Managing the Risk of Fraud

A Good Practice Guide

Office of the Auditor General
CAYMAN ISLANDS

To help the public service spend wisely

TABLE OF CONTENTS

WHY IS UNDERSTANDING AND ADDRESSING THE RISK OF FRAUD IMPORTANT

SOME FACTS AND FIGURES

1. According to the Association of Certified Fraud Examiner's (ACFE) in its 2014 *"Report to the Nations on Occupational Fraud and Abuse"* organizations around the world lose an estimated 5 percent of their annual revenues to fraud, including corruption. If applied to the 2013 estimated Gross World Product, this translates to a potential projected global fraud loss of nearly US$3.7 trillion. Within this the Government sector is one of the three main victims of fraud and corruption, along with the financial services and manufacturing sectors. Exhibit 1 provides a number of other valuable insights about the cost and impact of fraud from the ACFE's global survey.

Exhibit 1 – Cost and impact of fraud from the ACFE's global survey

The median loss per fraud case was US$145,000, and more than a fifth of the cases involved losses of at least US$1 million

The median duration — the amount of time from when the fraud commenced until it was detected — for the fraud cases reported was 18 months

The higher the perpetrator's level of authority, the greater fraud losses tend to be. Owners/executives only accounted for 19% of all cases, but they caused a median loss of $500,000. Employees, conversely, committed 42% of occupational frauds but only caused a median loss of $75,000. Managers ranked in the middle, committing 36% of frauds with a median loss of $130,000

Small organizations (<100 staff) tend to suffer disproportionately large losses due to occupational fraud, with certain categories of fraud being much more prominent at small entities

Collusion helps employees evade independent checks and other anti-fraud controls, enabling them to steal larger amounts. The median loss in a fraud committed by a single person was $80,000, but as the number of perpetrators increased, losses rose dramatically. In cases with two perpetrators the median loss was $200,000, for three perpetrators it was $355,000 and when four or more perpetrators were involved the median loss exceeded $500,000

The presence of anti-fraud controls is associated with reduced fraud losses and shorter fraud duration. Fraud schemes that occurred at victim organizations that had implemented any of several common anti-fraud controls were significantly less costly and were detected much more quickly than frauds at organizations lacking these controls

Employees accounted for nearly half of all tips that led to the discovery of fraud

Most occupational fraudsters exhibit certain behavioral traits that can be warning signs of their crimes, such as living beyond their means or having unusually close associations with vendors or customers.

Tips are consistently and by far the most common detection method. Over 40% of all cases reported were detected by a tip — more than twice the rate of any other detection method.

Organizations with hotlines were much more likely to catch fraud by a tip. These organizations also experienced frauds that were 41% less costly, and they detected frauds 50% more quickly.

The vast majority of occupational fraudsters are first-time offenders; only 5% had been convicted of a fraud-related offense prior to committing the crimes. Furthermore, 82% of fraudsters had never previously been punished or terminated by an employer for fraud-related conduct

2. As a result of the study, the ACFE concluded that occupational fraud is a universal problem for businesses, including governments, around the globe.

3. The ACFE also reported a significant portion of organisations are overlooking many of the most effective anti-fraud controls. Proactive detection measures — such as hotlines, management review procedures, internal audits and employee monitoring mechanisms — that are vital in catching frauds early and limiting their losses. They highlighted that many organisations placed too much reliance on passive detection methods (confession, notification by law enforcement, external audit and by accident) which tend to take longer to bring fraud to management's attention, and thus allow the related losses to grow.

4. They also highlight small organisations (less than 100 employees) are both disproportionately victimized by fraud and notably under-protected by anti-fraud controls, a combination that makes them significantly vulnerable to this threat. Two key factors contribute to this:

    - organizations with small staffs often lack basic accounting controls; and
    - there tends to be a greater degree of trust among co-workers in small businesses.

5. In the United Kingdom the National Fraud Authority estimated that fraud in the public sector was around 20 billion pounds and in 2013 the White House Office of Budget Management estimated that the federal government lost US$106 billion due to fraud. Other studies provide estimates of fraud and corruption of up to 10% and highlight countries where it is estimated to reach 25% of GDP.

