Queensland Health

Fraud and corruption control

Department of Health Guideline
QH-GDL-295-1:2015

1. Statement

This fraud and corruption control guideline (the Guideline) supports implementation of the Fraud and Corruption Control Policy and Standard.

2. Scope

This Guideline provides information for all employees, contractors and consultants within the Department of Health Divisions and Business Units (BUs). The Queensland Ambulance Service's local Fraud and Corruption Control framework is aligned to this guideline.

3. Requirements

The roles and responsibilities for fraud and corruption control are detailed within the Fraud Control Standard.

3.1 Guideline for Fraud and Corruption control

3.1.1 Commitment to fraud control

The Department of Health (the department) has zero tolerance for corrupt conduct including fraud. This is supported by a hierarchy of governance and controls which will continue to build an ethical organisational culture. The Department recognises that fraud and corruption prevention and control are integral components of good governance and risk management.

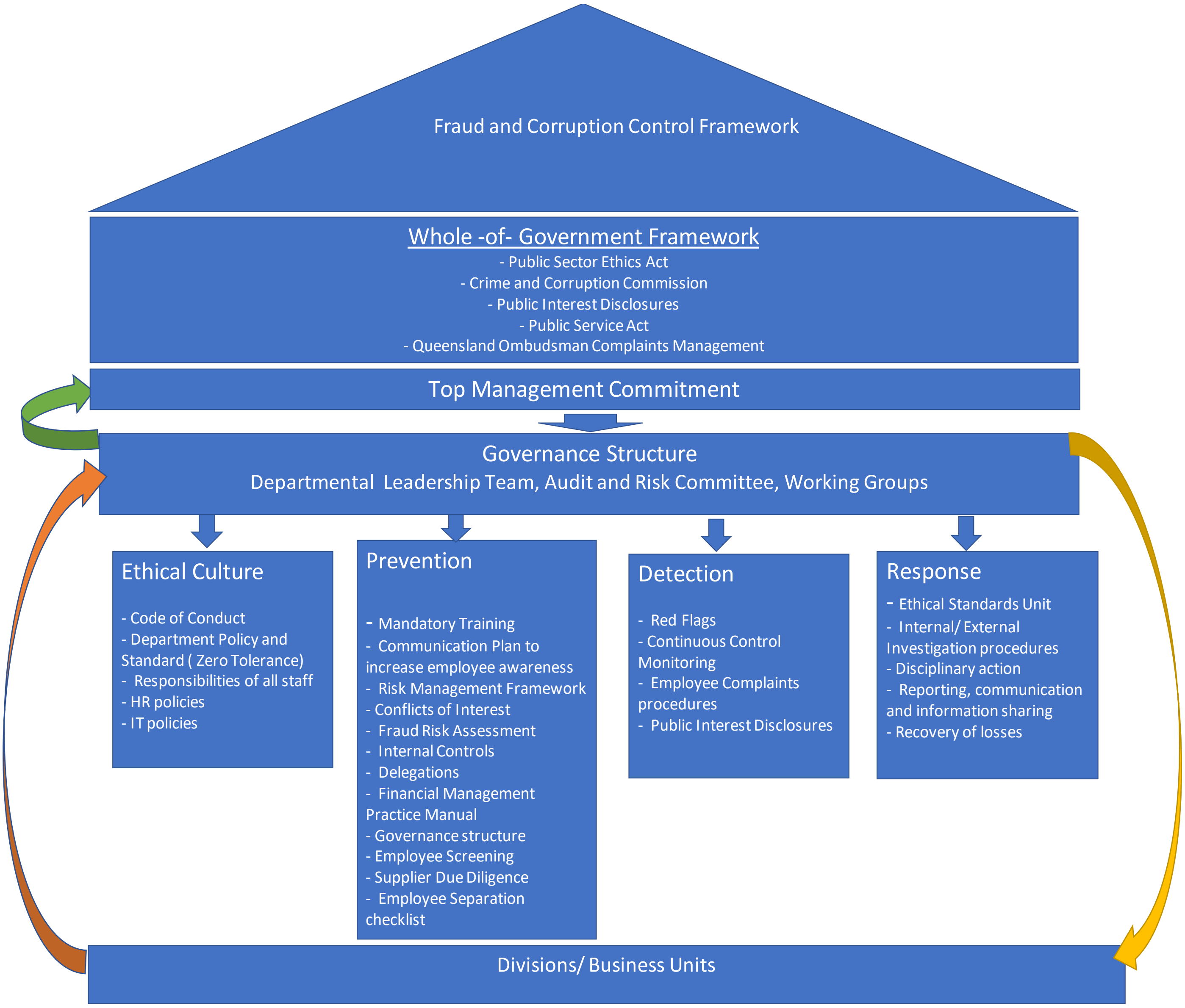
The Guideline provides guidance and direction to all employees and other stakeholders on the processes in the department for:

- preventing fraud and corruption;
- detecting fraud and corruption; and
- responding to incidents of suspected or actual fraud and corruption.

The department has adopted a structured governance framework and an integrated approach to the development, implementation and regular review of fraud prevention and detection, monitoring, reporting and response strategies. The framework is based on the Australian Standard Fraud and Corruption Control (AS 8001-2008).

Queensland
Government

The department’s Fraud and Corruption Framework is depicted below.



Fraud and Corruption Control Framework

Whole -of- Government Framework

- Public Sector Ethics Act
- Crime and Corruption Commission
- Public Interest Disclosures
- Public Service Act
- Queensland Ombudsman Complaints Management

Top Management Commitment

Governance Structure

Departmental Leadership Team, Audit and Risk Committee, Working Groups

Ethical Culture

- Code of Conduct
- Department Policy and Standard (Zero Tolerance)
- Responsibilities of all staff
- HR policies
- IT policies

Prevention

- Mandatory Training
- Communication Plan to increase employee awareness
- Risk Management Framework
- Conflicts of Interest
- Fraud Risk Assessment
- Internal Controls
- Delegations
- Financial Management Practice Manual
- Governance structure
- Employee Screening
- Supplier Due Diligence
- Employee Separation checklist

Detection

- Red Flags
- Continuous Control Monitoring
- Employee Complaints procedures
- Public Interest Disclosures

Response

- Ethical Standards Unit
- Internal/ External Investigation procedures
- Disciplinary action
- Reporting, communication and information sharing
- Recovery of losses

Divisions/ Business Units

3.1.2 Four major components of the Guideline to Fraud and Corruption Control

The information in this Guideline supports implementation of the policy and standard which are aimed at:

- reducing the potential for fraud and corruption;
- building and maintaining a culture which focuses on prevention of fraud and corruption;
- implementing adequate processes and risk management practices to detect and manage suspected fraud and corruption matters; and

- providing guidance on responding to and managing suspected instances of fraud and corruption within the department.

