Sheffield City Council

Finance and Commercial Services

# Fraud Risk Management Guidance for Managers

Revised
may 2018

## Introduction

1. Fraud is just one risk which can affect the Council. The Council currently has a risk framework which is there to ensure that all risks identified by services are recorded, reported and managed in a consistent manner.

2. It is appreciated that in a large and complex organisation such as the Council, which undertake a number of diverse functions that not every part of the organisation is subject to the same risks.

3. The purpose of this document is to aid managers in identifying potential fraud risks within their area, and then to develop the required processes to mitigate these risks as far as possible and to have suitable controls in place to identify if they do occur.

4. Fraud, by its nature, results in loss to the Council and therefore diminishes the resources available for it to achieve its objectives. A major difference between fraud and other common risks facing the Council is that we, as public servants, do not have the authority to be 'risk tolerant' in this area. Council Members and officers have a responsibility to ensure that we can demonstrate "Best Value" in all areas of expenditure therefore; we cannot simply accept a level of loss to fraud or theft. If we were to do this, we would not be fulfilling our statutory responsibilities. Additionally, fraud and theft are criminal offences. No Council officer or Member has the authority to tolerate a degree of criminality without themselves being culpable. Council officers have a responsibility in their code of conduct to report any incidents of fraud and theft to management for investigation and the strengthening of internal controls.

5. Consequently, whilst managers need to apply a balance between risk and cost, a 'risk averse' approach should be applied to the management of fraud risks.

## Impact of Fraud

6. Risk management generally relates to managing events and implementing effective mitigation which could strengthen the ability of an organisation to achieve its aims and objectives.

7. Some examples of the specific impacts of fraud within the organisation are:

    - Inadequate funding available to deliver services / deficit budget
    - Claw back of Central Government funding or the EU
    - Reputational damage (organisation / individuals)
    - Negative External Audit opinion leading to an increased cost of borrowing
    - Negative publicity in local / national press
    - Criticism in external assessments possibly resulting in greater scrutiny
    - Psychological / motivational effect on employees
    - Job losses
    - Legal action against the Council
    - Rectification costs

## Fraud Indicators

8. A fraud indicator is either a behavioral, or system based indication that fraud or theft is potentially occurring. System based indicators are specific to the systems involved in the delivery of a service and are covered later in this document. Behavioral indicators are more generic and can apply in any instance of fraud.

9. Some examples of behavioral fraud indicators are:

    - A reluctance to be absent from work for any significant period (annual leave or sickness)
    - Coming to work before other employees or / and staying later on a regular basis
    - An unwillingness to give up certain tasks or responsibilities
    - A disregard for central authority and / or processes
    - A 'cosy' relationship with suppliers / contractors
    - Indications of living beyond apparent means
    - Addiction or substance abuse issues
    - Willingness / encouragement to bypass certain controls
    - Sudden change in personality

10. It should be noted that this is not a definitive list and the existence of one or more of the above indicators is not evidence of fraud, however, they may highlight circumstances that require further examination.

## Internal Controls

11. Controls implemented to combat fraud within an organisation generally fall into two categories. These are:

    - **Preventive Controls**: Controls intended to prevent fraud from being perpetrated.

    - **Detective Controls**: Controls implemented to detect fraud if it occurs.

12. For the purposes of this document there is another group of controls which are often included in the preventive controls category, namely **Deterrent Controls**.

13. Whilst preventive controls are system specific, deterrent controls can be applied to fraud / theft generally. For each fraud risk identified, preventive and detective controls will be dealt with separately. The main deterrent controls are as follows:

    - **Zero tolerance approach to acts of fraud**: It is essential that Council Policy incorporates a zero tolerance approach to theft and fraud. It is equally important that this is communicated to all staff. A zero tolerance approach includes treating fraud / theft as 'gross misconduct' and including proven fraudsters on the dismissal register (even if employees leave during an investigation). Knowledge of the sanctions applied to acts of theft / fraud

through publicity and knowledge of internal procedures is enough of a deterrent to prevent most employees from committing such acts.

- **Fraud awareness**: If all employees have an understanding of the act(s) of fraud they are less likely to commit fraud because colleagues / managers are more likely to identify such acts.

