Recipients Guide on Best Practices for Internal Controls and Fraud Prevention

January 2021

PURPOSE

A key expectation for recipients that receive funding via contribution agreements from Immigration, Refugees and Citizenship Canada (IRCC) is to have a strong internal control framework and mechanisms in place to ensure accountability and good value for money. In addition to Internal Controls, recipients must be aware of potential banking and money fraud schemes targeted towards them. The purpose of this guide is to provide a general overview of internal controls and fraud prevention that can assist a funding recipient and its management with the development and implementation of an effective system of internal controls while understanding different aspects of fraud prevention. In fulfilling this responsibility, management should seek the assistance of both internal financial experts such as the accountant/bookkeeper and external experts such as the audit firm hired to conduct the annual audit of financial statements.

WHAT IS INTERNAL CONTROL?

Internal control is the framework of processes used to ensure an organisation's business is conducted in an orderly and efficient manner; its assets and resources are safeguarded; errors, fraud, and theft are prevented/detected; the accounting data is complete and accurate; financial and management information is reliable and timely; and policies and plans are followed.

The CPA Canada Handbook - Assurance defines internal control as:

> *The process designed, implemented and maintained by those charged with governance, management and other personnel to provide reasonable assurance about the achievement of an entity's objectives with regard to reliability of financial reporting, effectiveness and efficiency of operations, and compliance with applicable laws and regulations. The term "controls" refers to any aspects of one or more of the components of internal control.*

There are five components of internal control that must be present in order for an organisation to establish an effective internal control framework. These are:

- ***Control environment:*** the tone at the top and commitment by senior management and those in governance roles to promote internal control through effective leadership and an environment of honesty and ethical behaviour;
- ***Control activities:*** the establishment of policies and procedures to ensure control directives are properly implemented;
- ***Information, communication and related processes*:** ensure components of internal control are implemented and communicated to those employees, management, those in governance roles, and relevant external parties;
- ***Monitoring of controls:*** assesses how established internal control processes and procedures are monitored and corrective actions undertaken; and
- ***Risk assessment process:*** processes which assist management in understanding relevant risks, including identification, estimation of impact, likelihood of occurrence, and determination of responses to various types of risks associated with day to day functioning of the organisation.

To summarise, internal controls are required to manage business risks that could jeopardise achievement of the organisation's objectives.

Implementation of an Internal Control System

There are a multitude of controls and several ways of implementing them depending on the size, capacity and complexity of the organisation. The organisation has the sole responsibility for defining and implementing internal controls in an effort to mitigate identified risks. In larger organisations, an internal audit position and/or committee may exist. In cases of not-for-profit organisations (NPOs), the Board of Directors may assume this role. In addition to having internal controls in place, management is also responsible for testing these controls to ensure they are working properly and to make changes to processes as deemed necessary.

Essentially, management establishes an internal control system and ensures the:

- day-to-day operations of the entity follow established controls;
- organisation's assets are safeguarded;
- accuracy and reliability of information contained in the accounting records, financial reports and annual financial statements; and
- compliance with relevant regulations and legislation.

Most internal controls can be classified as preventive or detective, which are further described below.

Preventive controls are designed to prevent errors or irregularities from occurring. They are proactive and can include some of the following (not an exhaustive list):

- **Segregation of Duties:** duties are segregated among different people to reduce the risk of error or inappropriate action. Ideally, responsibilities for authorising transactions (approval), recording transactions (accounting) and handling the related payment (custody) are segregated.

- **Approvals, authorisations, and verifications:** management authorises employees to perform specific activities and execute transactions within limited parameters. In addition, management specifies activities or transactions that need supervisory approval before they are performed or executed by employees.

- **Safeguarding of assets:** providing only authorised employees with access, ensuring capital assets cannot be easily removed, etc.

- **Documentation:** Adequate documentation and record retention practices are clearly established. Cost allocation models are established, and well supported by reasonable methodologies, and there is a documented process in place for adjusting allocations.

Detective Controls are designed to detect and correct errors and irregularities after they have occurred. Examples of detective controls are (not an exhaustive list):

- **Reconciliations:** An employee compares various sets of data, identifies and investigates differences, and takes corrective action, when necessary. The following are usually subject to reconciliation with other sources to ensure completeness and accuracy:
    - Bank/Credit card statements (compared with General Ledger (G/L) accounts, proof of payment, transaction records), and
    - Petty cash fund (verified against receipts, G/L accounts).