The four essential components of fraud and corruption control are contained in Table 1.

Table 1 Components of the Guideline to Fraud and Corruption Control

1. Ethical Culture	Increasing levels of fraud and corruption awareness by embedding and implementing initiatives to deter and minimise the opportunities for fraud.
2. Prevention	Preventing instances of fraud and corruption by strengthening the systems of control and risk management.
3. Detection	Implementing initiatives to detect fraud and corruption as soon as possible after it occurs.
4. Response	Implementing initiatives to deal with detected or suspected fraud and corruption in accordance with relevant policies and legislation. Ensuring appropriate outcomes (disciplinary, civil, systemic or criminal justice system), thereby helping to deter and prevent fraud from re-occurring. The recovery of losses is maximised as far as possible, thereby limiting the financial impact

3.1.3 Review of the Fraud and Corruption Control Guideline

This Guideline will be reviewed at least every three years but a review can be initiated at any time by changes in the policy environment.

3.1.4 What is fraud and corruption?

The definitions of fraud and corruption are provided in section 6 of the Guideline. Refer to Table 2 below for examples of fraud and corruption.

Table 2 Examples of fraud and corruption

Internal	External	(Joint) Collusion
• False claims for travel, petty cash, overtime and expenses • Misuse of corporate credit cards and cab charge • Falsifying invoices for goods or services • Dishonestly using purchase order forms to gain a personal benefit • Dishonest use of intellectual or confidential property • Falsifying hours on timesheet • Falsifying a medical certificate • Working elsewhere during working hours or whilst on leave (e.g. sick leave) without permission.	• Inappropriate access to information and use • Charging for goods or services that are incomplete or not delivered • Goods not supplied as per the samples approved or supply of low quality product at high price • Fraudulently inflating invoices • Phishing emails sourcing payments	• Certification for goods or services as being delivered when they are not • Unlawful or unauthorised release of information • Knowingly making or using forged or falsified documentation • Collusion with external vendors (e.g. kickbacks and providing insider information etc.) • Raising fraudulent invoices and colluding

Internal	External	(Joint) Collusion
• Conflicts of Interest which is not declared • Misappropriation (embezzlement) or theft of department assets • Creating false entries in the Dangerous Drugs Register to obtain controlled drugs • Financial statement fraud • Creating false bank accounts to transfer money • False information on CV • Sharing of sensitive data or information intentionally for own or others benefit		with an authorising officer to approve them.

3.2. Ethical Culture

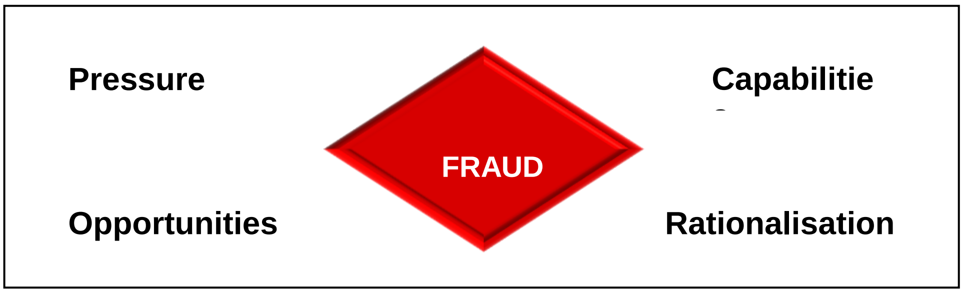
3.2.1 Understanding why people commit fraud – The Fraud Diamond

The Fraud Diamond at Figure 1 describes the four key contributing elements to fraud within the department. Fraud is more likely to occur when:

- Pressure: A person has an incentive or pressure to commit fraud e.g. gambling addiction, financial issues etc.
- Opportunities: Weak internal controls or oversight provide a person with opportunities to commit fraud e.g. ineffective control monitoring can provide an avenue to commit fraud.
- Capabilities: The person has the knowledge of the systems and ability to manipulate others. The person has the capability to recognise the opportunity to commit fraud and takes advantage of it.
- Rationalisation: The person can justify or rationalise the fraudulent behaviour.

Raising awareness of the above four contributing elements can support an ethical culture and assist staff in recognising early warning signs of fraudulent activity (red flags).

Figure 1 – The Fraud Diamond



Adapted from The Fraud Diamond: Considering the Four Elements of Fraud, David Wolfe and Dana Hermanson (2004)

3.2.2 Embedding an ethical culture

Raising awareness of ethical behaviours will assist in minimising the risk of fraud across the organisation. The organisation’s expectations on ethical behaviour are outlined in the Code of Conduct for the Queensland Public Service (the Code of Conduct) which describes its commitment to creating and maintaining an environment which is professional, client responsive, safe and free of any form of unlawful or inappropriate behaviour. This commitment supports the expectations of the people of Queensland that all activities of the department are conducted with efficiency, impartiality and integrity.

3.2.3 Fraud and corruption control education and training program

Fraud and corruption can go undetected due to lack of employee knowledge in recognising the early warning signs of fraudulent activity. Employees may be unaware of how to report their suspicions or have a lack of confidence in the integrity of the complaints management processes. The department has mandatory fraud awareness training to assist in raising the awareness of fraud and corruption and how employees should respond should this type of activity be suspected or detected.

Fraud awareness training is available online and through the Risk, Assurance and Information Management (‘RAIM’) Branch. Managers or executives may request or conduct additional training specifically related to their area of business operations.

The RAIM Branch can also provide targeted education and training as a bespoke extension to the standard, online training that offers an in-depth analysis of fraud risks, controls and treatments specific to the work area.

