Cayman Islands Government

ANTI-FRAUD POLICY

Version:	2.5
Date of version:	March 27, 2017
Created by:	V. Chinsee, C. Cooper, L. Knight, K. Brown
Approved by:	Deputy Governor
Confidentiality level:	Public

Change history

Date	Version	Created by	Description of change
09 Jan 2017	1.0	Vinton Chinsee	First draft of the Fraud Policy
31 Jan 2017	2.0	Vinton Chinsee	Post Discussion Draft to include Hosting Policy and Definitions
08-Feb-2017	2.1	Vinton Chinsee	Formatting updates
15-Feb-2017	2.2	Vinton Chinsee	Feedback on communications and resources
03-Mar-2017	2.3	Vinton Chinsee	Adjustment to communications section
16-Mar-2017	2.4	Vinton Chinsee	Name Change and minor cosmetic and wording changes
27-Mar-2017	2.5	Carrol Cooper	Name Change and minor cosmetic and wording changes
03-May-2017	2.6	Vinton Chinsee	Replace Record retention policy with Records and Information Standard

Table of contents

1. Introduction

This corporate fraud policy is established to facilitate the development of controls that will aid in the detection and prevention of fraud against The Cayman Islands Government, and to require and authorize appropriate investigation of suspected fraud-related incidents. It is the intent of Cayman Islands Government to promote consistent organizational behaviour by providing guidelines and assigning responsibility for the development of controls and conduct of investigations.

2. Statement of policy

This organisation has a commitment to high legal, ethical and moral standards. All members of staff are expected to share this commitment. Accordingly, management is committed to and responsible for the detection and prevention of fraud, abuse, misappropriations, and other irregularities. This policy is established to facilitate the development of procedures, which will aid in the prevention, detection, and investigation of fraud and related offences.

The purposes of establishing this fraud policy are to:

- provide a framework for setting objectives and establishes an overall sense of direction and principles for action with regard to management of fraud risk, including development and maintenance of effective internal controls to prevent, detect, and treat fraud and abuse risk;
- ensure that vigorous and prompt investigations are conducted if reasonable professional predication exists that fraud has occurred, is occurring, or could occur as a result of unmitigated vulnerabilities;
- taking appropriate legal and/or disciplinary action against the perpetrators of fraud;
- taking action where supervisory failures have contributed to the commission of the fraud or abuse;
- take into account business and legal or regulatory requirements, and contractual obligations;
- align risk management with the organization's strategic context in which the establishment and maintenance of the fraud risk management system will take place;
- establish criteria against which fraud risk will be evaluated;
- specify how fraud risk management performance will be measured and reported;
- ensure necessary resources are available to assist those accountable and responsible for managing risk;
- ensure that all fraud risk management activities are conducted and implemented in an agreed and controlled manner; and
- achieve a fraud risk management capability that meets changing business needs and is appropriate to the size, complexity and nature of the organization.

This Policy also specifies set-up activities for establishing a fraud risk management capability, incorporating the specification, end-to-end design, build, implementation and exercising of the fraud risk management capability.

This Policy shall also specify the ongoing management and maintenance of the fraud risk management capability, including:

- assigning of accountabilities and responsibilities at appropriate levels within the organization;
- ensuring that the necessary resources are allocated to fraud risk management;
- embedding of fraud risk management within the organization by communicating the benefits of risk management to all stakeholders;
- exercising of fraud risk treatment plans and related controls regularly;
- updating and communicating of the fraud risk treatment plans – particularly when there is significant change in premises, personnel, process, market, technology or organizational structure; and
- ensuring that the framework for managing fraud risk continues to remain appropriate.