- **Police involvement**: Employees should be made aware that it is standard practice for the authority to report any criminality to the Police.

- **Whistleblowing**: Employees should be aware that they are contractually required to report acts of fraud or theft. They should also be aware of the Council's Whistleblowing policy and the legal protection afforded to whistleblowers via the Public Interest Disclosure Act.

- **Declaration of Interests:** Employees should be aware of their contractual and legal obligations in relation to declaring financial / other interests which could conflict with their council role.

- **Signed Code of Conduct Agreement:** Employees show on Myview that they have read and understand the Council's Code of Conduct. This will not only ensure that they are aware of the Council's stance on fraud and corruption but will also understand what constitutes unacceptable conduct.

- **Data Protection / Security:** Employees should be aware of their responsibilities in maintaining the security of data held by the Council and the potential penalties for non-compliance.

**Principles of Fraud Risk Management**

14. The first consideration for any officer tasked with managing fraud risk within a service area is the extent of the risk i.e. what assets could be targeted by fraudsters. These assets could take a number of forms including:

    - Service area budget (via cheque fraud, procurement fraud, expenses claims, timesheet fraud, payroll fraud, income diversion etc.)
    - Physical items such as stocks, stores or items of equipment
    - Grants, allowances, permits, licenses, benefits etc. which could be approved by the service area
    - Cash / assets belonging to service users for whom the service area has responsibilities
    - Procurement / contracts granted by the service area

15. As with all risk management techniques, the key factors in managing fraud risk are the impact it would have if a particular fraud took place, and the probability that it will occur.

16. In assessing the impact of instances of fraud, it is not only the monetary values which should be considered. Officers should refer to the **Impact** section (2) in this document.

17. The probability of an event can vary significantly depending upon the potential for gain and the effectiveness of controls in place.

18. The probability of a person committing fraud or theft is directly related to the motive(s) they have and the opportunity which exists. A person who would not normally commit theft or fraud may do so if they suddenly have a compelling motive. Likewise, in instances of poor internal control, some may find the opportunity in itself compelling. Where fraud occurs management controls are often found to be lacking, for example an absence of time recording or regular appraisal. Therefore, it is reasonable to treat the probability of fraud as 'high' in the absence of adequate internal controls.

19. In establishing a control environment, officers should consider the potential perpetrators of fraud within the risk area in question. Perpetrators could be officers / members of the Council, contractors / partners / suppliers, members of the public or a combination of these parties where corruption is involved.

20. It is critical that officers do not discount managers or officers involved in systems under consideration on the basis that they are liked / trusted / respected / long standing employees. Controls must serve to protect assets / resources against fraud by all potential perpetrators, no matter how unlikely.

21. As in all areas of risk management, the cost of implementing internal controls must be proportionate to the fraud risk identified.

22. For example: In a procurement scenario, two quotations may be appropriate for small value purchases however, the risk attached to the letting of multi million pound contracts should follow a strict tender process with a much greater degree of control.

23. Proportionality will depend largely upon the recurring factors of impact and probability.

24. The most common cause of fraud is a lack of effective controls i.e. existing controls failed to deter / prevent / detect fraud. Whilst this is often due to missing controls, it is equally common to identify controls which were not working as intended.

25. It is essential that any controls, which are relied upon to prevent / detect fraud, are tested to ensure that they are applied as intended and work effectively. Over a period of time the application of controls may deteriorate and should be periodically reviewed. Controls should not only apply to interactions within the Council and with third parties but also to prevent collusion between third parties against the Council's interests.

26. To summarise, the process for effective fraud risk management is as follows:

- Identify fraud risk ‘targets’
- Assess potential for loss (including non-financial impacts)
- Identify individuals who may have an opportunity to commit fraud
- Review existing controls.
- Test for adequacy
- Implement new controls if necessary
- Periodically evaluate systems to ensure controls are operating effectively

N.B. Fraud risk management, like all risk management, is a dynamic process. fraud risks and corresponding controls should be reviewed periodically and considered as part of any change / project management process. Further guidance is provided in the Risk Management Framework.

**Risk Management Plan**

27. Officers should refer to the Risk Management Framework for guidance on compiling a Risk Management Plan. Fraud risks should be included in the Risk Management Plan for the service area.