  Reconciliations should be approved at a senior level on a regular basis

- **Physical inventory counts:** Periodic inventory counts substantiate the existence of assets as reported on the financial statements and other records and

- **Reviews:** Spot checks, variance analyses, and other analyses can be performed by management (over process, transactions, employee attendance records, etc.), while external firms may be engaged to conduct audits or reviews

One of the main objectives of internal control systems is to ensure that policies, regulations and legislation are followed and applied as intended. It is important that sound internal policies, guidelines and procedures are established and adhered to. Examples of internal policies, guidelines and procedures may cover the following areas (not an exhaustive list):

- Human resources (hiring and termination of employees, employee leave and benefits),
- Delegation of powers/authorities (over transactions and assets),
- Values and ethics,
- Key accounting areas (such as accounts payable/receivable, bad debts allowance, write-offs),
- Contracting,
- Information Technology and telecom usage,
- Collection, use, protection, and retention of personal information, and
- Whistleblower policies

Benefits of an Effective Internal Control System

There are many benefits to having a well-established and effective internal control system. Overall, organisations tend to run more efficiently when there are strong internal controls in place, as everyone is aware of their responsibilities and processes tend to involve multiple individuals at various levels. Detection of errors and fraudulent activity may occur earlier in the process and can be resolved before escalating into larger issues that could have greater adverse impacts on the organisation, including its reputation. Management, as well as outside firms, such as auditors, will have more confidence in a financial system with a strong internal control system in place.

Additionally, internal controls can be used to protect employees and management at all levels. By establishing clear policies, guidelines and procedures, controls outline responsibilities and authorities for everyone in the organisation, thereby assisting management to attain organisational goals.

Key Features of Efficient Internal Control Systems

The following is a list of key internal controls, their features and best practices. Although not exhaustive, it covers many of the controls an organisation may use to attain its objectives. Not all of these controls need to be present; however, existing controls should be aligned with the organisation's processes.

1- **Segregation of duties:** No one person should have responsibility for the recording and processing of a complete transaction. Having several people involved reduces the risk of accidental errors or intentional manipulation and increases the overall accuracy of operational and financial information. Functions that should be separated include authorisation, execution, custody, recording and in the case of a computerised accounting system, processing and reconciliations. Some tasks could be combined in small-size organisations, however, additional controls such as pre-approvals, frequent reviews and reconciliations should be in place as a compensating measure. By having duties segregated, this reduces the risk of processing errors, misappropriations, collusion and fraud.

2- **Authorisations and approvals:** The organisation has clearly defined financial authorisation and approval levels for specific positions to guide employees in handling financial transactions. Organisations often establish thresholds of financial authorisation, requiring more progressive levels of approval (i.e. at senior level) as transactions increase in size.

   For instance, an organisation may have established a procurement and signing authority's policy, which clearly defines the levels of authority. In such a scenario, a manager may have an approval limit of $5,000, while a CEO may have one of $15,000. Transactions over $15,000 may require the signature of at least one director. Such a policy should clearly outline who has payment authority, who can sign/approve payments on behalf of the organisation, and how many signatures are required for various types of payments.

3- **Safeguarding of assets:** This concerns physical custody of assets and includes procedures designed to limit access to authorised personnel only. For example, petty cash and credit cards should be kept in secure environments, with access limited to designated employees only.

4- **Staffing processes and procedures:** Organisations have clearly defined hiring practices supported by policy, which ensure all processes and procedures are impartial and result in hiring the most qualified individual for the position. Management must ensure that individuals performing the work have the skills and capacity for the position. Also, it is the responsibility of management to provide employees with appropriate monitoring and training to carry out their roles successfully. Generally, a human resources policy or equivalent will describe measures the organisation takes to successfully achieve this.

5- **Contracting processes and procedures**: There are clearly defined contracting practices that are fair and ensure value for money. As a general rule, organisations obtain multiple quotes for all major purchases, and the decision of which vendor to select should involve senior management. Additionally, organisations as a rule maintain copies of contracts on file for reference, as well as monitoring and audit purposes. It is recommended that organisations establish a policy on

contracting processes, which ensures staff know what steps must be completed to ensure integrity and value for money.

6- **Data Integrity:** Controls must be in place to ensure all transactions are recorded using proper coding and cost allocations. These controls include but are not limited to:
    - Arithmetic and accounting controls in the recording of financial data to ensure the recorded/processed transactions are:
        - complete,
        - recorded correctly and accurately, and
        - processed in a timely manner.

    - Management controls are exercised by management outside of day-to-day routine practices:
        - overall supervisory controls and spot checks,
        - ensure all data is appropriately backed up,
        - review of accounts and other financial reports (variances, general ledger, trial balance) and
        - budget comparisons and forecasting.