3. Reference documents

- Register of Interest Policy
- Code of Business Ethics and Conduct
- Public Service Management Law (2013 Revision)
- Policy On Offering and Receiving Hospitality, Entertainment or Gifts
- Public Management and Finance Law (2013)
- Official Whistle-Blower Policy
- Records and Information Standard
- The Standards in Public Life Law, 2014
- Cayman Islands Constitution Order 2009

4. DEFINITIONS AND ACRONYMS

"Fraud" is the use of deception with the intention of obtaining personal gain, avoiding an obligation or causing loss to another party. Fraud can be used to describe a wide variety of dishonest behaviour such as forgery, false representation and the concealment of material facts. The fraudulent use of IT resources is included in this definition, where its use is a material factor in carrying out a fraud.

"Corruption" is dishonest activity in which a person acts contrary to the interests of the Office and abuses his/her position of trust in order to achieve some personal gain or advantage for themselves, or provide an advantage/disadvantage for another person or entity.

"Dishonesty" the quality of being untruthful or deceitful. To lack honesty.

"Organisation" in this document refers to the Civil Service or Ministry unless otherwise specified.

"Government" means the Cayman Islands Government, its subsidiary and related organisations.

5. Terms of reference: Actions constituting fraud

The terms defalcation, misappropriation, and other fiscal irregularities refer to, but are not limited to:

- Any dishonest or fraudulent act
- Misappropriation of funds, securities, supplies, or other assets
- Impropriety in the handling or reporting of money or financial transactions
- Profiteering as a result of insider knowledge of corporate activities
- Disclosing confidential and proprietary information to outside parties
- Disclosing to other persons securities activities engaged in or contemplated by the Government.
- Accepting or seeking anything of material value from contractors, vendors, or persons providing services/materials to the Government. Exception: Gifts less than the amount specified in accordance with the Policy On Offering and Receiving Hospitality, Entertainment or Gifts.
- Destruction, removal, or inappropriate use of records, furniture, fixtures, and equipment; and/or
- Any similar or related irregularity

6. Fraud Risk Management

6.1. Goals and strategies for fraud risk management

The primary goals for the fraud risk management system are to:

- establish risk management group to facilitate and co-ordinate the overall risk management process;
- conduct a fraud risk assessment and implement programs to prevent, detect and respond to fraud;
- periodically measure, evaluate, and report the effectiveness of the fraud risk management program;
- develop an anti-fraud culture and define management and employee responsibilities for fraud prevention, detection, and investigation;
- reduce the opportunity for fraud by integrating preventative and detective measures/controls into systems and processes;
- ensure that anti-fraud controls are considered and built into new systems and processes at the design stage based upon risk assessment according to the Government's risk assessment and risk treatment methodology;
- promote an open and ethical culture within the organisation which deems unethical behaviour as unacceptable;
- increase the vigilance of management and staff through raising fraud risk awareness;
- ensure that those charged with governance meet their statutory responsibilities towards fraud, as per regulatory requirements for corporate governance;
- learn from previous incidents, and continuously improve the Government's ability to control risk of fraud and abuse;
- increase detection of past, existing, or potential fraud by encouraging management and staff to report their suspicions while guaranteeing anonymity where requested;
- investigate impartially and thoroughly all cases or suspected cases of fraud, prosecute offenders and, where appropriate, seek to recover monies and costs through legal means.

6.2. Code of Business Ethics and Conduct

All individuals within the defined scope of this policy shall be required to strictly adhere to the Code of Business Ethics and Conduct.

- Every individual within the scope of this Policy shall receive a complete copy of the Government's Code of Business Ethics and Conduct, and shall attend special training provided to ensure complete understanding of its requirements. This training shall be provided within 60 days of employment, and once annually thereafter.

- Upon completion of the training or re-training, these individuals must complete the Government's corresponding Code of Conduct Compliance Questionnaire, which shall be permanently retained and recorded in the individual's employment records.

