Fraud Response Plan

Author : Associate Director of Financial Accounting

Version : 3

Date : August 2024

Introduction

The University's activities require significant funds, much of which are 'public'; as a publicly-funded body, the University is accountable to a wide range of stakeholders for the use and management of those funds, and the associated controls.

It is the responsibility of all University officers and staff to ensure that University funds and resources are used honestly and correctly, and to report any circumstances which may indicate their improper use. Channels to make such reports are covered later in this plan.

Proactive fraud prevention is the primary counter-fraud related objective of any University - but when fraud is suspected or indicated, it is essential that prompt and professional reactive action is taken, and it is here where the need for trained fraud 'first-responders' within the University is clear.

Primary responsibility for the prevention and detection of fraud rests with officers and staff who also have responsibility to manage the risk of fraud. Investigation of fraud is the overall responsibility of the Chief Operating Officer, supported by fraud first-responders or other trained investigators and the project team that may be set up to investigate selected cases.

The University's Fraud Response Plan detailed below outlines the process to be adopted if suspected fraud is reported or detected; the Appendices also contain a range of useful information, including potential fraud indicators or warning signs.

What is Fraud?

The term fraud is a broad and widely-used term to describe a number of fraudulent-type activities that include theft, false accounting, misappropriation, bribery, corruption, deception and collusion. Some definitions of these and related terms are contained in Appendix A.

In general, a fraud may be described as any type of deception that results in a gain to one party and/or a loss to another, in this case the University. The Fraud Act 2006 outlines three classes of fraud:

1. Fraud by false representation
2. Fraud by failing to disclose information
3. Fraud by abuse of position.

Additionally, theft - such as the removal and/or misuse of funds, assets or cash - is not prosecuted as a fraud but falls under the various Theft Acts.

In terms of the University's Fraud Response Plan, fraud may be defined as deception with the intention of:

- Gaining an advantage, personally and/or for friends and relatives;
- Avoiding liability; or,
- Causing a financial and/or reputational loss to the University or one of its subsidiary organisations.

The main types of irregularity are:

- Theft: As above;
- False accounting: dishonestly destroying, defacing, concealing or falsifying any account, record or documents required for any accounting purpose, with a view to personal gain or gain for another, or with the intent to cause loss to the University or subsidiary or furnishing information which is or may be misleading, false or deceptive;
- Abuse of position: This is where fraud is committed by a person or people by virtue of their position, or authority where they are expected to safeguard another's financial interests (e.g. that of the University as their employer) or not act against those interests.

Whilst they can be very varied in nature, some examples of these irregularities within the University context include:

- Abuse of the expenses process and system;
- Abuse of recruitment processes, including failure to disclose relevant information;
- Use of the University logo and/or letterhead for personal gain;
- Abuse of the research grants, including misrepresentation and/or 'siphoning' of funds for personal gain;
- Abuse of procurement processes;
- Conflicts of Interest.

Fraud Response Plan - Purpose

In summary, the purpose of the Fraud Response Plan is to define authority levels, responsibilities for action and reporting lines in the event of a suspected fraud or financial irregularity. The use of the plan should allow the University to:

- Respond quickly and professionally to any suspicion or suggestion of fraud or irregularity;
- Assign responsibility for initial and subsequent investigation;
- Prevent further loss;
- Establish and secure evidence necessary for disciplinary and/or criminal action against those who have committed the fraud;
- Notify our regulator if required;
- Notify the University's insurers if required;
- Minimise and recover losses;
- Establish an internal and external communications strategy and process;
- Establish the need (or otherwise) for external specialist involvement;
- Establish the need for police notification, and the lines of communication;
- Review the circumstances of the fraud, actions taken to prevent a recurrence and any action needed to strengthen future responses to fraud;
- Deal with HR-type issues such as references in relation to staff disciplined and/or prosecuted for fraud.

It is therefore important that the plan covers the following 15 key stages:

1. Initial Response
2. Initial Reporting
3. Meeting of the Fraud Response Team
4. The Lead Investigator's plan
5. Communications during, and after, the investigation
6. Establishing and securing evidence
7. Staff under suspicion
8. Interviewing/statements
9. Police involvement
10. Prevention of further losses
11. Recovery of losses
12. Administration, including HR-type issues such as references
13. Reporting, including notifying OfS
14. Review, communication and action on findings
15. Closure.

