____

Reviewed by :_____ **Date:**_____

Checklist 3— Red Flags for Computer and Internet Wrongdoing and Fraud

For "Yes" answers, auditors should:

- determine the reasons for the Yes answer,
- assess the significance of any Yes answers, and
- assess the implication of several Yes answers and how they relate.

The auditor should consider undertaking additional work to clarify or resolve these warning signs or red flags.

Auditors can amend the questions or add questions as appropriate to reflect the uniqueness of the entity.

QUESTIONS	YES	NO	COMMENTS
1. Is the organization's information technology security policy ineffective?			
2. Is the funding for information security inadequate?			
3. Is there no person or group responsible for computer and Internet security?			
4. Is the security training for the systems administrator and other technical personnel inadequate?			
5. Are security audits inadequate or not performed?			
6. Is the organization's physical security poor?			
7. Is the password security for computer or Internet access poor?			
8. Are the internal system controls poor?			
9. Is there no segregation of duties at the data centre? For example, do the duties for system programming and computer operations reside with one person?			
10. Are the procedures and controls for making changes to existing programs absent?			
11. Does access to computer programs and files extend beyond the needs of specified job duties?			
12. Are reviews of access logs inadequate or non-existent?			
13. Has management failed to take responsibility for the design and implementation of secure systems?			

QUESTIONS	YES	NO	COMMENTS
14. Has the organization failed to produce, review and resolve exception reports?			
15. Do any companies only deal with the government electronically?			
16. Are any companies using free e-mail addresses?			
Other Questions			

Completed by:_____ Date:_____

Reviewed by :_____ Date:_____

Checklist 4 – Screening Contracts for Possible Wrongdoing and Fraud

For "Yes" answers, auditors should:

- determine the reasons for the Yes answer,
- assess the significance of any Yes answers, and
- assess the implication of several Yes answers and how they relate.

The auditor should consider undertaking additional work to clarify or resolve these warning signs or red flags. Auditors can amend the questions or add questions as appropriate to reflect the uniqueness of the entity.

1. Stage 1 of the Contracting Process—Requirements Definition

QUESTIONS	YES	NO	COMMENTS
a) Was advice from technical experts missing in drawing up specifications for technical projects?			
b) Is there unusual involvement by a senior official?			
c) Did the contracting unit fail to determine if goods, services or information to be purchased were already owned?			
d) Was the needs analysis rushed?			
e) Has excessive stock been acquired?			
f) Is the information in files or the needs analysis for potential sources of materials only provided to the successful bidder?			
g) Has the replacement period for goods been shortened?			
h) Is surplus material that is in good operating condition being replaced?			
i) Are the requirements specifications too narrow?			
j) Is the consultant who helped develop the contract specifications also permitted to bid on the contract?			
k) Is there unusual involvement by a senior official?			
l) Is the needs analysis product oriented, rather than performance oriented?			
Other Questions			

2. Stage 2 of the Contracting Process—Acquisition, Bidding, and Selection

QUESTIONS	YES	NO	COMMENTS
a) Are the bid specifications unclear?			
b) Is there unusual involvement by a senior official?			
c) Is there a questionable relationship between the contractor and the government officials responsible for selecting the contractor?			
d) Has confidential information been released?			
e) Are there unusual bidding patterns?			
f) Are only a few bids submitted?			
g) Is the evaluation of a contractor inconsistent with the contractor's previous performance?			
h) Is the review of bids rushed?			
i) Does one person, rather than a panel, evaluate the bids?			
j) Are several small contracts issued sequentially to the same supplier?			
k) Are exceptions made to the tender deadline?			
l) Are bids changed after they are submitted?			
m) Are specifications changed after the contract is awarded but before it is signed?			
n) Does the request for proposal contain a mistake that invalidates the tender call or request for proposal?			
o) Is the lowest responsive bidder not selected?			
Other Questions			