**Fraud Risk Areas**

28. Whilst this section will attempt to identify most fraud risks applicable to Sheffield City Council, officers should not treat it as an exhaustive checklist. Officers in service areas are often best placed to determine service specific risks and should use this specialist knowledge along with the methodology above to create a comprehensive fraud risk management strategy.

**INDEX**

## *Risk Area 1: Tendering*

The tender process is intended to ensure that contracts of significant value are granted in a fair and transparent manner and that value for money is obtained. Because some contracts involve very large sums of money, fraud is an ever-present concern:

**Risks**

Contracts are awarded to inappropriate contractors due to fraud / impropriety in the tender process leading to financial losses / reputational damage

**Causes**

- Cartel behaviour amongst potential contractors – price fixing
- Failure to grant contract to best value qualifying tender
- Bribery of officers involved in the tender process
- Tender values of other contractors released to competitor(s) before tender opening date
- Manipulation of contract documents to suit particular contractors
- Improper use of approved contractor lists
- Changing evaluation criteria after submission deadline to benefit particular contractor
- Manipulation of the initial criteria for the selection of contractors

**Key Controls**

- Defined tender process (within SCC, all tenders must be obtained by a 'procurement professional')
- Approved contractors list
- Internal controls and procedures
- Separation of duties between key process stages
- Independent tender assessment process
- Defined authorisation levels
- Contracts register
- Clear controls/records of contractor negotiations

## *Risk Area 2: Procurement*

Procurement can be defined as the process of obtaining goods and services. For the purposes of this document it is treated as a separate area to 'Tendering' as the combined area would be unwieldy. The tendering process applies a relatively small number of Council contracts whereas all service areas are involved in procurement.

**Risks**

- Goods or services are paid for but are not received
- The Council is charged for goods or services supplied which have not been ordered
- Goods / services supplied do not represent value for money
- Payments intended for suppliers are diverted
- Goods are not used for delivery of Council services

**Causes**

- Submission and payment of invoices for which no order exists (SCC uses three way matching)
- Submission and payment of invoices which do not represent goods / services supplied
- Submission and payment of inflated invoices
- Submission and payment of invoices for unsolicited goods / services
- Inadequate control over ordering process (manual / computerised)
- Inadequate control over quotation process
- Inadequate control over goods received processes
- Collusion between contractors / suppliers and SCC employees
- Supplier bank account details amended inappropriately

**Key Controls**

- Defined procedures: requisition / ordering / goods received / authorisation
- Matching invoices to orders / delivery notes (OEO)
- Defined authorisation levels, with corresponding system controls.
- Creditor payments system access controls
- Separation of duties
- Effective budget management process
- Effective stock control process and security marking
- Asset register / inventory including periodic checks
- Strict controls over changes to BACS details

## *Risk Area 3: Contract Management*

This section relates to the risks which exist beyond the tendering process i.e. once contracts are in place.

**Risks**

- Mis-representation of KPIs
- Contract variations are made inappropriately to the benefit of the contractor
- Increased risk of fraud to client due to inadequate internal controls within contractor systems
- Additional charges submitted for functions within contract
- Open book accounting manipulation

**Causes**

- Contractors fabricate or exaggerate performance information to maximise payments from client / avoid penalties
- Collusion / bribery with / of client employees
- Inadequate counter fraud policies / procedures within contractor organisation
- Contract terms / SLAs fail to adequately cover counter fraud requirements / instances of fraud
- Insufficient separation between client and contractor staff

**Key Controls**

- Independent client testing of performance measures
- Separation of duties / independent check / formal approval process for contract variations
- Adequate contractual requirements relating to fraud risk management and access to records
- Independent review of contractor policies / procedures in relation to fraud e.g. employee vetting, fraud response plan, reporting arrangements, disciplinary policy, policy statement – fraud and corruption, whistle-blowing policy etc.
- Review of charges (standard/variations) against contract terms
- Periodical rotation of contract management staff
- Open book accounting training

## *Risk Area 4: Staffing*

The largest cost to the Council each year is staffing. This section covers the fraud risks associated with staffing budgets as well as recruitment and selection of new staff.