Initial Response

A fraud or financial irregularity may be discovered in a variety of ways, from your own or a colleague's observations, someone from inside or outside the University 'blowing the whistle', financial controls identifying a discrepancy, internal or external audit discovering a problem or external bodies identifying an issue.

A fraud or financial irregularity may also come to light through:

- The University's public interest disclosure policy;
- The University's disciplinary procedures;
- The University's procedures for addressing misconduct;

- Disclosure by the person, or persons, involved.

Irrespective of how a potential fraud is discovered, the following - Things to do, Things not to do and Things to remember - should always be borne in mind:

Things to do:

1. Stay calm - remember you are a witness not a complainant.
2. If possible, write down your concerns immediately - make a note of all relevant details such as what was said in phone or other conversations, the date, the time and the names of anyone involved.
3. Consider the possible risks and outcomes of any immediate action you may take.
4. Make sure that your suspicions are supported by facts, as far as is possible at this stage.

Things not to do:

1. Don't become a private detective and personally conduct an investigation or interviews.
2. Don't approach the person/persons potentially involved (this may lead to conflict, violence, him/her destroying evidence etc.)
3. Don't discuss your suspicions or case facts with anyone other than the Fraud Response Team unless specifically asked to do so by them.
4. Don't use the process to pursue a personal grievance.

Things to remember:

1. You may be mistaken or there may be an innocent or good explanation - but this will come out in the investigation.
2. The fraud response and investigation process may be complex and relatively lengthy and, as a consequence, you may not be acknowledged immediately. Moreover, the situation may lead to a period of disquiet or distrust in the University despite you having acted in good faith.
3. Any decision on changes to the maintenance of confidentiality will be made by the Fraud Response Team.

Fraud - Initial Reporting

All actual or suspected incidents should be reported immediately either:

- To the Chief Operating Officer and/or the Associate Director Financial Reporting or, in their absence, the University Secretary.

- Via the University's whistle-blowing process; provided reports are made in good faith then an individual is generally protected by the University and the law against retribution, harassment or victimisation and the individual's confidentiality must be preserved.

If the disclosure involves or implicates any members of the Fraud Response Team then the disclosure should be made to the Vice Chancellor and/or the Chair of the University's Board of Governors and/or the Chair of Audit and Risk Committee as appropriate.

Meeting of the Fraud Response Team

As soon as practicable (ideally within 24 hours) a meeting of the Fraud Response Team should be convened, normally consisting of the following group to decide on the initial response:

- Vice-Chancellor or Chief Operating Officer;
- University Secretary;
- Executive Director of People;
- Associate Director Financial Reporting.

It may also be necessary to involve colleagues from the communications team if there are potential public relations and/or media issues. This group will decide:

- Whether an investigation is required;
- Who should lead the investigation;
- Who should undertake the investigation and the composition of any project group set up to co-ordinate the investigation;
- Whether, and at what stage, Internal Audit need to be involved in the investigation - and whether a special audit is warranted;
- Whether the staff member or members need to be suspended;
- Whether the matter should be reported to the police;
- What stakeholder communications should be undertaken at this stage e.g. advising the Chair of the Board of Governors or of the Audit Committee.

Guidance for managers on receiving a report of fraud

Managers who receive a report of a fraud should:

- Listen to the concerns of your staff and treat every report you receive seriously and sensitively. Make sure that all staff concerned are given a fair hearing, bearing in mind that they could be distressed, upset and/or frightened;
- Reassure your staff that they will not suffer because they have told you of their suspicions, as long as they are made in good faith;
- Get as much information as possible. Do not interfere with any evidence and make sure it is kept in a safe place;

- Ask the member of staff to keep the matter fully confidential in order that it can be investigated without alerting the suspected/alleged perpetrator.

Establishing and securing evidence, and interviewing/statements

The University will follow standard and established disciplinary procedures against any member of staff who has committed fraud. Additionally, the University will normally consider prosecution of any such individual. The investigators will ensure that:

- Evidentiary requirements and standards are met during any fraud investigation;
- Staff involved in fraud investigations are familiar with and follow rules on the admissibility of documentary and other evidence in criminal proceedings;
- Where required, external forensic services (such as IT) meet evidentiary requirements and standards, such as those relating to continuity of evidence.

Where the initial investigation provides reasonable grounds for suspecting a member or members of staff of fraud, the Fraud Response Team will decide how to prevent further loss. This may require the suspension of the individual(s) suspected of fraud and removal of physical (i.e. campus, building and office) and systems access rights. Any suspension will be in accordance with University's disciplinary procedures but it may be necessary to plan the timing of suspensions to prevent individuals from destroying or removing evidence that may be needed to support the investigation process. However, it should be recognised that there may occasionally be circumstances where it is decided to allow a fraud - and associated losses - to continue to identify, for example, further culprits.