TYPES OF FRAUD

6. Fraud occurs in many forms. For many organizations internal fraud committed by employees is a risk that they need to manage effectively. Examples of internal fraud include: **misappropriating assets** – for example, stealing inventory, not recording all sales, setting up fictitious employees on the payroll, setting up false suppliers or shell companies, falsifying expense claims, or using business credit cards inappropriately; or **making fraudulent statements or claims** – for example, falsifying academic or training credentials or "cooking" financial records (such as creating fictitious revenues or concealing expenses).

7. Internal frauds are a big issue for organisations and are usually triggered by one of four situations:

   - **Opportunistic crime**: employees commit fraud for their own benefit. This may be entirely opportunistic or carefully planned. There are likely to be a number of possible motives.
   - **Lack of a corporate ethic**: in some organisations low-level fraud, such as the inflation of expenses claims, may appear to be condoned by both employer and employee.
   - **The recruited criminal:** some individuals seek employment (often in the financial sector) with the deliberate intention of defrauding their employer or gathering intellectual property.
   - **Employee intimidation:** organised crime groups are increasingly involved in the intimidation of staff to directly participate in frauds or to provide information on customer accounts or internal procedures in order to assist other attempts. A common threat is the harming of family and friends. Employees who have succumbed to an approach from a third party, provided information and accepted a fee in return often feel they have been 'bought for life'.

8. External fraud can be committed by outside parties such as contractors or suppliers misappropriating an organization's assets, through billing for services not provided and falsifying eligibility for claims. Fraud can also occur if an employee colludes with a party outside the organisation. This can lead to corruption-related fraud, such as conflict of interest schemes and kickbacks.

CAYMAN PUBLIC SECTOR

9. There is no clear gauge for determining the level of fraud and corruption in the Cayman Islands public sector. There is no national collection of data on instances of fraud and corruption, or potentially fraudulent losses. There are no requirements for the fraud reporting as part of the public financial management regime, except for duties to report fraud to law enforcement. However it is clear that instances do occur as they do in all jurisdictions.

10. In the theory of fraud and corruption there is little that entities can do to directly mitigate an individual's motivation or rationalization for undertaking fraudulent or corrupt acts. The one area that entities can influence though is the opportunity that individuals have to commit fraud or corruption through building an anti-fraud culture and putting in place the systems and controls for prevention and detection.

11. In our performance and financial audits we have highlighted on numerous occasions weaknesses in the management frameworks which heightened the risk of the misuse of public funds. In our financial audits we have particularly reported on the challenges around the internal control environment and systems in many entities, that leave entities exposed to the risk of invalid or inappropriate transactions being processed. For example we have identified: weaknesses in computer and manual systems not enforcing appropriate segregation of duties and approval processes; override of controls in place; and limited or little monitoring by management. We have also reported on issues around governance, risk management and ethics, all of which increase the risk of fraud and misuse of public funds.

12. It is not the primary function of external auditors to identify and investigate instances of fraud and corruption. However, as public sector auditors we have a significant public interest role in ensuring the appropriate use and stewardship of public funds and a broader mandate to ensure that entities fulfil the significant responsibilities for the effective stewardship of public money, including how they address the risks of fraud and corruption. Through our work we have seen a number of instances of fraud or red flags of potential fraud. Examples include:

    - Cheque Tampering
    - Misuse of Assets
    - Misappropriation of cash and non-cash assets
    - Financial Statement manipulation
    - Procurement schemes
    - Conflict of interests

13. Risk management is an area that we have identified through our audits that is not well developed across entities in Cayman Islands public sector, including the risk of fraud. Our work indicates that risk management and the consideration of fraud risks by the public sector is ad hoc and sporadic, and preventative and detective measures aimed to mitigate the risk of fraud are not generally considered.

14. The purpose of this guide is to provide guidance for the Government and individual entities to consider in enhancing the proactive management of fraud and corruption risks, as risk management arrangements are further developed and enhanced.

15. The guide is principles based and provides examples of key areas that should be considered by public sector entities. Certain aspects would be best addressed on a global level by Government, for example the development of an overarching fraud policy and response plan for application across the public sector or the development of annual fraud reporting arrangements.

16. Application of the principles, in particular the measures that entities put in place to prevent and detect fraud or corruption, should be based on a clear assessment of the risks entities faced and proportionate to those risks, including a consideration of the costs.