In addition, the department develops an annual communication plan which includes fraud and corruption awareness activities conducted throughout the year. This is an opportunity to revisit lessons learned and promote awareness of new, emerging or changing fraud risks. During fraud awareness activities, managers are encouraged to facilitate discussions with their work groups regarding the importance of fraud awareness and effective fraud controls. Fraud awareness communications are coordinated by the RAIM Branch.

3.2.4 Tasks for improving an ethical culture

Additional best practice tasks for improving an ethical culture include the following initiatives. These initiatives are supported by effective and continuous communication and example-setting by management (tone from the top approach):

- Fraud and corruption control responsibilities forms part of the performance management framework. Ensuring all employees receive information on the Fraud and Corruption Control Policy, Standard and the Code of Conduct upon induction.
- Ensuring updates and changes to relevant policies and procedures are effectively communicated to all employees.
- Confirming that all employees have participated in relevant training including Ethics, Integrity and Accountability (Code of Conduct) training.
- Regular liaison between Executives and key branches, including RAIM, Human Resources, Internal Audit, Finance, Payroll, Procurement and Ethical Standards Unit.
- Regular discussion of standards of conduct or behaviours at team /unit meetings.
- Use of available media to disseminate fraud awareness materials, including newsletters, intranet information, emails, leaflets.
- Roll-out of the fraud awareness e-Learning package across the department.
- Measurement of employee awareness levels through an annual Fraud Awareness survey.

- Regular communication with employee to ensure that key messages are disseminated effectively.
- Fraud Awareness communications to reinforce key fraud control messages.

These initiatives are supported by effective and continuous communication and example-setting by management (tone from the top approach).

3.3. Prevention

Key aspects of a fraud prevention program include:

- Ensuring internal controls are in place to manage potential fraud risks.
- Ensuring managers are aware of and accountable for identified fraud risks, policies, procedures and systems within their jurisdiction.
- Identifying control weaknesses and implementing measures to address these weaknesses.
- Undertaking regular fraud risk assessments to identify potential risks and control weaknesses and appropriate treatments.
- Proactively assessing effectiveness of treatments and controls for fraud risks and revising as relevant.
- Continuous monitoring of controls as per the Continuous Monitoring Framework

3.3.1 Internal controls

Internal controls are the first line of defence against fraud. The department maintains a strong internal control system and promotes and monitors the use of effective internal controls. The Financial Management Practice Manual has been designed to provide high level policy (statements of principles) which is referenced to the other documents which support the policy. These include relevant department procedures, documents and processes which implement the high-level policy. The Financial Management Assurance Program is undertaken annually for financial risks to provide assurance to the Chief Financial Officer (CFO) that the internal financial controls are operating efficiently, effectively and economically. The Divisions/BU’s complete a self-assessment after reviewing the relevant financial controls.

Effective internal controls are developed and maintained through the cooperation of multiple work areas within the department including governance, finance, human resources, procurement, information technology etc.

Internal Audit provides an independent assurance that the financial and non-financial internal controls are operating in an efficient, effective, economical and ethical manner.

3.3.2 Fraud and corruption risk assessment

The department (through the fraud risk owners, risk personnel, governance unit and Working Group) adopts a formal identification, analysis and evaluation of fraud and corruption risks through a periodic assessment of risks of fraud and corruption. The following section identifies key areas which are particularly susceptible to fraud risk. It should be noted however, that regardless of the business area concerned, fraud risk is heightened when executives and managers fail to properly manage people, systems and processes. It is the responsibility of the leadership team and managers in the department to clearly articulate to employees their roles, responsibilities and expected standards of behaviour.

Furthermore, if specific, identified fraud risks exist within a manager’s business unit or jurisdiction, it is the responsibility of that manager to monitor, control and/or treat that risk. If a change in the business environment occurs that has an impact on a fraud risk, it is the responsibility of the manager or fraud risk owner to ensure the risk is updated on the fraud risk register in the RiskMan system. The Working Group will review and monitor the changes to the fraud risk.

3.3.3 Fraud and corruption risk identification

Fraud and corruption risk identification is the process of finding, recognising and recording risks. Whilst employees are responsible for their own behaviour and actions, managers have a responsibility to ensure they provide a clear message that the types of behaviours and activities outlined in the following examples are unacceptable and will not be tolerated. The examples should also be considered while identifying fraud risks within respective areas.

Correspondence and information management

All employees must ensure confidential information and personal information relating to individuals' own privacy is securely held and only used for the purpose for which it is collected.

The following are examples of inappropriate use of correspondence and information resulting in fraud and corruption:

- A former employee obtaining confidential information and providing it to a new employer to aid their dealings with Queensland Health.
- An employee leaking commercial-in-confidence information obtained through the performance of their work to a member of the public.

Managers should ensure their employees are aware of their obligations and responsibilities regarding the management and control of correspondence and information.

Delegations

Delegation of authority within the department establishes who is empowered to make decisions and to take action on its behalf. The department's Corporate Delegations Policy and related procedures identify requirements, roles and responsibilities in relation to delegating decisions, authority or power.

Employees may exercise their delegation through actions such as approving expenditure and purchase requisitions, approving appointments or leave applications, or signing a contract that commits the department to expenditure.

The following are examples of inappropriate use of delegations which may raise concerns about fraud and/or corruption:

- Using delegation for fraudulent or corrupt purposes, such as intentionally awarding a contract to a contractor without proper due consideration of alterative suitable providers as per Queensland Health procurement policy and procedure.
- Exceeding delegated authority e.g. intentionally authorising an invoice for $15,000 where the delegated limit is $10,000.

Employees with delegated authority are responsible for ensuring they understand their delegations and use them appropriately.

Facilities and public resources

All departmental employees are accountable for resources they use or have access to in the course of performing their duties. The Code of Conduct section 4.3 requires all employees to be economical, avoid waste and extravagance when using public resources for their proper purposes and use any public resource in accordance with Queensland Government and agency policy.

The poor management and misuse of public resources can undermine the integrity and operational efficiency of the department as a Queensland Government agency thereby not providing the public with value for money.