When interviewing employees under suspicion it must be made clear whether it is a formal interview or an informal discussion. It should be explained that the University and the interviewers have no pre-set view, the suspicion should be outlined and the employee given adequate time to respond.

If it is decided that formal questioning is needed because potential involvement in a criminal offence is suspected, then the interview should be conducted in accordance with the principles of the UK Police and Criminal Evidence Act (PACE). Guidelines can be found on the Home Office Website.

PACE provides protection for the individual and ensures that any evidence collected through interviews, (including the taking of statements) can be presented in court, whether or not such interviews are being carried out under caution. PACE covers such rights as the right to silence, to legal advice, not to be held incommunicado, to accurate recording and protection against evidence obtained through oppression.

Because of this, very early consideration should be given to police involvement, or consultation in these circumstances. Legal advice should also always be sought, recognising that there may be variations in local legislation where an overseas campus, for example, is involved. Interviews should only be carried out with the approval of the Fraud Response Team. There are strict rules relating to tape

recorded interviews and investigators must be suitably trained, skilled and experienced if these are to be used.

Ideally, statements should be taken from witnesses using their own words. The witness must be happy to sign the resulting document as a true record - the witness can be given a copy of the statement if desired. It is also very important to keep contemporaneous notes on file, in the event that they are needed for future reference (e.g. court, tribunal or disciplinary hearing).

Police involvement

At some point a decision will need to be made as to whether an incident is reported to the police. However, even if it is reported there needs to be an element of realism as to the likely extent of police involvement. For large-scale frauds, it may be appropriate to ask the police to attend meetings of the Fraud Response Team.

The lead investigator should prepare an 'Evidence Pack' that can be handed to the police at the time the fraud is reported, and a Crime Reference Number obtained. The Evidence Pack should include a summary of the fraud, highlighting (where known) the amount, the modus operandi, and the location, and including photocopies of key supporting documents and contact details of the person leading the investigation. All contact with the police should be channelled through one person which would generally be the investigator or, possibly, the communications lead (i.e. the person leading the investigation).

Recovery of losses

Recovering losses is clearly a major objective of any fraud response investigation. Internal Audit or those investigating the incident should ensure that in all fraud investigations the amount of any loss is quantified. Repayment of losses should be sought in all cases.

Where the loss is (potentially) substantial, legal advice should be obtained without delay about the need to freeze an individual's assets through the courts pending the conclusion of the investigation. Legal advice should also be sought about the prospects for recovering losses through the civil court in circumstances where the perpetrator(s) refuse repayment. The University would normally expect to recover costs in addition to losses. The University's insurers should be involved in such cases and, indeed, their notification (above) may be a mandatory requirement of cover.

Administration, including HR-type issues such as references

Careful administration of the investigation is of vital importance. A disordered investigation, without clear records and logs of events, communications, key dates etc., will cause problems at any court hearing, tribunal or disciplinary panel. It is equally important that confidentiality is kept both for paper and electronic (e-mail)

communications. Where e-mail is used for communication, subject names that have no direct link to the investigation should, for example, be considered.

Within the employment law framework, HR must deal with any requests for references from staff who have been disciplined or prosecuted for fraud and related issues.

Reporting, including notifying regulators

The Fraud Response Team should provide a confidential and regular report to the Chair of the Audit and Risk Committee, the Vice Chancellor, the external audit partner and other nominated individuals at an agreed frequency. The scope of the report should include the circumstances surrounding the case, contributory factors and progress with the investigation.

Any incident meeting the criteria for a report to regulators should be reported without delay to the Vice-Chancellor, the Chair of the Audit and Risk Committee and the Chair of the Finance and Resources Committee where there is a (potential) financial loss. The Team should also consider if incidents not meeting the criteria should be reported, both to the regulator as well as to sector fraud alert networks, to anonymously warn other sector bodies of potential risks.

Review, communication and action on findings

On completion of the investigation the Fraud Response Team should submit to the Audit and Risk Committee a report typically containing:

- A description of the incident, including the value of any loss, the people involved and the means of perpetrating the fraud;
- Actions taken to prevent recurrence; and,
- A plan detailing any recommendations and actions (with timings) required to strengthen future fraud responses.