2.1 Anti-Competition Activities:

QUESTIONS	YES	NO	COMMENTS
a) Does an analysis of bidders and contract awards indicate patterns?			
b) Is competition restricted by when and how the request for proposal/call for tenders is published?			
c) Do bids refer to industry-wide pricing practices?			
d) Is there any correspondence with contractors that suggests collusion?			
e) Are there any unusual withdrawals of tenders?			
f) Do any bids contain peculiar information?			
g) Does the successful contractor use any competitors as subcontractors?			
h) Are bid estimates higher than expected?			
i) Have related companies submitted individual bids?			
j) Is there a low number of bidders and only one qualified contractor because dummy bids were submitted?			k)
Other Questions			

2.2 Sole-Source Contracts

QUESTIONS	YES	NO	COMMENTS
a) Are contracts changed from competitive to non-competitive?			
b) Is the documentation used to justify sole-source contracting inadequate?			
c) Are contracts repeatedly awarded to the same contractor?			
d) Are standing orders used for large purchases?			
e) Are local purchase orders (LPOs) higher than the approved dollar limits?			
Other Questions			

3. Stage 3 of the Contracting Process—Administration, Performance, and Evaluation

3.1 Fixed-Cost Contracts

QUESTIONS	YES	NO	COMMENTS
a) Are there changes to a contract after it is awarded that result in substantially increased charges?			
b) Is a change order issued without an adequate explanation or as a result of circumstances that the contractor should have foreseen?			
c) Is the contract extended unexpectedly?			
d) Are there significant cost over-runs?			
e) Is the system for reviewing contractor invoices inadequate?			
f) Is the test certification documentation inadequate?			
g) Is the certification of contractor performance (required under section 34 of the *Financial Administration Act)* missing or incorrect?			
h) Are inspections or inspection reports missing or inadequate?			
i) Are there any complaints about the quality of deliverables?			
Other Questions			

3.2 Cost-Plus and Cost-Per Contracts

QUESTIONS	YES	NO	COMMENTS
a) Is the inspection process inadequate?			
b) Are the rates charged higher than those stipulated in the contracts?			
c) Are photocopies submitted to support charges?			
d) Is there evidence of double billing?			
e) Is the contractor identification on the invoice inadequate?			
f) Are there questionable invoice details?			
g) Are invoices lacking certification as being paid?			
h) Do the contractor's employees lack required skills?			
i) Do labour costs appear high?			
j) Do overtime charges seem unreasonable?			
k) Is quality assurance weak?			
l) Are incomplete cheques submitted as proof of payment?			
m) Does the timing of progress payment charges seem unrelated to plans?			
n) Are there claims for materials that were not purchased?			
Other Questions			

Completed by:_____ Date:_____

Reviewed by :_____ Date:_____

Checklist 5—Screening Grants and Contributions for Possible Wrongdoing and Fraud

For "Yes" answers, auditors should:

- determine the reasons for the Yes answer,
- assess the significance of any Yes answers, and
- assess the implication of several Yes answers and how they relate.

The auditor should consider undertaking additional work to clarify or resolve these warning signs or red flags.

Auditors can amend the questions or add questions as appropriate to reflect the uniqueness of the entity.

1. Stage 1, Grants and Contributions—Proposal, Application and Selection

QUESTIONS	YES	NO	COMMENTS
a) Is the recipient's application and justification for funding not on file?			
b) Are proposals or business plans vague?			
c) Is there reason to suspect a possible conflict of interest between a government employee and an applicant?			
d) Is the funding for a organization that has no previous financial history or a history of limited success?			
e) Is audited financial information on the recipient organization limited or unavailable?			
f) Does the recipient organization regularly receive funding under the program?			
g) Does the recipient organization barely meet the required eligibility criteria?			
h) Is matching funding provided by the recipient organization potentially misleading or incorrect?			
i) Does the proposal make claims that cannot be supported?			
Other Questions			

2. Stage 2, Grants and Contributions—Establishing the Agreement and Initiating Funding

QUESTIONS	YES	NO	COMMENTS
a) Are the term of the agreement vague?			
b) Do certain terms and conditions unreasonably favour the recipient and broaden the scope of permitted expenditures?			
c) Is the name and address of the applicant on the initial funding application different from those on the contribution?			
Other Questions			