**Risks**

- Staffing costs which relate to fictional employees
- Increased staffing costs due to fraudulently increased salaries/overtime
- Staff employed who do not meet specification for role
- Staff working hours not adequately controlled
- Payments made to incorrect/ changed bank accounts

**Causes**

- Starter forms (manual / electronic) processed for fictional employees
- Leavers continue to be paid with changes made to bank accounts
- Inappropriate salary increases processed (honorariums, TARA's, acting up allowances, overtime, increments etc.)
- Fiction / exaggeration / omission on application forms
- Non-adherence to recruitment process
- Absence of positive pay system (confirmation of ongoing employment)

**Key Controls**

- Formal recruitment process with adequate separation of duties / independent approval
- Formal 'variation' process with independent approval
- Payroll system access controls
- Effective budget monitoring process
- Effective applicant vetting process
- Limited responsibility for amending bank account details

## *Risk Area 5: 'Approvals'*

The term 'Approvals' in the context of this document is used to refer to any process falling under SCC remit where there is a potential gain to third parties via qualification criteria. Examples of such 'approvals' are: Grants, licenses, benefits, concessions, permits, planning applications, health inspections etc.

**Risks**

- 'Approvals' are granted to parties to which they are not entitled

**Causes**

- False information submitted during application process accepted by SCC
- Changes in entitlement circumstances not notified to SCC
- SCC employees grant 'approvals' when entitlement is known not to exist
- Staff inducements

**Key Controls**

- Robust, evidence based verification process
- Separation of duties in for checking and authorisation
- Independent post authorisation sample checks
- Periodic update requests
- Independent intelligence sources including data matching
- Periodic rotation of staff

## *Risk Area 6: Expenses (Employees / Members)*

Although payments to individuals may be relatively small, the expenses system is readily accessible to those wishing to defraud the authority.

**Risks**

- Payments are made for expenses which have not been incurred at all or not incurred on behalf of authority activities
- Payments are made to employees where no entitlement exists

**Causes**

- Exaggeration of mileage / other expenditure
- Substitution of receipts / false receipts
- Non-compliance with expenses policy(s)

**Key Controls**

- Clear and consistent policies
- Payment via payroll
- Checks on mileages for accuracy
- Comparison of activities claimed against supplementary records
- Controls over adequacy of evidential records
- Clearly defined and secure authorisation process
- Exception reports
- Independent checking of 'significant' expense claims
- Timely submission / processing requirements
- Direct payment i.e. not made via third party

## *Risk Area 7: Stocks and Stores*

Stocks and stores maintained by the Council are attractive to thieves and fraudsters as they are readily usable and easily converted to cash. In many cases, losses of stocks and stores will be simple theft however in some cases a single or more prolonged series of thefts may involve manipulation of records and would therefore be classed as fraud e.g. building materials, fuel etc.

**Risks**

- Misappropriation of Council assets
- Stocks and stores are used for non-authority purposes

**Causes**

- Simple theft (internal / external)
- Over-estimation of stocks / stores required for official purposes

**Key Controls**

- Physical security measures including CCTV
- Effective stock control, write off and disposal procedures
- Periodic un-announced independent stock checks
- Independent review / approval of stocks / stores requisitions
- Effective budget management
- Comparison of volumes of materials used on similar jobs
- Separation of duties between those issuing stock and those performing stocktakes

## *Risk Area 8: Inventory / Equipment*

The Council owns or has access to a vast amount of valuable equipment ranging from electrical and IT resources to plant and machinery. Many of these items are desirable to thieves and fraudsters either for personal use or to convert into cash. In addition to the risk of permanent deprivation of such items, their temporary use for personal gain by individuals must also be considered.

**Risks**

- Inventory items / equipment is stolen and / or used for non-official purposes

**Causes**

- Simple theft
- Equipment purchased for personal use via council processes
- Utilisation of council equipment for personal gain
- Permanent equipment ‘loans’ or items removed for ‘testing’ on a long term basis

**Key Controls**

- Physical security measures
- Up to date inventory / asset register with clear descriptions and identification marks
- Un-announced independent physical checks including occasional out-of-hours checks
- Signing in / out registers with independent checks
- Checks from purchase orders to inventory records
- Procedures governing the removal / use of resources
- Security marking of assets (lessening desirability / aiding identification)
- Ensure that assets are assigned to individual budget centres.
- Robust process for disposal approval (separation of duties)

## *Risk Area 9: Income*

The authority has many sources of income which are crucial to the maintenance of a balanced budget. A significant part of this income is collected in cash which is particularly attractive to thieves / fraudsters as it requires no conversion.