Appendix A –Definitions

Fraud:

1. Wrongful or criminal deception intended to result in financial or personal gain
2. A person or thing intended to deceive others, typically by unjustifiably claiming or being credited with accomplishments or qualities
3. A false representation of a matter of fact - whether by words or by conduct, by false or misleading allegations or by concealment of what should have been disclosed
4. A deception practiced in order to induce another to give up possession of property or surrender a right

Corruption:

1. The use of public office for private gain
2. Dishonest or fraudulent conduct by those in power, typically involving bribery

Bribery:

1. The offering, giving, receiving, or soliciting of something of value for the purpose of influencing the action of an official in the discharge of his or her duties
2. Money, favour or benefit given or promised in order to influence the judgment or conduct of a person in a position of trust

Theft:

1. The illegal taking of someone else's property without that person's freely-given consent. Apart from the obvious theft of physical assets such as computers, stock and money, it includes:
2. Misappropriation of funds
3. Misuse of assets, including cash, stock and other assets, for example ‘borrowing’ petty cash, use of photocopiers for private purposes
4. Theft from a client or supplier
5. Theft of intellectual property, including designs and data

Deception:

1. To intentionally distort the truth in order to mislead others. It would include obtaining property, services or pecuniary advantage by deception or evading liability. Deceptions typically include:
2. Misrepresentation of qualifications to obtain employment
3. Obtaining services dishonestly via technology
4. Undeclared and unauthorised private and consultative work

Forgery:

1. Making or adapting objects or documents with the desire to deceive

Extortion:

1. Obtaining money or property from another through coercion or intimidation

Embezzlement

1. Fraudulent appropriation by a person to their own use of property or money entrusted to that person's care but owned by someone else

Conspiracy:

1. An agreement between two or more persons to break the law at some time in the future

Collusion:

1. Any case in which someone incites, instigates, aids and abets, conspires or attempts to commit any of the crimes of fraud

Money Laundering:

1. How criminals process illegal or dirty money derived from the proceeds of any illegal activity through a succession of transactions and deals until the original source of such funds has been obscured and the money take on an appearance of legitimate or clean funds - involves placement, layering and integration of the money

Appendix B: Examples of controls to prevent and detect fraud

- Comprehensive recruitment procedures, with full reference checks
- Physical security of assets
- Adequate supervision and workload management
- Separation of duties to ensure that key functions and controls are not performed by the same person
- Rotation of staff
- Random spot checks
- Complete and secure audit trails
- Appropriate performance monitoring
- Frequent budgetary and other financial reviews/reports
- Periodic reviews by independent bodies such as Internal Audit

Appendix C: Warning signs of fraud and fraud indicators

Warning signs can include:

- Staff under stress without a high workload
- Reluctance to take annual leave
- Being first to arrive in the morning and last to leave in the evening
- Refusal of promotion
- Unexplained wealth
- Sudden change of lifestyle
- Suppliers/ contractors who insist on only dealing with one staff member
- Individuals seen as risk-takers or rule-breakers
- Disgruntled at work and/or not supportive of the University

Fraud Indicators can include:

- Staff exhibiting unusual behaviour (see list above)
- Missing key documents, especially invoices and/or contracts
- Inadequate or no separation of duties
- Documentation which is photocopied or missing key information
- Missing expenditure vouchers
- Excessive variations to budgets and/or contracts
- Bank and ledger reconciliations not regularly preformed and cannot be balanced
- Numerous adjustments or exceptions
- Overdue pay or expense advances
- Duplicate payments
- Ghost employees on payroll
- Large payments to individuals
- Lack of bank account controls
- Crisis management coupled with a pressured work environment
- Lowest tenders or quotes passed over without adequate explanation
- Single vendors
- Climate of fear/low staff morale
- Consistent failure to implement key controls
- Controls frequently overridden

Appendix D: Example checklist to be used by those considering whether a fraud has been committed

This document provides a list of generic indicators of potential fraud. These include personal and organisational motives for fraud, possible weakness of internal controls, transactional indicators and possible methods of committing and concealing fraud. The document may be helpful for use as a reference document or a checklist where concerns exists that fraudulent activity may be taking place.