17. I hope that Government and the public sector find this good practice guide useful as they continue to build and strengthen their governance arrangements

Alastair Swarbrick MA(Hons), CPFA, CFE *14 September 2015*
Auditor General
George Town, Grand Cayman
Cayman Islands

FRAUD RISK MANAGEMENT

PRINCIPLE 1: GOVERNMENT SHOULD HAVE A WELL-DEVELOPED UNDERSTANDING OF THE FRAUD RISK INHERENT IN ITS PROGRAMS

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

UNDERTAKE A FRAUD RISK ASSESSMENT

19. Undertaking a fraud risk assessment is critical in identifying and addressing Governments vulnerabilities to fraud in its programs and operations. The extent to which an organisation carries out a fraud risk assessment will depend on its size and complexity and the nature of its activities.

20. Where there are complex delivery arrangements, or organisations are dependent on delivery partners, it may be appropriate to gauge the level of fraud risk in those bodies.

21. A high level consideration of fraud risk will determine whether there are areas that are vulnerable to fraud, and help to decide if there is a need to perform a more detailed risk assessment. It may not be cost effective to cover every possible threat situation; therefore the likelihood of occurrence of fraud and the impact on key organisational objectives must be assessed. This involves identifying the processes or activities at risk of fraud; and, assessing and ranking the nature and extent of vulnerability in each area. Some common criteria/factors used to make judgements about vulnerability (opportunities and inventive/pressures to commit fraud) include:

- size, scope and value of activities as well as the nature, security and value of assets held;
- the adequacy of operational controls, such as segregation of duties, supervision, approval and staff rotation, including appropriate skills/knowledge of operational staff and the ability for senior management to override controls;
- the particular forms of fraud threat e.g. theft, procurement, misuse of assets, fraudulent administration of contracts, falsification of records such as timesheets;
- extent of effective reporting mechanisms and the ability to stop frauds occurring quickly;
- degree of operational complexity and impact of technology;
- the quality, reliability and adequacy of staffing arrangements including the recruitment process; and
- Incentives (or pressures) that could induce staff to commit fraud e.g. the pressure on employees to achieve performance goals or deliver certain (political) results/outcomes, low levels of remuneration.

22. In assessing opportunities that might give someone reason or temptation enough to commit fraud, it is important to think like a potential fraudster. Ask: Where are controls weak? How could controls be circumvented? How could the fraud be concealed? Weak controls and a lack of segregation of duties can signal to some individuals a potential opportunity for committing fraud.

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

GATHERING INFORMATION ABOUT PAST FRAUDS

24. Opportunities for committing fraud are always changing and must therefore be constantly watched for. However, understanding the different types of fraud that government has already encountered in the past provides invaluable information for developing effective fraud prevention and detection techniques. Information that organisations would be expected to track:

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

EVALUATING THE SIGNIFICANCE OF FRAUD RISKS

25. In deciding how to address the fraud risks identified, it is important to evaluate their significance. An assessment of the possible impact and corresponding likelihood of occurrence should be made using consistent parameters that will enable the development of a prioritised risk analysis. The risk assessment should consider the financial impact, the potential political and commercial sensitivities involved and the likely effect on the organisation’s reputation. The analysis should be both qualitative and quantitative. The qualitative approach usually involves grading risks in high, medium or low categories.

26. Risks identified should then be “mapped” to existing controls, and new controls should be designed and implemented as necessary to fill in gaps. Both preventative and detective controls should be in place for risks that involve potential collusion or override by government managers, as controls such as segregation of duties will not likely be sufficient to detect fraud in those cases.

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

PRINCIPLE 2: PROMOTE AND DEVELOP AN ANTI-FRAUD CULTURE, DRIVEN BY A CLEAR TONE FROM THE TOP OF THE GOVERNMENT

28. Government can deter fraud by influencing the attitude towards it. Employees who view fraud as socially unacceptable or criminal are less likely to commit it than those who might try to justify doing it. The creation and maintenance of an anti-fraud culture is critical to maximizing the engagement of employees in combating fraud and minimizing its impact.