The following are examples of misuse of resources resulting in fraud and/or corruption:

- Regularly taking resources, such as office supplies, stationery or equipment, home for personal use, or to sell for personal benefit i.e. stealing/theft.
- Deliberately over-ordering resources to use the surplus for personal gain

Finance

The department’s Financial Management Practice Manual (FMPM) details policy, procedure and guidelines regarding accounting and financial management issues. It is fundamentally based on the *Financial Accountability Act 2009* and the *Financial and Performance Management Standard 2009*.

It encompasses all requirements imposed upon the public sector such as the Code of Conduct and incorporates all legislative requirements, whole of government requirements and generally held notions of best practice.

Compliance with the FMPM is mandatory. Managers of non-finance operational units should be aware of the sections of the FMPM that affect their particular area of operation. All employees directing and undertaking financial operations should familiarise themselves with the relevant requirements of the FMPM.

The following points represent some examples of fraud and/or corruption as they may relate to finance functions:

- Manipulating the financial system to make payments to a non-existent supplier, for personal financial or non-financial gain.
- Approving invoices for private expenses or colluding to do so for others.
- Manipulation of financial information to cover up poor performance or mistakes.
- Intentionally failing to record purchases properly in order to disguise a fraudulent gain.
- Charging personal expenses to a corporate credit card.
- Misusing Cab charge vouchers for personal use or profit.
- Allocating grant funds in contravention of departmental policy and procedure in order to obtain a financial benefit.

Human resource management

Human resource management in the department is governed by legislation, industrial instruments (e.g. awards, agreements), directives and policies.

The following represent examples of fraud and/or corruption in the management of human resources:

- Manipulating recruitment and selection procedures to secure an appointment for a close friend or family member.
- Promoting, engaging or giving an employee advantage over others for personal reasons.
- Unfairly disadvantaging, bullying, intimidating or discriminating against employees for personal reasons (e.g. unlawful use of authority in order to derive a personal gain).
- A job candidate falsifying qualifications, employment history or references to enhance their prospects of securing a position.

Information management and information technology

The department maintains a range of information management and technology policies and standards regarding its information resources. Compliance with these policies and standards is mandatory for all employees.

The department is reliant on information management and information technology systems to perform its functions. It is imperative that information maintained on these systems is accurate, complete and uncorrupted. It is critical for the organisation’s efficient and productive operation that the information contained on its systems is easily accessible for legitimate purposes while being protected from any misuse.

The following points represent some examples of fraud and/or corruption risks:

- Placing malware (e.g. viruses, spyware) on departmental information technology (IT) system in an attempt to damage software or information held on the system.
- Using another employee's log-in to gain network/system access.
- An IT contractor providing information about the department's information technology system to a third party who uses the information to attack the department's systems.
- An IT contractor building a 'back door' into information technology systems that enable unauthorised access to the department's electronic data and records.

Legal and contractual compliance

The department enters into legal contracts (e.g. agreements, deeds, service contracts, memorandums of understanding,) to meet service delivery obligations.

The following points represent some examples of fraud and/or corruption risks:

- A contract manager intentionally does not declare a conflict of interest but continues to deal with an associate, who is a personal friend and director of a company the department procures services from. The contract results in losses for the department.
- Solicits or accepts a bribe in order to exercise, or not exercise, their authority in a certain way.
- A Manager or Division/BU fails to properly monitor the quality of the work performed by a service provider, resulting in payment of invoices for work which has not been performed.

Regulatory compliance

There are two main areas of risks associated with regulatory compliance in the department. First, the department is subject to legislation and there may be risks associated with breaching the requirements of legislation (as covered in the previous sections). Second, the department acts as a regulator and as such, risks may be present regarding the appropriate or inappropriate use of this power by staff undertaking regulatory activities.

The following activities undertaken by the departmental staff authorised or delegated, may present risks of fraud, corruption or maladministration:

- Issuing a license to an individual or business based on factors other than objective assessment criteria (e.g. personal relationship).
- Deciding or recommending not to pursue prosecution because of a personal relationship with the person or business in breach of legislation.
- Choosing not to audit a person or business because of a relationship with that person or business.

Procurement

The department must comply with the Queensland Procurement Policy to ensure that principles, processes and procedures uphold the integrity of procurement decision making.

The following points represent some examples of fraud and/or corruption risks:

- Knowingly making payments on fraudulent procurement related claims.
- Splitting an order to avoid obtaining competitive quotes in the tending process or to 'work around' delegation limits for procurement transactions.
- Fraudulent procurement practices by suppliers like tender collusion, bid rigging, falsified claims.

Organisational Change

Fraud risk may be heightened in times of organisational change e.g. machinery of government changes, restructures, response to emergent situations or a migration to a new information system.

Poorly managed organisational change can lead to confusion or ambiguity in reporting lines, roles and responsibilities which can create the right conditions for fraud to occur.

The following are some examples of fraud risk during times of organisational change:

- Two business units merge and some employees are unsure of the new protocols due to lack of communication. Employees may falsify working hours, leave etc.
- Lack of oversight or monitoring over a rarely used fund source could result in fraudulent use of the funds.

Particular attention should be paid to the internal controls to prevent fraud and manage the fraud risks as part of the fraud risk analysis, assessment and treatment.

3.3.4 Fraud and corruption risk analysis

Analysing fraud and corruption risks is a key component for creating an effective ethical culture. The analysis phase involves developing an understanding of the risk. It provides input into risk evaluation and decision-making on whether risks need to be treated. Subsequently, the information gathered will determine the most appropriate risk treatment options and methods.

The risk analysis process as per the department's Risk Management Standard (QH-IMP-070-1:2015) and Risk Assessment and Treatment Guideline (including Risk Analysis Matrix) (QH-GDL-070-1-1) shall be used to:

- Determine the possible outcome should a risk occur and the likelihood of the risk occurring using the Consequence and Likelihood tables.
- Determine the level of risk rating.
- Determine the current and projected level of risk.

3.3.5 Fraud and corruption risk evaluation

Analysis of fraud and corruption risk against the department's risk analysis matrix takes into account the impact of the risk on the department and the existing internal controls.

A robust risk evaluation assists the department to decide on the responsible courses of action to take an integrated approach to fraud and corruption risk management and it can include the following evaluation considerations:

- Whether fraud and corruption risks need a formal treatment plan, or appropriate additional controls.
- Whether resources should be dedicated towards undertaking an activity (a course of action).
- Priorities for the treatment of identified risks linked to the areas of fraud and corruption.