6.3. Accountability

Enhanced fraud risk management includes comprehensive, fully defined and fully accepted accountability for fraud risks, controls and fraud risk treatment tasks. Designated individuals shall fully accept accountability, shall be appropriately skilled and shall have adequate resources to check controls, monitor risks, improve controls and communicate effectively about risks and their management to external and internal stakeholders. This can be facilitated by:

- identifying risk owners that have the accountability and authority to manage fraud risks;
- identifying who is accountable for the development, implementation and maintenance of the framework for managing fraud risk;
- identifying other responsibilities of people at all levels in the Government for the risk management process;
- establishing performance measurement and external and/or internal reporting and escalation processes; and
- ensuring appropriate levels of risk recognition.

Risk accountability shall be recorded in job/position descriptions, databases or information systems.

6.3.1. *Fraud Investigation Unit*

For the purposes of this policy the default Fraud Investigation unit is the Internal Audit Service of the Government of the Cayman Islands. Given the limited resources of the Internal audit service the Ministry/Portfolio may outsource individual investigations to a competent and qualified institution. Such outsourcing maybe reviewed by the Internal Audit Service or the Office of the Auditor General at their discretion.

The definition of risk management roles, accountabilities and responsibilities shall be part of all the Government's induction programs, as well as any contracted arrangements with third-party service providers. The organization commits to ensuring that those who are accountable are equipped to fulfil that role by providing them with the authority, time, training, resources and skills sufficient to assume their accountabilities.

A specialized fraud investigation unit shall:

- Achieve, prove, and maintain competence in the principles, methods, processes, and standards incorporated in and referenced by this Policy;
- Assist the Government in establishing specialized risk policies and controls (risk treatment) for fraud risks in accordance with the Government's approved risk management risk assessment and risk treatment methodology;
- Keep up to date with developments in the specialized area; and
- Support investigations of fraud incidents and vulnerabilities.

The Fraud Investigation Unit has the primary responsibility for the investigation of all suspected fraudulent acts as defined in the policy. If the investigation substantiates that fraudulent activities have occurred, the Fraud Investigation Unit will issue reports to appropriate designated personnel and, if appropriate, to the Chief Officer.

6.3.1.1. Authorization for investigating fraud

Members of the Investigation Unit will have:

- Free and unrestricted access to all records and premises, whether owned or rented; and
- The authority to examine, copy, and/or remove all or any portion of the contents of files, desks, cabinets, and other storage facilities on the premises without prior knowledge or consent of any individual who might use or have custody of any such items or facilities when it is within the scope of their investigation.

6.3.2. *Human Resource Responsibilities*

6.3.2.1. Training and development

The Government shall ensure that all personnel who are assigned risk management responsibilities are competent to perform the required tasks by:

- Developing, proving, and maintaining competence in the principles, methods, processes, and standards incorporated in and referenced by this Policy;
- determining the necessary competencies for management and personnel who are assigned specific risk management roles and responsibilities for the planning, deployment, execution, testing, monitoring, and maintenance of fraud risk management and related internal controls;
- conducting an approved training needs analysis against necessary competencies on personnel assigned risk management roles and responsibilities; providing appropriate and consistent initial training for all members of the risk management steering/oversight committee, the Chief Officer and board members, the risk managers/risk officers, specialized fraud risk management project team members, business unit managers, internal audit manager and internal auditors, and trainers;
- providing appropriate and consistent training to newly inducted board members, management, and staff within 60 days of joining the organization
- testing to ensure that the necessary competence has been achieved;
    - Achievement of necessary competence of all management and personnel who are assigned specific risk management roles and responsibilities for the planning,

deployment, execution, testing, monitoring, and maintenance of [Fraud Risk Management] and related internal controls shall be evidenced by testing and, if appropriate, third-party professional certification and accreditation.

- maintaining records of education, training, skills, experience and qualifications; and
- maintaining competence with annual reassessment and refreshment of required skills of management and personnel who are assigned specific risk management roles and responsibilities for the planning, deployment, execution, testing, monitoring, and maintenance of [Fraud Risk Management] and related internal controls.

Training needs analysis and specialized personnel development shall be specific to supporting the principles, methods, processes, and standards incorporated in this Fraud Risk Management System Policy.