7- **Reconciliations:** There is a process in place to reconcile information between different sources that is understood and followed. Reconciliations can be either paper based or electronic and as a general rule, should be performed at least monthly. Once completed, a reconciliation should be reviewed and approved by someone other than the person who prepared the document. Reconciliations provide management with documented evidence that the general ledger account balances are accurate, valid, and approved. Regular reconciliations will uncover accounting errors, omissions, and misclassification of costs in a timely fashion. This will assist IRCC representatives to easily reconcile claims to the general ledger and supporting documentation.

WHAT IS BANKING/FINANCIAL FRAUD?

As our world has moved into more of a digital age, this has shifted the concept of theft or fraud from in person to now taking a digital form. While going digital offers security, certain individuals and organizations - either foreign or domestic - will seek to exploit weaknesses in an individual's or organization's internet and financial security, and will ultimately attempt to steal whatever money or financial information they can.

KEY EXAMPLES OF BANKING/FINANCIAL FRAUD

As a recipient of funding from governments, charities, other 3rd party organizations, etc. these attempts may be frequent and well-orchestrated. Below are a few ways to prevent yourself from being a victim of fraud, and what to look out for:

- **Phishing attempts:** Fraudsters can use very clever and legit-seeming emails or text messages to impersonate banks, financial situations, government agencies, communication providers or other companies to lure potential victims into providing personal or financial information. Included in these forms of communication may include a link requesting the potential victim to

click, resulting in a redirect to a fraudulent website. Also, the requested information may include usernames, passwords, credit/debit card numbers, PINs and other sensitive data that can be used to commit financial crimes.

- **Fake Service Provider:** Fraudsters may call or email posing as an employee of a well-known technology company such as Microsoft, Windows, Apple, Oracle, Sage, etc. - potentially one an individual or organization already uses. They will claim the individual's computer has been "hacked" or "compromised" and will request a fee payable by credit card or bank account in order to "fix" the issue. This effectively allows the fraudster to gain access to not only the individual credit card/bank account, but may allow malicious programs to be installed on the computer to steal further information.
- **Extortion:** One of the more current scams taking place is individuals calling identifying themselves from the collections division or legal department of Canada Revenue Agency. They will also follow statement with a demand for payment, and failure to do so will result in additional fines and/or jail time. It is important to remember CRA will never call an individual for this information.
- **Posing as a Bank Investigator:** Clients of a bank or financial situation may be contacted by someone posing as an investigator requesting help to catch a bank employee who has apparently stolen money. The fraudster will tell the potential victim to visit their local bank and withdraw funds without any reason under the guidance the teller may be involved in the made-up scam. The victim is then told to meet the fraudster to exchange these funds, or make a wire transfer via Western Union.
- **Fake Loans:** Sometimes customers when seeking loans will see offers posted on websites or other advertising resembling a reputable financial institution. Once the victim has submitted their information to this fraudulent company, it may be too late and the information has been compromised.

Fraud Prevention Tips

- If you receive an e-mail request for sensitive information from what looks like a valid source / contact, do a second level verification of these requests with a direct phone call to your contact
- Shred and dispose or destroy of all personal and financial documents – receipts, credit card statements/offers, bills after a designated retention period
- Keep personal and financial documents in a secure location
- Review on a regular basis financial statements to ensure there are no irregularities
- Never provide personal or banking account information over the phone, unless the call was initiated by you
- Never click on links in an email received from unknown senders

Fraud Prevention - Further Resources

Canadian Anti-Fraud Centre (CAFC): https://www.antifraudcentre-centreantifraude.ca/index-eng.htm

- Managed by the Royal Canadian Mounted Police (RCMP), Competition Bureau Canada, and Ontario Provincial Police (OPP)

Financial Institutions:

Scotiabank: https://www.scotiabank.com/ca/en/personal/advice-plus/features/posts.how-to-protect-yourself-from-financial-fraud.html

TD Canada Trust: https://www.td.com/privacy-and-security/privacy-and-security/how-you-can-protect-yourself/preventing-fraud/preventing-fraud.jsp

CIBC: https://www.cibc.com/en/privacy-security/banking-fraud.html

Royal Bank of Canada – RBC: https://www.rbc.com/cyber-security/how-rbc-keeps-you-safe/index.html

Bank of Montreal – BMO: https://www.bmo.com/main/personal/ways-to-bank/security-centre/

Section 7.0 - Contribution Agreement: Privacy and Security Obligations

CONCLUSION

It is the responsibility of an organisation's management to implement an effective internal control framework that will provide reasonable assurance that operations are efficient and effective; financial information is accurate; and the organisation is in compliance with applicable laws and regulations. When a weakness is identified in a control, management must assess the risks associated with the weakness and either take additional steps to enhance the controls or document its rationale for accepting the associated risk. IRCC requires that funding recipients have effective internal controls over the management of contribution agreements.