3.3.6 Fraud and corruption risk treatment

A risk treatment is an approved task/activity/program/project or other initiative that when implemented/ completed will reduce the likelihood and/or consequence of the current level of risk to the projected level. A risk treatment may also aim to improve, maintain or monitor the effectiveness of current controls. In treating the risks, decisions should be made on the most appropriate treatment/s to be pursued for each fraud or corruption risk. Consideration of treatments should include both positive and negative outcomes and its interdependencies to other controls that may arise from implementing each treatment option. The risk treatment should include timeframes and departmental officer responsible for ensuring treatments are implemented within the timeframes. This will assist in formally managing, monitoring, reducing or eliminating the identified risk associated with fraud and corruption.

3.3.7 Monitor and review of fraud and corruption risks

Risk registers and the risk treatment /action plans are used for reviewing and monitoring fraud risks. Fraud risk owners are responsible for identifying, assessing the risk, monitoring and reviewing the effectiveness of controls and treatments for that risk. Decisions undertaken for review, evaluation and treatment of risk should consider the total cost of the fraud or corruption risk under consideration, including increases or reductions in spending on controls as a result of the proposed treatment options.

A fraud /corruption risk can only be closed in the RiskMan system after obtaining an approval from the Risk Owners (Deputy Director-General/Chief Executive Officer) and presentation to the Working Group.

3.3.8 Pre-employment screening

The department is committed to maintaining public confidence in the integrity of all employees and as such all persons to be engaged in general employment, permanently or when the period of employment is expected to exceed one month, are required to have employment screening in accordance with Employment screening HR policy B40.

Pre-employment screening is one effective means of preventing fraud. For example, pre-employment screening may detect falsified qualifications or employment history. Employment screening may identify previous criminal convictions for offences within Australia or New Zealand. Selection panels, delegates for appointments, recruitment units and human resources managers shall ensure employees, prospective employees and other persons have the requisite employment screening undertaken including criminal history check prior to appointment.

Current employees may be required to undertake employment screening checks when their employment circumstances change (e.g. secondment, higher duties, promotion, transfer, deployment etc). The Employment screening HR policy B40 outlines the checks that hiring/line managers should consider when a current employee moves to a new role within Queensland Health e.g. verification of identify, citizen/visa checks, mandatory qualifications, professional registration/membership checks, reference checks etc.

3.3.9 Contractor and supplier due diligence

The department will perform effective due diligence on contractors and suppliers which may include but is not limited to the following:

- Search on company register
- Legal entity name
- ABN confirmation
- Verification of persons/positions authorised to commit the contract/supplier to a contract
- Assessment of financial viability
- Trading address verification
- Insurance certificates of currency
- Licensing and qualifications
- Media search such as Google etc.

The department will consider ongoing commercial relationships and reassess a future working relationship if it is found that there is a real or perceived increased risk of fraud or corruption. Refer to the Supplier Due Diligence guide for the requirements.

3.3.10 Tasks for fraud and corruption prevention

Additional best practice tasks for fraud prevention include the following:

- The Director-General and/or the Executive Director RAIM Branch in conjunction with the Working Group may request audits/reviews of specific areas of concern.
- Consider and where appropriate implement the recommendations made by the Crime and Corruption Commission (CCC) as a result of proactive reviews and investigations.

- Clear and consistent communication by executives/managers regarding adherence to relevant internal controls, policies, procedures, systems and expected standards of conduct.
- Routinely identify and manage possible conflicts of interest particularly in high risk areas such as finance, procurement and human resource management in compliance with the department policy

3.4 Detection

Despite prevention activities, fraud and corruption may still occur. Therefore, it is important specific strategies are in place to detect and report fraud as soon as possible after it has occurred.

3.4.1 Reporting instances of suspected corrupt conduct (including fraud)

As per the fraud and corruption standard and Requirements for reporting corrupt conduct (HR policy E9) all departmental employees who become aware of suspected corrupt conduct (including fraud) have an obligation to report the matter and must do so immediately.

It is recommended that suspected corrupt conduct is reported through line management in the first instance, who will arrange for the matter to be referred to the Ethical Standards Unit (ESU). However, for instances where this is not appropriate, an employee may report the matter to Senior Executive or directly to ESU (CO_Complaints@health.qld.gov.au) or call **1800195240.** Employees can also report to the CCC (http://www.ccc.qld.gov.au/corruption/report-corruption/how-to-report-corruption).

Employees reporting allegations of suspected corrupt conduct must maintain confidentiality i.e information regarding the alleged fraud or corruption must only be shared with persons directly involved in receiving, assessing or managing the complaint. Once a report is made, the employee reporting the allegation is to take no further action until advised by the ESU.

Staff can also make anonymous disclosures under the *Public Interest Disclosure Act* or report the matter to the External proper authorities like the CCC, Queensland Ombudsman etc.

A member of public can disclose the information to any department officer, another property authority with the power to investigate or remedy the matter or a Member of the Legislative Assembly.

The department will ensure complaints and disclosures are managed impartially and in accordance with the *Public Interest Disclosure Act 2010* (PID Act) and the Public interest disclosures HR Policy I5.

3.4.2 Protection for persons making a public interest disclosure

The PID Act supports the disclosure of improper conduct (corrupt conduct/ maladministration) or wrongdoing. One of the primary objectives of the act is to provide protections for persons who, in good faith, report wrongdoing. For a complaint to be considered a public interest disclosure it must be assessed against the definitions as per the PID Act. In the department this assessment is conducted by the ESU.

3.4.3 Identification of early warning signs (red flags)

Identifying and acting on possible warning signs (red flags) can play an important role in the early detection of fraud. Fraud awareness training promotes understanding of red flags amongst employees.

Red flags do not indicate guilt or innocence, but they may provide warning signs of possible fraud. Red flags are often categorised as either transactional or behavioural. Transactional red flags refer to unusual or out of the ordinary business or financial transactions. Behavioural red flags refer to unusual behaviours or traits exhibited by a person. Some examples are provided in the table below. It should be noted that a person engaging in fraud will often exhibit a combination of warning signs such as those listed in table 3. It is therefore important to consider the context and the bigger picture.