6.3.2.2. Other irregularities

Irregularities concerning an employee's moral, ethical, or behavioural conduct should be resolved by departmental management and the Human Resources rather than the Fraud Investigation Unit. If there is any question as to whether an action constitutes fraud, contact the Director of the Fraud Investigation Unit for guidance (Internal Audit Service).

6.3.2.3. Termination

If an investigation results in a recommendation to terminate an individual, the recommendation will be reviewed for approval by the designated representatives from Human Resources and the Legal Department and, if necessary, by outside counsel, before any such action is taken. The Fraud Investigation Unit does not have the authority to terminate an employee. The decision to terminate an employee is dealt with in accordance with the provisions of section (44) of the PSML (2013 revision) and section 39 of the Personnel Regulations (2013 revision).

6.3.3. ***Other roles and responsibilities***

Action Required	Internal Audit	Finance/ Accounting	Executive Mgmt	Line Mgmt	Risk Mgmt	Legal	Public Relations	Employee Relations
1. Controls to Prevent Fraud	S	S	SR	SR	S	S	S	S
2. Incident Reporting	P	S	S	S	S	S	S	S
3. Investigation of Fraud	P					S		S
4. Referrals to Law Enforcement	P					S		
5. Recovery of Monies due to Fraud	P							
6. Recommendations to Prevent Fraud	SR	SR	P	S	S	S	S	S
7. Internal Control Reviews	P							
8. Handle Cases of a Sensitive Nature	P		S		S	S		S
9. Publicity/Press Releases			S				P	
10. Civil Litigation	S					P		
11. Corrective Action/Recommendations		SR	SR	SR				
12. Monitor Recoveries	S	P						
13. Pro-active Fraud Auditing	P							
14. Fraud Education/Training	S		P	S			S	SR
15. Risk Analysis of Areas of Vulnerability		P	SR	SR	S			
16. Case Analysis	P				S			
17. Hotline	P							
18. EthicsLine	S		P					

P (Primary Responsibility) S(Secondary Responsibility) SR (Shared Responsibility

6.4. Reporting procedures for suspected fraud

Great care must be taken in the investigation of suspected improprieties or irregularities so as to avoid mistaken accusations or alerting suspected individuals that an investigation is under way.

An employee who discovers or suspects fraudulent activity will contact any of the following immediately; Chief Financial Officer, Chief Officer, or Internal Audit, or use the whistle blowing facilities established. The employee or other complainant may remain anonymous. All inquiries concerning the activity under investigation from the suspected individual, his or her attorney or representative, or any other inquirer should be directed to the Investigations Unit or the Legal Department. No information concerning the status of an investigation will be given out. The proper response to any inquiries is: “I am not at liberty to discuss this matter.” Under no circumstances should any reference be made to “the allegation,” “the crime,” “the fraud,” “the forgery,” “the misappropriation,” or any other specific reference.

The reporting individual should be informed of the following:

- Do not contact the suspected individual in an effort to determine facts or demand restitution.
- Do not discuss the case, facts, suspicions, or allegations with *anyone* unless specifically asked to do so by the Legal Department or Fraud Investigation Unit.

6.5. Integration into organizational strategy and governance

Fraud risk management shall be viewed as central to the organization's management processes, such that risks are considered in terms of effect of uncertainty on objectives. The governance structure and process are based on the management of fraud risk. Effective fraud risk management shall be regarded by managers as essential for the achievement of the Government’s objectives.

6.6. Integration into organizational processes

Fraud risk management shall be embedded in all the Government’s practices and processes in a way that it is relevant, effective and efficient. The fraud risk management process shall become part of, and not separate from, those organizational processes. In particular, fraud risk management shall be embedded into the policy development, business and strategic planning and review, and change management processes.