3. Stage 3, Grants and Contributions—Reporting and Monitoring Compliance With Terms and Conditions

QUESTIONS	YES	NO	COMMENTS
a) Have complaints been received from users about the recipient's services?			
b) Have subcontractors or suppliers complained that they are not being paid?			
c) Is the department's monitoring of contribution agreements inadequate?			
d) Do the recipient's performance reports appear exaggerated or inconsistent?			
e) Did the recipient become insolvent or bankrupt shortly after receiving government funding?			
f) Has most of the funding been spent but the purpose of the agreement is far from achieved?			
g) Does the valuation of in-kind matching funding appear unreasonable?			
h) Does matching funding provided by third parties differ from the amount expected?			
i) Are payments made without sufficient verification that the work has been performed?			
j) Has an adverse event suddenly brought into question the success of			

the project?			
Other Questions			

4. Stage 4, Grants and Contributions—Post-Agreement Reviews and Subsequent Events

QUESTIONS	YES	NO	COMMENTS
a) Is the project described in the final report different than the one described in the original agreement?			
b) Have specific requirements of the contribution agreement not been met?			
c) Are approvals for expenditures missing or made by unauthorized individuals?			
d) Are approvals for changes to the original agreement missing or made by unauthorized individuals?			
e) Have changes and/or expenditures been made without the Treasury Board approval, where required?			
f) Are the total actual costs significantly over budget, under budget or very near the original budget?			
g) Is the final report significantly delayed or lacking critical information?			
h) Are there repayments owed to the government that have not been recovered?			
i) Was the final payment made before all the terms and conditions of the agreement had been met?			
Other Questions			

Completed by:_____ Date:_____

Reviewed by :_____ Date:_____

Checklist 6—Screening Non-Tax Revenues for Possible Wrongdoing and Fraud

For "Yes" answers, auditors should:

- determine the reasons for the Yes answer,
- assess the significance of any Yes answers, and
- assess the implication of several Yes answers and how they relate.

The auditor should consider undertaking additional work to clarify or resolve these warning signs or red flags.

Auditors can amend the questions or add questions as appropriate to reflect the uniqueness of the entity.

QUESTIONS	YES	NO	COMMENTS
1. Are there transactions that do not have appropriate approvals?			
2. Are there transactions where there is unusual involvement of senior officials?			
3. Are there any reasons to suspect a questionable arm's length relationship between an employee and an organization doing business with the government?			
4. Are there any unusual trends in revenues that are not explained by market conditions?			
5. Are there differences between federal and provincial revenues earned for lumber and mineral rights from similar packages of land?			
6. Are only a few bids received on surplus Crown lands which have good marketable value?			
7. Are Crown assets sold as surplus replaced soon afterward?			
8. Is the lead time for disposing of Crown assets very short?			
9. Is there little or no advertising of the disposal of Crown assets?			
10. Are surplus Crown assets resold by the purchaser within a short period of time?			
11. Are fees charged less than fair market value?			
12. Are there differences between postings to accounts receivable and bank deposits?			

13. Is there poor segregation of duties for accounts receivable?			
14. Are accounts that are not in arrears sent to collection agencies?			
15. Are there problems reconciling the accounts receivable ledger with the control account?			
16. Is there a history of poor collection of accounts receivable?			
17. Are there unexpected changes to accounts receivable balances?			
18. Are any accounts receivable write-offs missing proper approvals?			
19. Are there any unusual write-offs of accounts receivable?			
Other Questions			

Completed by:_____ Date:_____

Reviewed by :_____ Date:_____

Checklist 7—Screening Acquisition Cards/Credit Cards for Wrongdoing and Fraud

For "Yes" answers, auditors should:

- determine the reasons for the Yes answer,
- assess the significance of any Yes answers, and
- assess the implication of several Yes answers and how they relate.

The auditor should consider undertaking additional work to clarify or resolve these warning signs or red flags.