Table 3 Early Warning Signs (Red Flags)

Transactional Red Flags
• Transaction occurring at an unusual time (e.g. a cab charge receipt for a taxi fare on weekend or public holiday • Frequency of the transaction is unusual (e.g. the transaction may be a one off, or an unusual transaction consistently processed at a certain time by the same person) • Place of transaction is unusual (e.g. corporate card transaction from a casino or clothing store) • Amount of the transaction is unusual (e.g. amount of transaction just under the delegated authority of a person, an invoice split into two halves in order to appear within delegation limits) • Unusual relationships between persons (related parties, over personalised relationship between parties, management performing clerical functions which could easily be delegated to subordinate employees.)
Behavioural Red Flags
• Unexplainable excessive personal lifestyle: expensive cars, jewellery, homes, clothes • Changed performance, conduct or behaviour which may be resultant from gambling alcohol or other drug use • Creditors or collectors appearing/contacting the workplace • Overly familiar, non-professional relationships with contractors/suppliers. • Refusing vacations or promotions • Lack of a strong code of personal ethics • Deliberate disregard of internal controls • Prior criminal history (charges and/or convictions) • Unnecessary retention/control of records or a function • Insisting on working unusual or non-standard business hours • Avoiding or delaying provision of documentation when requested by Auditors • Giving gifts to peers, supervisors or colleagues in positions of influence • Lack of transparency, vagueness or dismissiveness to questions regarding roles, functions or projects.

3.4.4 Continuous Monitoring Program

Continuous monitoring is a powerful means of detecting fraud and other improper behaviour. It is a process of uncovering patterns and relationships in datasets that appear unrelated and it can also highlight discrepancies which may indicate fraud and irregular behaviour. Risk Owners are responsible for ensuring that the continuous monitoring program focuses on key fraud risk areas. The Working Group will oversee the Continuous Monitoring Program, exception report analysis and escalate matters as relevant to the Audit and Risk Committee.

The Continuous Monitoring Program is aimed at the strategic use of digital systems in the identification of fraud indicators. Using continuous monitoring techniques, trends can be examined and investigated which may be indicative of fraudulent conduct or provide information on any outliers.

3.4.5 Detection of Financial transaction fraud or fraud threat

In the event a financial transaction fraud threat or actual financial transaction fraud is detected, employees follow the practical guidance outlined in the document ‘Detection of financial transaction fraud or fraud threat Response protocol’ available on QHEPS.

(https://qheps.health.qld.gov.au/__data/assets/pdf_file/0025/2042683/fraud-response-protocol-2.pdf).

3.4.6 Post-Incident review

The department, through the Working Group, will ensure an effective review process is established following an incidence of significant corruption including fraud. The review process will be after the investigations are completed and a final report is issued. This includes a broader assessment of the issue/s and putting into practice the feedback from lessons learned.

3.4.7 The role of Internal Audit

Internal Audit supports efforts to establish a culture that embraces ethics, honesty, and integrity. Internal Audit assists with the evaluation of internal controls and provides advice to the department’s working group and is a participant on the working group in an advisory capacity

Internal Audit is the third line of defence for assessing the effectiveness of internal controls as per the approved Internal Audit Plan. Internal Audit may provide advice to business areas in relation to fraud and corruption risks and controls

Internal Audit has regular, direct access to the department’s executive via representation in the Audit and Risk Committee.

3.4.8 The role of Risk and Business Continuity Unit

The Risk and Business Continuity Unit (“Risk Unit”) is responsible for updating the Risk Management framework and providing advice to Divisions and BUs on risk assessment and best practices. The Risk Unit will provide a quarterly risk report including the fraud risks to the Audit and Risk Committee.

3.4.9 External Audit

The department will take a proactive approach and will liaise with the Queensland Audit Office (QAO) to facilitate the exchange of information in relation to the prevention and detection of fraud and will respond quickly to concerns identified during the course of external audit work.

3.4.10 Fraud Control Officers

As outlined in the Fraud Control Standard, departmental managers, risk owners, and the Departmental Leadership Team are responsible for identifying, assessing, managing and monitoring the fraud risks within their area of operations as the first line of defence. The Divisions/BUs may have local staff carrying out second line of defence activities including oversight and management functions. The CFO is accountable for the financial control framework.

As a second line of defence, the RAIM Branch has Fraud Control Officers with specialist skills, qualifications and experience who work together to lead fraud and corruption control policy, planning and programs within Queensland Health: Executive Director RAIM Branch, Director Governance and Principal Fraud Control Program Officer.

- The Executive Director oversees the overall program implementation, monitoring and reporting.
- Director Governance works together with the Executive Director and Principal Fraud Control Program Officer to develop and maintain departmental policies and standards.
- The Principal Fraud Control Program Officer ensures current best practice in fraud control is integrated into training and development programs, works with the Director Governance and the

Executive Director to develop and maintain departmental policies and standards, and works with the relevant risk owners and working group to manage the department's exposure to fraud risk. The Principal Fraud Control Program Officer provides the bi-annual FCAP report to the Director Governance and Executive Director on the effectiveness
s of the metrics and targets in FCAP.

3.4.11 Tasks for Fraud Detection

Where appropriate, fraud detection measures should be communicated and promoted to all employees. Awareness of detection measures often acts as a deterrent and therefore, a preventative measure. Additional best practice tasks for fraud detection include the following:

- The Director-General and/or the Audit and Risk Committee and/or Executive Director RAIM Branch may request audits/reviews of specific areas of concern.
- Reinforcing to employees their obligations to report wrongdoing.
- Ongoing monitoring of the fraud risks and control effectiveness by the risk owners and working group.
- Deep dive fraud risk assessment.

3.5. Response, Outcomes and Recovery

3.5.1 Assessing and managing complaints of suspected corruption (including fraud)

The ESU shall respond to reports of suspected corrupt conduct (including fraud) by:

- Assessing each matter to determine whether or not it meets the thresholds for corrupt conduct and public interest disclosures.
- Conducting internal investigations where appropriate or engage external investigators.
- Providing appropriate assistance and/or guidance to the relevant business unit on management of the incident/matter.
- If the matter could amount to corrupt conduct, making appropriate referrals to the CCC
- If the matter is assessed as a public interest disclosure, making appropriate referrals to the office of the Queensland Ombudsman.
- Where appropriate, referring serious allegations of suspected criminal conduct to the Queensland Police Service (QPS) on behalf of the department.
- Overseeing and coordinating investigations in accordance with the CCC guidelines as outlined in their publication 'Corruption in Focus'.
- Providing quarterly updates to the Working Group on categories of complaints in relation to fraud or corruption.
- Reporting on system weaknesses to relevant internal and external stakeholders e.g. RAIM Branch, Working Group and Audit and Risk Committee.