**Risks**

- Income due to the Council is diverted causing a loss
- Income is not raised for the correct amount (unofficial discount)

**Causes**

- Income is not banked intact
- Income is not checked and verified by each party during transfers
- Income is stolen in transit
- Income is stolen from storage
- Cash in hand services by Council employees (e.g. trade waste)
- Debts are written off / credited inappropriately (employee bribery / collusion)

**Key Controls**

- Physical security measures
- Pre-numbered receipts clearly distinguishable as Council stationery
- Procedures / signage confirming what proof of purchase should be expected by the public (receipts)
- Use of security firms for significant cash income sources
- Prompt banking / collection arrangements
- 'Mystery shopping'
- Income budget monitoring / reconciliation including trend analysis
- Rotation of duties for employees involved in income collection
- Separation of duties at key stages
- Limit use of cash wherever possible, by encouraging up front or online payment
- Independent review of write-offs / credit notes
- Rule prohibiting expenditure being funded direct from income – income must be fully banked intact on a timely basis

## *Risk Area 10: Cash / Bank Accounts/ Procurement Cards*

The Council still has some areas where cash is received or paid out. Cash is always vulnerable as it is a non-traceable item with immediate value. For this reason there are additional controls required to keep it safe. In addition bank accounts are also vulnerable as they give access to cash. Criminals are increasingly targeting bank accounts in order to divert payments to their own accounts. The Council also has procuremnt cards

**Risks**

- Theft or misappropriation of monies
- Amendments to bank accounts (bank mandate fraud)

**Causes**

- Simple theft
- Use of procurement cards for non-council expenditure
- Use of BACS / Direct Debits etc. for non-council expenditure

**Key Controls**

- Cash / Procurement Cards should be held securely at all times.
- Procurement cards are only used for Council expenditure and comply with procurement controls.
- Access to cash should be restricted to named personnel.
- Rule prohibiting encashment of personal cheques
- Effective controls over keys to safes etc.
- Cash balances should be kept to a minimum, recorded and reconciled periodically
- Authorised cheque signatory list with a minimum of two signatures required on all cheques
- Cheques marked “non-transferable” and “a/c payee only”
- Changes and additions to payee details and other standing data independently authorised
- System access to make and authorise these changes restricted and logged
- Supervision of all staff particularly new, inexperienced or temporary staff
- Restrict knowledge of transfer codes (and passwords if payments are initiated by computer) to approved individuals.
- Payment reports independently reviewed for accuracy immediately before the transfer of funds
- Regular bank reconciliations
- Regular petty cash reconciliations

## *Risk Area 11: Unofficial Funds*

This section refers to monies which are not funded via the council but may be maintained by SCC employees and / or on SCC premises for example private school funds, social funds.

**Risks**

- Funds are misappropriated

**Causes**

- Simple theft
- Manipulation of records (mis-representation of financial position)

(Income and Procurement causes also apply)

**Key Controls**

- Physical security
- Minimum funds kept in cash
- Regular transparent cash / bank reconciliations
- Controlled signatory list
- A minimum of two signatories to sign cheques
- Rotation of administration duties
- Independent annual audit and statement of accounts
- (Income and Procurement controls also apply)
- Only administer funds where there is a clear business case for doing so

## *Risk Area 12: Grants*

This section covers the risks and controls associated with grant funding managed by the Council and allocated to third parties for activities associated with council programmes. The Council often remains accountable for distributed funds and should ensure that appropriate controls are applied to and by the third parties. Grant funding is often targeted by fraudsters due to the often significant amounts available.