For your own internal use if required:

Name: **Position:** **Date of completion:**

Ref.	Area	Response
1	***Possible Personal Motives***	
1.1	Personnel believe they receive inadequate compensation and/or rewards (recognition, job security, vacations, promotions etc.)	
1.2	Expensive lifestyle (cars, trips etc.)	
1.3	Personal problems (gambling, alcohol, drugs, debt, etc.)	
1.4	Unusually high degree of competition/peer pressure	
1.5	Related party transactions (business activities with personal friends, relatives or their companies)	
1.6	Conflicts of interest	
1.7	Disgruntled employee (recently demoted, reprimanded etc.)	
1.8	Recent failure associated with specific individual	
1.9	Personal animosity or professional jealousy	
2	***Possible Organisational Motive***	
2.1	Organisation experiencing financial difficulty	
2.2	Commercial arm experiencing financial difficulty	
2.3	Tight or under unusually tight time deadlines to achieve level of outputs	
2.4	Organisation closely identified with/dominated by one individual	
2.5	Organisation under pressure to show results (budgetary, exam results etc.)	
2.6	Organisation recently suffered disappointment/reverses/consequences of bad decisions	
2.7	Organisation wants to expand its scope, obtain additional funding	

Ref.	Area	Response
2.8	Funding award up for continuation	
2.9	Organisation due for a site visit by auditors or other quality controllers	
2.10	Organisation has for-profit component	
2.11	Organisation recently affected by new/changing conditions (regulatory, economic, environmental etc.)	
2.12	Organisation faces pressure to use or lose funds to sustain future funding levels	
2.13	Record of previous failure(s) by one or more organisational areas	
2.14	Sudden change in organisation practice or pattern of behaviour	
3	**Internal Controls Are Weak**	
3.1	Management demonstrates lack of attention to ethical values; lack of communication regarding importance of integrity and ethics, lack of concern about presence of temptations and inducements to commit fraud, lack of concern regarding instances of fraud, no clear fraud response plan or investigation policy	
3.2	Management fails to specify needed levels of competence	
3.3	Management displays a penchant for taking risks	
3.4	Lack of an appropriate organisational and governance structure with defined lines of authority and reporting responsibilities	
3.5	Institution lacks policies and communication relating to individual accountability and best practices e.g. procurement, travel and subsistence, use of alcohol, declarations of interest	
3.6	Lack of personnel policies and recruitment practices	
3.7	Institution lacks personnel performance appraisal measures or practices	
3.8	Management displays lack of commitment towards the identification and management of risks relevant to the preparation of financial statements; does not consider significance of risks, likelihood of occurrence or how they should be managed	
3.9	There is inadequate comparison of budgets with actual performance and costs, forecasts and prior performance, no regular reconciliation of control records and lack of proper reporting to governing body	
3.10	Management of information systems is inadequate; no policy on information technology security, computer use and access, verification of data accuracy completeness or authorisation of transactions	

Ref.	Area	Response
3.11	There is insufficient physical security over facilities, assets, records, computers, data files, cash; failure to compare existing assets with related records at reasonable intervals	
3.12	There is inadequate or inappropriate segregation of duties regarding initiation, authorization and recording of transactions, maintaining custody of assets	
3.13	Accounting systems are inadequate; ineffective method for identifying and recording transactions, no tracking of time periods during which transactions occur, insufficient description of transactions and to which account they should be allocated to, no easy way to know the status of funds on a timely basis, no adequate procedure to prevent duplicate payments or prevent missing payment dates, etc.	
3.14	There is a lack of internal, ongoing monitoring of controls which are in place; failure to take any corrective actions, if needed	
3.15	Purchasing systems/procedures inadequate; poor or incomplete documentation of purchase, payment, receipt; poor internal controls as to authorization and segregation of duties	
3.16	Subcontractor records/systems reflect inadequate internal controls	
3.17	Management is unaware of or displays lack of concern regarding applicable laws and regulations e.g. Companies Acts, Charities Acts, Funding Agreement, Child Protection	
3.18	Specific problems and/or reportable conditions identified by audits or other means of oversight have not been corrected. This may include a history of problems, a slow response to past findings or problems, or unresolved present findings	
3.19	No mechanism exists to inform management and governors of possible fraud	
3.20	General lack of management oversight	
4	**Transactional Indicators**	
4.1	Related party transactions with inadequate, inaccurate or incomplete documentation or internal controls (business/research activities with friends, family members or their companies)	
4.2	Not-for-profit entity has a for-profit counterpart with linked infrastructure (shared board of governors or other shared functions and personnel)	
4.3	Specific transactions that typically receive minimal oversight	
4.4	Previous audits with findings of	