3.5.2 External investigation procedures

In Queensland's public sector there are a number of independent agencies responsible for promoting governance, accountability, integrity and provision of law enforcement including:

- The CCC
- The QAO
- The Queensland Ombudsman
- The Queensland Police Service (QPS).

The Director-General, Queensland Health has a duty to notify the CCC of suspected corrupt conduct as per Section 38 of the *Crime and Corruption Act 2001*. The Director-General delegates this function to the Director ESU.

If assessed as corrupt conduct, the CCC will advise the appropriate action which may include:

- Refer the complaint to the department to deal with, subject to some level of review or audit by the CCC.
- Ask the department to carry out further enquiries before a final assessment is made.
- Investigate the complaint itself
- Investigate the complaint in cooperation with the relevant public official
- Refer possible criminal activity to the QPS.

The department will ensure that investigators are appropriately appointed, experienced and accredited.

In all cases of suspected corrupt conduct, including alleged fraud, the QPS will inform the initial assessment process by advising the department whether or not it is in the public interest for the Queensland Police Service to involve themselves in the matter.

3.5.3 Reviewing systems and procedures post, audit, investigation or inquiry

The RAIM Branch and/or ESU will work with relevant stakeholders to reassess the adequacy of the internal control environment and actively plan and implement improvements where required. Reviews of systems and procedures may arise from investigations into an alleged fraud, an audit (internal or external) or a system review of a specific function or area. ESU will raise recommendations to improve controls based on investigations.

3.5.4 Information sharing

Information pertaining to fraud or corruption related events (internal or external to the department), trends and analysis of data will be shared with relevant stakeholders. This will be coordinated by the ESU in consultation with the CCC.

The ESU will advise the Director-General and develop Ministerial Briefs and other communication for any potential or actual incident or on request from the Minister.

3.5.5 Provision of information to external agencies

The department shares relevant information with external agencies (e.g. the CCC, QPS, QAO, Office of Health Ombudsman) as identified in the Standard.

The Strategic Communications Branch will communicate with the media and handle any negative publicity in a timely manner, in response to a fraud and corruption incident.

3.5.6 Disciplinary action

Action taken in response to allegations of fraud and corruption will be in accordance with relevant legislation, policies and the principles of natural justice.

The management of discipline in the department is contained in the Discipline HR Policy E10 and the responsible delegates are detailed in the Human Resource Delegations. The appropriate delegate will consider reasonable management and/or disciplinary action against staff resulting from substantiated allegations of fraud or corruption. Action may include, but is not limited to: reprimand, reduction of the level of remuneration, transfer or redeployment or termination of employment.

The department may undertake the necessary disciplinary action against an employee.

3.5.7 Recovery of losses

The department is committed to maximising the recovery of losses incurred from fraud and corruption activities and will pursue every possible avenue in doing so through the appropriate agencies and legal avenues. The recovery of losses will limit the financial impact this may have on the department's objectives.

Finance Branch is responsible for notifying the Queensland Government Insurance Fund of any potential claim under the insurance cover. Finance Branch will also ensure that the actual losses are recorded and allocated to the relevant cost centres where the loss has occurred.

The Finance Branch in consultation with ESU, Legal Branch and relevant external agencies will determine and proceed for recovery of losses through civil or criminal proceedings to maximise the recovery of the losses.

4. Legislation

- *Ambulance Service Act 1991*
- *Crime and Corruption Act 2001*
- *Criminal Code Act 1899*
- *Criminal Proceeds Confiscation Act 2002*
- *Financial Accountability Act 2009*
- *Financial and Performance Management Standard 2009*
- *Hospital and Health Boards Act 2011*
- *Public Interest Disclosure Act 2010*
- *Public Sector Ethics Act 1994*
- *Public Service Act 2008*

5. Supporting documents

External Publications

- *Australian Standard Fraud and Corruption Control AS 8001-2008*
- *Code of Conduct for the Queensland Public Service 2011*
- *Crime and Corruption Commission, Queensland Ombudsman, and Public Service Commission "Managing a Public Interest Disclosure Program. A guide for public sector organisations 2011"*
- *Crime and Corruption Commission Fraud and Corruption Control- Best Practice Guide March 2018*
- *Corruption in Focus (Crime and Corruption Commission)*
- *Public Service Commission: Discipline Guidelines 01/17*
- Public Service Commission: Employment screening 7/11
- *Public Service Commission: Directive 22/09 Gifts and Benefits*
- *Public Service Commission: Guidelines Gifts and Benefits 2010*
- *Queensland Procurement Policy*

- *Queensland Ombudsman: Public Interest Disclosure Standard No.1, 2 and 3 2019*

Internal policy

- Control Framework for Expenditure (2016)
- Discipline HR Policy E10 (QH-POL-124)
- Employment Screening HR Policy B40 (QH-POL-122)
- Employee Complaints HR Policy E12
- Fraud and Corruption Control Policy (QH-POL-295)
- Financial Management Practice Manual (FMPM)
- Public Interest Disclosures HR Policy I5 (QH-POL-202)
- Risk Management Policy (QH-POL-070)
- Recruitment and Selection Policy HR Policy B1 (QH-POL-212)
- Requirements for Reporting Corrupt Conduct HR Policy E9 (QH-POL-218)
- Supplier Due Diligence Guide
- Workplace Conduct and Ethics HR Policy E1

6. Definitions

Term	Definition
Collusion	Secret or illegal cooperation or conspiracy in order to deceive others; Law collusion between ostensible opponents in a lawsuit
Confidential Information	Confidential information means all information that is: a) by its nature confidential to Queensland Health; b) is designated or described as being confidential; c) an employee, contractor or consultant knows or ought to know is confidential to Queensland Health and includes: d) information which relates to Intellectual Property Rights of Queensland Health and its Personnel; e) information concerning clinical processes, policies, commercial operations, financial arrangements, information technology systems and programs or other affairs of Queensland Health; f) information that is defined as 'confidential information' by Queensland Health portfolio legislation, including the Hospital and Health Boards Act 2011 (Qld) and Public Health Act 2005 (Qld); and g) information that is defined as 'personal information' under the Information Privacy Act 2009 (Qld).