All decision making within the Government, whatever the level of importance and significance, shall involve the explicit consideration of fraud risks and the application of fraud risk management to some appropriate degree. This shall be indicated by records of meetings and decisions to show that explicit discussions on risks took place. In addition, all components of risk management are represented and evidenced within key processes for decision making in the Government, e.g. for decisions on the allocation of capital, on major projects and on re-structuring and organizational changes.

For these reasons, soundly based fraud risk management shall be seen within the Government as providing the basis for effective governance.

There shall be an organization-wide fraud risk management plan to ensure that the risk management policy is implemented and that fraud risk management is embedded in all of the Government's practices and processes. The fraud risk management plan can be integrated into other organizational plans, such as strategic plans.

6.7. Resources

The Government shall allocate and budget for appropriate resources for fraud risk management. Consideration should be given to the following:

- people, skills, experience and competence;
- resources needed for each step of the fraud risk management process;
- the organization's processes, methods and tools to be used for managing fraud risk;
- documented processes and procedures;
- information and knowledge management systems; and
- training programs.

It is important to understand the roles and responsibilities that personnel at all levels of the Government have with respect to fraud risk management. These roles should be defined by policies, job descriptions and delegations of authority. The key resources required include the following:

Management

Management has overall responsibility for the design and implementation of a fraud risk management programme. This includes the following:

- Setting the tone at the top.
- Encouraging and supporting implementation of the Fraud Policy.
- Ensure that it is clear that fraud will not be tolerated and whistleblowers will not suffer retribution.
- Implementing adequate internal controls.
- Reporting to senior management or the board (where applicable) on what actions have been taken to manage fraud risks.
- Reporting actual incidents of fraud.

Staff

Strong controls against fraud are the responsibility of everyone in the organization.
All levels of staff should:

- Have a basic understanding of fraud and be aware of the red flags.
- Understand their roles within the internal control framework.
- Understand how their jobs relate to potential fraud opportunities within the organization.
- Read and understand Anti-Fraud policies and procedures.
- Participate in the process of creating a strong control environment and designing and implementing fraud control activities.
- Report suspicions or incidences of fraud.
- Cooperate in investigations.

Internal Auditing

A key function in the organisation is the Internal Audit Service.

Internal auditors are independent of the organization in principle and fact. Standard operations should:

- Consider the organization's assessment of fraud risk when developing their annual audit plan.
- Communicate regularly with those conducting the organization's risk assessments. This will help them ensure that all fraud risks have been considered appropriately.
- Spend adequate time and attention evaluating the design and operation of internal controls related to fraud risk management.
- Apply professional skepticism when reviewing activities and be on guard for the signs of fraud.
- Potential frauds uncovered during an engagement should be treated in accordance with the established Anti-Fraud policy and procedures.

6.8. Policy communication

Enhanced fraud risk management includes continual communications with external and internal stakeholders, including comprehensive and frequent reporting of risk management performance, as part of good governance.

Communication with stakeholders is an integral and essential component of risk management. Communication is rightly seen as a two-way process, such that properly informed decisions can be made about the level of risks and the need for risk treatment against properly established and comprehensive risk criteria.

Comprehensive and frequent external and internal reporting on both significant risks and on risk management performance contributes substantially to effective governance within an organization.

6.8.1. *Establishing internal communication and reporting mechanisms*

Government entities shall establish internal communication and reporting mechanisms in order to support and encourage accountability and ownership of fraud risk. These mechanisms should ensure that:

- key components of the fraud risk management framework, and any subsequent modifications, are communicated appropriately;
- there is adequate internal reporting on the framework, its effectiveness and the outcomes;
- relevant information derived from the application of fraud risk management is available at appropriate levels and times; and
- there are processes for consultation with internal stakeholders.

These mechanisms should, where appropriate, include processes to consolidate risk information from a variety of sources, and may need to consider the sensitivity of the information.