Ref.	Area	Response
	• questioned costs • evidence of non-compliance with applicable laws or regulations • weak internal controls • inadequate management response to any of above • a qualified opinion	
4.5	Transactions and/or accounts which are difficult to audit or subject to management judgment and estimates	
4.6	Multiple sources of funding with inadequate, incomplete or poor tracking, failure to segregate funds and/or existence of pooled funds	
4.7	Unusual, complex or new transactions, particularly if occur at year end, or end of reporting period	
4.8	Transactions and accounts operating under time constraints	
4.9	Cost sharing, matching or leveraging arrangements where industry money or other donation has been put into a foundation (as in a foundation set up to receive gifts) without adequate controls to determine if money or equipment has been spent/used; whether it has gone to allowable costs and at appropriate and accurate valuations; outside entity such as foundation provided limited access to documentation	
4.10	Travel accounts with • inadequate, inaccurate or incomplete documentation or poor internal controls such as appropriate authorisation and review • variances between budgeted amounts and actual costs • claims in excess of actual expenses • reimbursement for personal expenses • claims for non-existent travel • duplicate payments	
4.11	Credit card accounts with inadequate, inaccurate or incomplete documentation or internal controls such as appropriate authorisation and review	
4.12	Accounts in which activities, transactions or events involve handling of cash or wire transfers; presence of high cash deposits maintained with banks	
4.13	Assets and inventory are of a nature to be easily converted to cash (small size, high marketability, lack of ownership identification, etc.) or easily converted	

Ref.	Area	Response
	to personal use (cars, houses, equestrian centres, villas etc.)	
4.14	Accounts with large or frequent shifting of budgeted costs from one line item to another without adequate justification	
4.15	Payroll (including fringe benefits) system with controls that are inadequate to prevent an individual being paid twice, or paid for non-delivery or non-existence; or outsourced but poor oversight of starters / leavers and payments	
4.16	Consultant agreements which are vague as to work, time period covered, rate of pay, product expected; lack of proof that product or service actually delivered	
4.17	Subcontract agreements which are vague as to the time period covered, the rate of pay, the product expected, or lack of proof that product or service actually delivered	
5	**Possible methods of committing/concealing fraud**	
5.1	Auditee issues such as: • Refusal or reluctance to turn over documents • Unreasonable explanations • Annoyance at questions • Trying to control the audit process (timetables, access, scope) • Auditee blames a mistake on a lack of experience with financial requirements or regulations governing funding • Promises of cooperation followed by subsequent excuses to limit or truncate co-operation • Subtle resistance • Answering a question that wasn't asked • Offering more information than asked • Providing wealth of information in some areas, little to none in others • Explaining a problem by saying "we've always done it that way", or "someone at Xx told us to do it that way" or "Mr X said he'd take care of it" • A tendency to avoid personal responsibility (overuse of "we" and "our" rather than "I"); blaming someone else • Too much forgetfulness • Trying to rush the audit process	
6	**Record Keeping/Banking/Other**	
6.1	Issues with documents such as:	

Ref.	Area	Response
	• Missing documents • Documents are copies, not originals • Documents in pencil • Altered documents • False signatures/incorrect person signing	
6.2	Deviation from standard procedures (all files but one handled a particular way; all documents but one included in file, etc.)	
6.3	Excessive journal entries	
6.4	Transfers to or via any type of holding or suspension account	
6.5	Inter-fund loans to other linked organisations	
6.6	Records maintained are inadequate, not updated or reconciled	
6.7	Use of several different banks, or frequent bank changes; use of several different bank accounts	
6.8	Failure to disclose unusual accounting practices or transactions • Uncharacteristic willingness to settle questioned costs • Non-serial-numbered transactions or out-of-sequence invoices or other documents • Duplicate invoices • Eagerness to work unusual hours • Access to/use of computers at unusual hours • Reluctance to take leave • Insistence on doing job alone • Refusal of promotion or reluctance to change job • Creation of fictitious accounts, transactions, employees, charges • Writing large cheques to cash or repeatedly to a particular individual • Excessive or large cash transactions • Payroll cheques with unusual/questionable endorsements • Payees have similar names/addresses • Non-payroll cheques written to an employee	
6.9	Defining delivery needs in ways that can only be met by one source	
6.10	Continued reliance on person/entity despite poor performance	
6.11	Charging items to project account for personal purposes (books and supplies bought for family	

Ref.	Area	Response
	members, home gym equipment charged to project account etc.)	
6.12	Materials erroneously reported as purchased; repeated purchases of same items; identical items purchased in different quantities within a short time period; equipment not used as promised, doesn't work, doesn't exist	