Term	Definition
Corrupt Conduct	As per Section 15(1) of the Crime and Corruption Act 2001, corrupt conduct is conduct that: • adversely affects, or could adversely affect, the performance of functions or the exercise of powers of a unit of administration or a person holding an appointment; and • is not honest or impartial; or involves a breach of trust (knowingly or recklessly); or involves a misuse of information; and • would, if proven, be a criminal offence or a disciplinary breach providing reasonable grounds for termination of the person's employment. As per Section 15(2) of the Crime and Corruption Act 2001, corrupt conduct is conduct that: • impairs, or could impair, public confidence in public administration; and • involves, or could involve: ▪ collusive tendering; ▪ fraud relating to an application for a licence, permit or other authority under an Act with a purpose of protecting health or safety of persons, protecting the environment, or protecting or managing the use of the State's natural, cultural, mining or energy resources; ▪ dishonestly obtaining, or helping someone to dishonestly obtain, a benefit from the payment or application of public funds or the disposition of State assets; ▪ evading a State tax, levy or duty or otherwise fraudulently causing a loss of State revenue; ▪ fraudulently obtaining or retaining an appointment; and ▪ would, if proven be a criminal offence or a disciplinary breach providing reasonable grounds for termination of the person's services, if the person is or were the holder of an appointment. For the full definition, please refer to section 15 of the *Crime and Corruption Act 2001.*
Corruption	Dishonest activity in which an employee of an organisation acts contrary to the interest of the organisation, in order to achieve some gain or advantage, or to avoid loss or disadvantage, for the employee or for another person or entity. Corruption can include, but is not limited to, behaviour such as fraud, deception, misuse of position or authority (Australian Standard 8001:2008 *Fraud and Corruption Control*)

Term	Definition
Formal Investigation	Pursuant to s190 of the *Hospital and Health Boards Act 2011*, a 'formal' investigation process involves the appointment or engagement of an investigator by the Director-General, or delegate. The investigation is a focused and detailed examination or inquiry, for which an investigator(s) is appointed to uncover facts and determine the truth of an allegation. This may include collecting, processing, analysing, storing, and evaluating evidence and providing findings and recommendations. The final product of a formal investigation is an investigation report. After considering the report, the Director-General, or delegate, may take the action he or she considers appropriate in relation to the matters identified in the report.
Fraud	Dishonest activity causing actual or potential loss to any person or entity including theft of moneys or other property by employees or persons external to the entity and where deception is used at the time, immediately before or immediately following the activity. This also includes the deliberate falsification, concealment, destruction or use of falsified documentation used or intended for use for a normal business purpose or the improper use of information or position for personal financial benefit (from Australian Standard 8001:2008 *Fraud and Corruption Control*). A Criminal Offence as defined in Section 408C of the *Criminal Code Act 1899*. *For example: false claims on a CV, using a cab voucher for personal travel, falsely making a claim on a timesheet, false invoicing, unauthorised use of credit cards, theft of intellectual property or other confidential information, falsifying time-sheets to claim overtime not worked.*
Fraud Risk	The effect of possible fraud on the objectives of the department, division and/or business unit.
Fraud Risk Owner/Risk Owner	A person with the accountability and authority to manage a risk A position with the most responsibility for the risk Most responsible means able to coordinate risk treatments and engage with other business areas that may have some responsibility for an aspect of the risk and/or delegation to support risk treatment. As a matter of principle, each risk has only one Risk Owner.

Term	Definition
Maladministration	An administrative action that— (a) was taken contrary to law; or (b) was unreasonable, unjust, oppressive, or improperly discriminatory; or (c) was in accordance with a rule of law or a provision of an Act or a practice that is or may be unreasonable, unjust, oppressive, or improperly discriminatory in the particular circumstances; or (d) was taken— (i) for an improper purpose; or (ii) on irrelevant grounds; or (iii) having regard to irrelevant considerations; or (e) was an action for which reasons should have been given, but were not given; or (f) was based wholly or partly on a mistake of law or fact; or (g) was wrong
Misconduct	Inappropriate or improper conduct in an official capacity; or in a private capacity that reflects seriously and adversely on the public service.
Natural Justice	Natural justice is an administrative law principle that provides for fairness in decision-making. It is concerned with ensuring that an objective decision maker reaches a procedurally fair decision. Natural justice has two rules: • Rule against bias: decision-makers are to be objective, free of bias, and have no personal interest in the matter being decided. • Hearing rule: an individual is to be informed of the substance of an allegation/s against them and have the opportunity to present their case prior to decision being made.
Public interest disclosure (PID)	A public interest disclosure is a disclosure under Section 12 and Section 13 of the *Public Interest Disclosure Act* and includes all information and help given by the discloser to a proper authority for the disclosure.
Staff/Employees (including contractors and consultants)	For the purposes of this policy the term 'staff' refers to all Department of Health employees, and all individuals acting as its agents or consultants.
Stealing / Theft	Theft is dealt with under Sections 391 of the Criminal Code *For example:* *an employee steals a laptop or TV belonging to Department of Health without consent and with the intention of not returning the laptop or TV.*

Term	Definition
Working Group	Working Group contributes to the effective risk management, implementation of fraud and corruption control and drive consistency and visibility of continuous monitoring activities. The Working Group reports the results to the Department Leadership team and the Audit and Risk Committee

Version Control

Version	Date	Comments
Version 1.0	March 2015	Scheduled review by Risk and Governance Unit
Version 1.1	17 June 2015	Policy Rationalisation Project- Minor editorial changes. Migration of content
Version 2.0	21 August 2019	Scheduled review by Risk, Assurance and Information Management Branch - Inclusion of graphical representation for the fraud framework, clarification of responsibility for handing negative publicity, notification, recovery, allocation of losses and other general updates.