The actual mechanisms should include but not limited to the following:

- Face-to-face meetings – one on one or town hall style.
- Email to stakeholders.
- External stakeholders should be given an email to use so communication can be both ways.
- Publish on websites – Government and Department

Through tools such as Degreed and the Civil Service College

Establishing external communication and reporting mechanisms

Government entities shall develop and implement a plan as to how it will communicate with external stakeholders. This should involve:

- engaging appropriate external stakeholders and ensuring an effective exchange of information;
- external reporting to comply with legal, regulatory, and governance requirements;
- providing feedback and reporting on communication and consultation;
- using communication to build confidence within each entity; and
- communicating with stakeholders in the event of a crisis or contingency.

These mechanisms should, where appropriate, include processes to consolidate risk information from a variety of sources, and may need to consider the sensitivity of the information.

The actual mechanisms should include the following:

- Face-to-face meetings – one on one or town hall style.
- Email to stakeholders.
- External stakeholders should be given an email to use so communication can be both ways.
- Publish on websites – Government and Department

6.9. Implementing fraud risk management

6.9.1. *Implementing the framework (system) for managing risk*

In implementing the framework for managing risk, Government entities shall:

- define the appropriate timing and strategy for implementing the framework;
- apply the fraud risk management policy and process to the organizational processes;
- comply with legal and regulatory requirements;
- ensure that decision making, including the development and setting of objectives, is aligned with the outcomes of fraud risk management processes;
- hold information and training sessions; and
- communicate and consult with stakeholders to ensure that its fraud risk management framework remains appropriate.

6.9.2. *Implementing the fraud risk management process*

Fraud risk management shall be implemented by ensuring that the risk management process outlined in the Government's **Risk assessment and Risk Treatment Methodology** is applied through a fraud risk management plan at all relevant levels and functions of the organization as part of its practices and processes.

6.10. Fraud risk monitoring

Ongoing monitoring and review is necessary to ensure that the context, the outcome of the fraud risk assessment and fraud risk treatment, as well as management plans, remain relevant and appropriate to the circumstances. The Government should make sure that the fraud risk management process and related activities remain appropriate in the present circumstances and are followed. Any agreed improvements to the process or actions necessary to improve compliance with the process should be notified to the appropriate managers to have assurance that no

risk or risk element is overlooked or underestimated and that the necessary actions are taken and decisions are made to provide a realistic risk understanding and ability to respond.

Additionally, the organization shall regularly verify that the criteria used to measure the fraud risk and its elements are still valid and consistent with business objectives, strategies and policies, and that changes to the business context are taken into consideration adequately during the risk management process.

Government entities shall ensure that fraud risk assessment and risk treatment resources are continually available to review fraud risk, to address new or changed threats or vulnerabilities, and to advise management accordingly.

6.11. Continual improvement

An emphasis shall be placed on continual improvement in fraud risk management through the setting of organizational performance goals, measurement, review and the subsequent modification of processes, systems, resources, capability and skills.

This shall be supported by the existence of explicit performance goals against which the organization's and individual manager's performance is measured. The organization's performance shall be published and communicated. Normally, there shall be at least an annual review of performance and then a revision of processes, and the setting of revised performance objectives for the following period.

This fraud risk management performance assessment shall be an integral part of the overall organization's performance assessment and measurement system for departments and individuals.

7. Support for Fraud Risk Management System implementation

Hereby the executive management declares that all phases in Fraud Risk Management System implementation, execution, monitoring, maintenance, and communication will be supported with adequate resources in order to achieve all goals and objectives set in this Policy.

8. Validity and document management

This document is valid as of May 1, 2017

The owner of this document is the Chief Financial Officer, who must check and if necessary update the document at least once a year, or within 30 days of any significant organizational change.

When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered:

- number of employees and external parties who have a role in the Fraud Risk Management System, but are not familiar with this document
- non-compliance of the Fraud Risk Management System with the laws and regulations, contractual obligations, and other internal documents of the organization
- ineffectiveness of Fraud Risk Management System implementation and maintenance
- unclear responsibilities for Fraud Risk Management System implementation
- insufficient fulfilment of assigned fraud risk management roles and responsibilities