29. Setting the right tone from the top of Government is fundamental to developing an anti-fraud culture. Political leaders, senior managers need to lead by example by behaving ethically and demonstrating their intolerance of fraud, and effectively communicating their expectations for ethical behaviour throughout the organisation. If senior officials do not take this lead it creates a culture where there is an acceptance of inappropriate, unethical and potentially fraudulent behavior throughout the organisation.

30. In developing an anti fraud culture Government also needs to:

    - have a **clear statement of ethical values and a code of conduct** that sets out expectations for behavior throughout the organisation. This would address issues including compliance with organisations controls, dealing with conflicts of interests, receiving gifts, the need to keep certain information confidential, requirements for employees to report suspected fraud or money laundering, and that breaches would be treated as disciplinary offences;
    - **establishing a robust fraud policy** (as discussed under Principle 3);
    - **stressing in new employee orientations the organisation's anti fraud culture and fraud risk management program** – initial orientation about the organisation's anti-fraud culture and ongoing education on the fraud risk management program are important for all employees. This will help reinforce the tone from the top;
    - **running annual fraud awareness training programs** – fraud awareness training for staff should include defining fraud, explaining the fraud policy, and giving examples of public sector fraud and of red flags that should alert employees to suspicious behaviour. Attendance at these training sessions and at periodic refreshers should be mandatory;
    - **publicising internally** across the organisation information about frauds that have been detected and the disciplinary action taken;
    - **maintain good staff morale**- a positive workplace environment improves staff morale and loyalty. Managers should try to create the conditions in which staff have neither the motivation nor the opportunity to commit fraud. The maintenance of good staff morale can help minimize the likelihood of an employee causing harm to the organisation through fraud;
    - **increase the perception detection**; and

- **good communication** - publicising the fact that preventative, deterrence and detective controls are in place. Effective preventative controls that are in place, working and well known throughout the organisation will also serve as strong deterrents because most people are afraid of getting caught. Continuous communication and reinforcement of all controls are important. The message needs to get out to both internal parties (employees) and external parties (suppliers and contractors). Getting the message out to service deliverers that fraud will not be tolerated will also help get the same message out to service users (e.g. Grant recipients, benefit claimants).

PRINCIPLE 3: CREATE AND MAINTAIN THE RIGHT STRUCTURES TO MANAGE THE RISK OF FRAUD

31. Establishing clear roles and responsibilities for managing fraud risk must begin first with establishing a focused and clearly explained fraud policy. The policy should be part of the organisation's administrative policies, procedures or manuals, available to all staff. The requirement to comply with all should also be included in the standard terms and conditions of employment contracts for all staff.

DEVELOPING A COMPREHENSIVE FRAUD POLICY

32. An organisation should ensure that its fraud policy includes:

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

33. The fraud policy should also require employees and contractors to report suspected fraud immediately to the individual with the designated responsibility, ideally through a hotline. The fraud policy should promote the awareness of this hotline and the fact that protection exists for employees using the service. Government should ensure that employees at all levels, plus contractors, have acknowledged through an annual sign-off that they have read the fraud risk policy and the organisation's code of conduct and are abiding by those policies. The sign-off may also include an acknowledgement that the employee is not aware of anyone committing fraud against the government. Having a conflict of-interest policy in place also ensures that employees and contractors must come forward and disclose any potential or actual conflicts of interest they may have in carrying out their work.

ASSIGNING CLEAR ROLES AND RESPONSIBILITIES

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

35. Whilst everybody in an organisation contributes to the management of fraud risk, Chief Officers, MDs and CEOs have overall responsibility in their organisation and are accountable for the effectiveness of fraud risk management. Specific responsibility of managing the risk of fraud may be allocated to an appropriate senior officer such as the CFO.