**Risks**

- Grant application / approval process is manipulated to fraudulently obtain funding
- Grant funding is misappropriated
- Grant conditions are not observed

**Causes**

- Corruption / false claims
- Misrepresentation of grant purpose in application
- Funding spent on non-qualifying items
- Submission of false receipts / invoices
- Multiple applications for same purpose
- Changes in personnel
- Misrepresentation of inputs/outputs and supporting documentation

**Key Controls**

- Regular interaction with the **External Grant Funding Team** from the outset.
- Transparent vetting process with separation of duties (independent check)
- Data matching for multiple applications
- Effective monitoring including periodic inspections
- Full documenting of decisions
- Audit of grant usage at conclusion

## *Risk Area 13: Time*

This section includes fraud risks associated with the employees' contractual time. By overstating hours worked or spending most of a working day performing non-council activities, employees are committing fraud.

**Risks**

- Service delivery is reduced due to employees failing to undertake Council responsibilities
- False claims for time worked causes additional costs to the Council

**Causes**

- Employees paid on a timesheet basis make false / exaggerated claims for time worked
- Employees working under a flexi-time scheme misrepresent start / finish / lunchtimes / breaks in order to meet contracted hours
- Employees spend excessive time on non-council activities during Council contracted working hours
- Employees conduct secondary employment during Council contracted working hours

**Key Controls**

- Effective performance monitoring
- Physical clocking-in machines / swipe-cards / attendance control procedure
- CCTV
- Internet monitoring software
- Flexi-time trend analysis
- IT usage analysis / access controls

## *Risk Area 14: Data Theft*

The Council holds a significant volume of data which requires protection such as residential and benefits information, pupil data, information on vulnerable adults and children, payment information etc. Data has a value; be it to telemarketers or organised criminals involved in identification (ID) and banking fraud. The security of this data is at risk from employees and external individuals alike and the failure to protect such data can lead to wide ranging repercussions for the authority.

**Risks**

- Protected / sensitive data is disclosed to third parties for gain

**Causes**

- Hacking
- Data removal by employees
- Data removal by third parties who have gained access to premises / records
- Loss of IT equipment containing protected data
- Provision of access details to non-employees (bribery / collusion)
- Inadvertent provision of date to third parties by their deception this can be through Phishing (general email scam), SmiShing (SMS / text message scam)Vishing (telephone scam), or even Whaling (targeted email scam)

**Key Controls**

- Maintenance of up to date records of all information assets
- Physical security of buildings, paper records, servers etc
- Password security standards across systems including change times and deletion of leavers' access
- User access restrictions - minimum 'need to know'
- Limit means to remove data e.g. laptops, USB ports, CD/DVD writers

- Monitor system activity logs and test against users' work assignments
- Email encryption
- Limit email attachment file size
- Maintain up to date firewall and malware software
- Physical / system based penetration testing
- Raising awareness through training on email, phone or text scams

## *Risk Area 15: Cash / Assets Belonging to Service Users*

Some Council employees involved in social care have a responsibility to manage assets belonging to service users. This for example may take the form of legal guardianship or accountability for funds spent by third parties. The reputational damage associated with employees who steal from or defraud service users is significant. It is important that measures are in place to protect service users from such activities.

**Risks**

- Misappropriation of cash / assets belonging to service users by Council employees

**Causes**

- Simple theft of cash / property
- Falsified invoices, or receipts for goods purchased on behalf of service users
- Items purchased for employees using service users' cash / bank accounts

**Key Controls**

- Limit access to cash / valuable property via consultation with service users' families
- Ensure that service users have a way to report concerns
- Independent visits to service users by senior staff

- Arrange appointeeship for service user
- Regular independent reconciliation of service users accounts

## *Risk Area 16: Liability Claims*

The Council is responsible for injuries caused by negligence in maintaining its roads, buildings and public spaces. False compensation claims for 'trips and slips' are commonplace due to the current blame-claim culture.

**Risks**

- Compensation is paid to claimants whose injuries / vehicle damage were not caused by Council negligence
- Compensation is paid to claimants who are not injured / vehicles not damaged or whose injuries / vehicle damage have been exaggerated

**Causes**

- False / exaggerated claims
- Claims fabricated by employees with systems access

**Key Controls**

- Implementation of insurance fraud indicator protocol to identify false claims
- Prompt assessment of site alleged to have caused injury / damage
- Data matching (serial claimants)
- Inspection of medical records
- Vehicle inspections
- Witness / claimant interviews
- Prosecution and publicity of claimants who submit fraudulent claims

- Separation of duties in claims submission / authorisation process