Auditors can amend the questions or add questions as appropriate to reflect the uniqueness of the entity.

QUESTIONS	YES	NO	COMMENTS
1. Are multiple purchases made at the same vendor on the same day?			
2. Are purchases made with an odd business vendor or with a vendor where credit cards are not normally used?			
3. Are receipts supporting statement transactions incomplete or non-existent?			
4. Is there a lack of monthly review of acquisition card statements by auditors?			
5. Do cardholders make purchases on weekends, during their vacation time or on special leave?			
6. Is there any evidence that a cardholder has personal financial difficulties?			
Other Questions			

Completed by:_____ Date:_____

Reviewed by :_____ Date:_____

Checklist 8—Screening Expense Accounts for Wrongdoing and Fraud

For "Yes" answers, auditors should:

- determine the reasons for the Yes answer,
- assess the significance of any Yes answers, and
- assess the implication of several Yes answers and how they relate.

The auditor should consider undertaking additional work to clarify or resolve these warning signs or red flags.

Auditors can amend the questions or add questions as appropriate to reflect the uniqueness of the entity.

QUESTIONS	YES	NO	COMMENTS
1. Are expense receipts missing?			
2. Are detailed receipts missing (i.e. only credit card slips were submitted)?			
3. Are photocopies of receipts submitted rather than originals?			
4. Are receipt dates old or missing?			
5. Does the employee submitting the expense report have an entity credit card?			
6. Are there discrepancies between dates of travel receipts and the employee's travel, work schedule, or timesheets?			
7. Is the purpose of the expense not indicated?			
8. Are credit card statements and expense reports not compared?			
9. Is the expense report review process inadequate?			
10. Is no T4A issued for taxable benefits?			
11. Are the Code of Conduct or ethics policies weak, non-existent or not enforced?			
Other Questions			

Completed by:_____ Date:_____

Reviewed by :_____ Date:_____

Checklist 9—Screening Payroll and Personnel for Wrongdoing and Fraud

For "Yes" answers, auditors should:

- determine the reasons for the Yes answer,
- assess the significance of any Yes answers, and
- assess the implication of several Yes answers and how they relate.

The auditor should consider undertaking additional work to clarify or resolve these warning signs or red flags.

Auditors can amend the questions or add questions as appropriate to reflect the uniqueness of the entity.

QUESTIONS	YES	NO	COMMENTS
1. Is there poor internal control of payroll and personnel functions? For example, is there a lack of segregation of duties for payroll functions such as authorization for additions or deletions to payroll records?			
2. Do senior officials cash-out vacation leave on a regular basis?			
3. Are there any illegitimate or duplicate social insurance numbers?			
4. Is there a high proportion of reclassifications upwards or other unusual trends in staffing actions?			
5. Are there any duplicate addresses or deposit accounts for employees?			
6. Are basic deductions missing from any payroll cheques?			
7. Are there notices from the Canada Revenue Agency that payroll tax notices are delinquent?			
8. Are there a large number of manual payroll cheques?			
Other Questions			

Completed by:_____ Date:_____

Reviewed by :_____ Date:_____

Checklist 10—Screening Assets Management for Wrongdoing and Fraud

For "Yes" answers, auditors should:

- determine the reasons for the Yes answer,
- assess the significance of any Yes answers, and
- assess the implication of several Yes answers and how they relate.

The auditor should consider undertaking additional work to clarify or resolve these warning signs or red flags.

Auditors can amend the questions or add questions as appropriate to reflect the uniqueness of the entity.

QUESTIONS	YES	NO	COMMENTS
1. Is there poor segregation of duties related to asset management?			
2. Is the monitoring of assets inadequate? For example, is there inadequate supervision or verification of inventory counts?			
3. Are assets delivered to questionable addresses?			
4. Are write-offs of assets or sales poorly controlled?			
5. Are authorizations and valuations for the disposal of assets questionable?			
Other Questions			

Completed by:_____ Date:_____

Reviewed by :_____ Date:_____