36. All staff should be kept informed of about the organisation's anti-fraud policy, what part they are expected to play in it and their responsibilities under the law. This can be achieved in a number of ways which we discuss under principle 2 on the developing an anti-fraud culture

37. Internal audit is responsible for providing assurance on the adequacy and effectiveness of the organisation's framework of governance, risk management and control. In carrying out its work, internal audit must be alert to the possibility of significant errors, fraud or non-compliance. It is a management responsibility to put in place procedures to deter, detect and investigate fraud, but internal audit can be a significant resource in assessing the adequacy of the control framework, acting as a deterrent and potentially investigating potential instances of fraud

ESTABLISHING APPROPRIATE AVENUES FOR REPORTING SUSPICIONS OF FRAUD AND SYSTEM VULNERABILITIES

38. Staff are the first line of defence in combating fraud. There should be avenues for reporting suspicions of fraud or concerns about control weaknesses that could be exploited for fraudulent purposes. Staff should be encouraged to report suspicions to their line mangers or to a hotline set up for the purpose. It is important that staff know where to report their suspicions, that any suspicions reported in this way are seen to be acted upon by management and to assure those who report their suspicions that any information received will be treated confidentially. Information on reported suspicions should routinely be made available to internal audit.

PRINCIPLE 4: GOVERNMENT SHOULD HAVE APPROPRIATE PREVENTATIVE AND DETERRENCE MEASURES IN PLACE AND REGULARLY MONITOR THEIR PERFORMANCE

39. Prevention measures aim to stop frauds from occurring. These measures are the first line of defence against fraudsters, and it is essential that the measures be effective in stopping the majority of fraudulent activity. Frauds that circumvent these preventative and deterrence measures will require subsequent detective measures if they are to be found. A critical preventative and deterrent measure to fraud is the development and promotion of an anti-fraud culture which is addressed in principle 2.

DEVELOP A PROPORTIONATE SYSTEM OF INTERNAL CONTROL

40. Prevention and deterrence is almost always preferable to detection. The strongest defence is a sound system of internal control. Setting the tone at the top, building an anti-fraud culture and developing a clear fraud policy (as highlighted under principles 1, 2 and 3) are key parts of an internal control system. Other examples are: segregation of duties; supervision; approval; staff rotation; monitoring by management; and appropriate skills/knowledge of operational staff.

41. In designing controls, it is important that the controls put in place are proportionate to the risk. Every control action has an associated cost and it is important that the control action offers value for money in relation to the risk that it is controlling. Internal audit is an important source of advice on the range of appropriate controls to assist management in preventing and detecting fraud.

42. The importance of effective internal controls is clearly demonstrated in the ACFE's report to the nations on occupational fraud. In nearly one-third of the cases reported in the survey, the victim organisation lacked the appropriate internal controls to prevent the fraud. A lack of controls played an even bigger role in those cases affecting small organisations; this was attributed as the primary weakness in more than 41% of cases at organisations with fewer than 100 employees. Additionally, one-fifth of the reported cases could have been prevented if managers had done a sufficient job of reviewing transactions, accounts or processes.

43. The survey also highlighted that the implementation of effective controls had a significant effect on limiting the cost and duration of fraud schemes. For example proactive data monitoring and analysis was highlighted as being the most effective at limiting the duration and cost of fraud schemes; victim organisations that implemented this control experienced losses 60% smaller and schemes 50% shorter than organisations that did not.

44. Weak controls can signal to some individuals a potential opportunity for committing fraud, and therefore by ensuring there is a robust system of internal controls in conjunction with other measure can increase the perception of detection and act as a deterrent to committing fraud.

45. The instances of fraud that we have identified during our audits generally reflect a breakdown or absence of controls. For example we have seen fraud arise due to:

- a lack of segregation of duties;
- lack of supervision or management monitoring;
- the ability of senior officials to override controls; and
- mechanisms not well developed for employees to report fraud or override of controls.

ESTABLISHING FRAUD HOTLINE AND WHISTLEBLOWER PROTECTION

46. It is important that employees and third parties have a process to report instances of non-compliance with the expected behaviour. A hotline for reporting tips anonymously is a common way. Those who do report fraud (whistleblowers) must also know they will be protected (this is both a preventative and detective measure, and is discussed in detail under Principle 5).

CONDUCTING REFERENCE CHECKS AND CRIMINAL RECORD CHECKS

47. Criminal record checks and background checks are important preventative and deterrent measures. The people being hired (employees and contractors) are in a position of trust and authority. A past history of criminal activity is a red flag for fraud. A policy that encourages criminal record checks for all staff in a position of financial management and trust over public funds is good practice and government should consider requesting this from all such employees and contractors before beginning a business or employment relationship. Confirming reference checks and educational history can also uncover fraudulent statements. Any embellished or falsified statements represent increased risk that needs to be considered in the hiring process.

48. Include in supplier contracts information about government's fraud policy. All contractors should be made aware of the fraud policy and required to sign off in the contract that they have read the terms of the policy and will comply with it.

MONITORING COMPLIANCE WITH INTERNAL CONTROLS

49. Regularly monitor compliance with internal controls and communicate the findings of that work with all employees (this is both a preventative and detective measure and is discussed in detail under Principle 5). The importance a government organisation attaches to its Internal Audit department is an indication of its commitment to maintaining internal controls. With respect to fraud risk management, Internal Audit can be involved in fraud investigations, conducting internal control reviews and making recommendations for improvement, monitoring fraud hotlines and providing fraud awareness training sessions.

LIMITING SOME EMPLOYEE ROLES AND RESPONSIBILITIES

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

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

MAKING FRAUD RISK AN INTEGRAL PART OF NEW PROGRAM DEVELOPMENT

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

MAINTAINING A CONTINUOUS REVIEW OF EXISTING CONTROLS

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

PRINCIPLE 5: GOVERNMENT SHOULD HAVE APPROPRIATE DETECTIVE, INVESTIGATIVE AND DISCIPLINARY PROCEDURES IN PLACE AND REGULARLY MONITOR THEIR PERFORMANCE

54. Tackling fraud head-on using proactive methods of detection is good practice. Detective procedures are required to uncover frauds when preventative measures are not in place or are not strong at mitigating the risk. Detecting frauds and prosecuting fraudsters will not only reduce losses to an organisation but also deter other potential fraudsters. Fraud detection will also help to identify new threats, or themes, that are developing. Based on these developments, the organisation's strategic approach to managing fraud risk can be suitably updated (if necessary). Important to keep in mind is that these are not intended to prevent fraud occurring. The cost-effectiveness of prevention techniques versus detective techniques should be considered when designing fraud controls. It may be more cost-effective to have good detective measures in place versus preventative controls.

55. The ACFE report to the nations details how the results of fraud cases tend to differ based on the initial detection method. One of the most visible distinctions is that the five detection methods with both the shortest duration and lowest loss — surveillance/monitoring, account reconciliation, IT controls, internal audit and management review — involved proactive efforts to discover fraud. In contrast, detection methods that are not the result of efforts within the organisation to detect fraud — confession, notification by law enforcement, external audit and by accident — tended to last longer and cost more. In other words, having adequate controls that seek out fraud, rather than relying on external or passive detection methods, can dramatically reduce the cost and duration of such schemes.

DETECTING FRAUD ACTIVITIES

56. Establishing detection measures: Reconciliations, independent reviews, physical inspections, analysis and audits are all process controls designed in part to detect fraudulent activity. The design of these process controls is best done after first analyzing the types of frauds that could be committed in the government environment. Two especially good proactive detection measures to analyze financial data are installing fraud hotlines and using computer-assisted techniques.

    - Fraud hotlines: Fraud hotlines are the most common source of detected frauds, and can be a cost-effective way for staff – and even members of the public – to report suspicious activity. The ACFE report shows that tips are consistently the most common detection method for cases of occupational fraud by a significant margin.
    - Data Analytics: Techniques such as data matching and data mining can also aid in detecting suspicious activity. Data matching uses computers to match different data files and scan for abnormalities. For example, matching a series of electronic payment transfers to an approved supplier list can be used to look for suspicious payments. Data mining uses computer models to generate patterns, themes or associations that may help identify suspicious activity. For example, sorting an organisation's credit card transaction data by payee or transaction day can be used to look for suspicious activity. The advantage of data matching and data mining is that a large amount of transaction data can be reviewed and analyzed in a relatively short time. Operators can also easily filter and prioritize data based on pre-determined risk assessments. Before undertaking this work, however, government should be aware and take account of any legislation that may limit the collection and use of personal information for purposes of data matching.

57. Monitoring effectiveness of detection methods: It is important to assess the effectiveness of the detective measures in use through continuous monitoring.

Exhibit 2 - Guideline for setting up a fraud hotline:

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

INVESTIGATING AND RESPONDING TO FRAUDULENT ACTIVITIES

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

59. Organisations should draw up fraud response plans to ensure that timely and effective action is taken in the event of a fraud. Such plans can also help minimise losses and increase the chances of a successful investigation. The fraud response plan should reflect the risk assessment undertaken; include guidance about when to contact the police; and should be reviewed periodically.

60. Organisations are responsible for undertaking thorough investigations where there is suspected fraud and for taking the appropriate legal and/or disciplinary action in all cases where that would be justified.

61. When a fraud has been detected it should be stopped at the earliest opportunity. Appropriate disciplinary action should also be taken where supervisory or management failures have occurred. Fraud investigation is a specialised area of expertise, and organisations should ensure that those tasked with any investigation have received appropriate training, including that relating to the gathering of evidence, and an appropriate level of authority. Investigations should consider how the fraud was perpetrated, if any control failures occurred and make recommendations on systems and procedures to minimise the risk of a recurrence. Weak controls may be an indicator that the fraud was not an isolated incident and other similar frauds may be underway. Legal advice should be taken where necessary.

62. The investigation team should document and track the steps of the investigation, items collected as evidence, requests for documents and other information, interview meeting notes, conclusions drawn from analysis of evidence, and interviews conducted. A case management system should be used where the allegations of fraud can be logged and monitored. If the allegations are determined to warrant further investigation, a clear, high-quality investigative process should be in place both to mitigate losses and to ensure that appropriate corrective action is taken.

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

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

65. In some cases – for example, to mitigate loss and preserve evidence – it may be necessary to take corrective action before the investigation is complete. Those under investigation may need to be suspended or re-assigned while the investigation is ongoing and assets may need to be protected. Management should seek legal advice before taking any actions. Important to keep in mind as well is that employees may be under an obligation to respond to their employer’s questions while they are still employed. Thus, if they are fired before the investigation is complete, this obligation will no longer exist and investigation delays could result. Possible corrective actions include:

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

66. A report on investigation findings should be prepared by, or submitted to the appropriate designated senior officer. The external auditor should also be notified of all fraudulent activities. The external auditor will also want to conduct an assessment of whether there is a more serious and pervasive problem rather than relying on management's own assessment. This makes it critical that all known frauds be communicated in a timely manner to the external auditor. The investigations unit should also keep track of performance measures such as:

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

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

PRINCIPLE 6: GOVERNMENT SHOULD HAVE APPROPRIATE REPORTING PROCEDURES IN PLACE TO COMMUNICATE THE RESULTS OF ITS FRAUD RISK MANAGEMENT ACTIVITIES TO ITS STAKEHOLDERS

INTERNAL REPORTING ON FRAUD RISK MANAGEMENT ACTIVITIES

68. A reporting mechanism should be in place to enable government departments to report instances of known losses immediately to the individual with the designated responsibility as prescribed in the fraud policy. By having timely information from all departments, that individual will be able to spot trends of losses by type and decide what investigative and corrective actions are required. Those staff responsible for fraud risk management throughout government should also receive regular, comprehensive reports on fraud risk management activities. This will help them identify trends and move to mitigate losses effectively and efficiently. Such reports reviewed regularly can also illuminate where program or operating procedural changes may be required. If a good case management system is in place in the centralized investigative unit, then this reporting will be easier to complete.

REPORTING EXTERNALLY ON FRAUD RISK MANAGEMENT ACTIVITIES

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

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

Contact us

Physical Address:
3rd Floor Anderson Square
64 Shedden Road, George Town Grand Cayman

Business hours:
8:30am - 4:30pm

Mailing Address:
Office of the Auditor General
P. O. Box 2583 Grand Cayman KY1– 1103
CAYMAN ISLANDS
Email: auditorgeneral@oag.gov.ky
T: (345) 244 3211 Fax: (345) 945 7738

Complaints

To make a complaint about one of the organisations we audit or about the OAG itself, please contact Garnet Harrison at our address, telephone or fax number or alternatively email:garnet.harrison@oag.gov.ky

Freedom of Information

For freedom of information requests please contact Garnet Harrison at our address, telephone or fax number. Or alternatively email: foi.aud@gov.ky

Media enquiries

For enquiries from journalists please contact Martin Ruben at our phone number or email: Martin.Ruben@oag.gov.ky

www.auditorgeneral.gov.ky

Office of the Auditor General
CAYMAN ISLANDS

September 2015