Sheffield City Council

Finance and Commercial Services

MANAGERS GUIDANCE

FRAUD, THEFT AND CORRUPTION RESPONSE PROCEDURE

Policy reviewed and revised July 2022

INDEX

Note this document does not cover the reporting of potential acts of money laundering, these are covered by a separate Anti-Money Laundering policy.

INTRODUCTION

1. Sheffield City Council is committed to ensuring that public monies are not diverted by acts of fraud away from the Council's front line services. The Council's Policy Statement – Fraud & Corruption (Appendix B of the Code of Conduct) communicates its zero tolerance approach to those who seek to steal from or defraud the authority.

2. This document is primarily intended to act as a guide for managers who suspect that theft, fraud or corruption is occurring within the authority either via their own observations or via reports from an employee, contractor, partner or member of the public.

3. The Council's Code of Conduct states the following:

   If you have concerns that someone is stealing, committing fraud or behaving in a way that might be unethical, you must report this to your manager, or someone named in the Whistleblowing procedure.

4. This means that all officers of the Council are contractually required to report any concerns relating to theft, fraud or conspiracy via appropriate channels. Failure to report such activity is taken very seriously and can lead to action being taken against the employee under the relevant Council procedures.

5. The purpose of this plan is to define the responsibilities for action in the event of a suspected fraud, corruption or bribery. Its focus is to:
   - establish responsibilities for investigating the incident and taking appropriate action;
   - establish and secure evidence for disciplinary and/or criminal action;
   - prevent further loss;
   - recover losses;
   - establish lines of communication with the police.

6. This procedure does not cover specific guidance on money laundering and its reporting (as this is covered by specific legislation), this can be found in the Council's Anti-Money Laundering Policy.

7. The Council has guidance for managers about the Conduct of Investigations which can be found on the Human Resources SharePoint site on the Intranet. It details how investigations should be undertaken for all employee investigations and should be read in conjunction with this document.

DEFINITIONS

Fraud

8. Fraud is defined by offences contained in the Fraud Act 2006.
   To be guilty of fraud a person must have:

   'Committed a dishonest act with the intention of making a gain for themselves or another party or causing a loss, or the risk of a loss, to another party.'

9. A "gain" or a "loss" is limited to money or property (including intangible property), such as information and could be temporary or permanent. A "gain" could be construed as gaining by keeping their existing possessions, not just by obtaining new ones, and "loss" includes losses of expected acquisitions, as well as losses of already-held property.

10. It should be noted that no gain or loss need actuality have taken place for guilt to exist. The mere intention is adequate to define guilt.

11. The three main offences created by the act are:

- Fraud by false representation – dishonestly making a false representation, and intention, by making the representation, to make a gain for themselves or another, or to cause loss to another or to expose another to a risk of loss;

- Fraud by failing to disclose information – dishonestly fails to disclose to another person information which they are under a legal duty to disclose, and intends, by failing to disclose the information, to make a gain for themselves or another, or to cause loss to another or expose another to a risk of loss;

- Fraud by abuse of position – occupies a position which they are expected to safeguard, or not to act against, the financial interests of another person, dishonestly abuses that person, and intends, by means of the abuse of that position to make a gain for themselves or another, or to cause loss to another or to expose another to a risk of loss. A person may be regarded as having abused his position even though their conduct consisted of an omission rather than an act.

Theft

12. In the context of this document, theft can be defined as: The taking of property rightfully belonging to another party (i.e. Sheffield City Council, its customers, service users, partners etc.) with the intention of permanently depriving the rightful owner of it.

13. There are two key differences between theft and fraud:

- To be guilty of theft, a person does not need to have made false representations, failed to disclose information or abused their position.

- To be guilty of theft, a person has to have actually taken something not belonging to them with the intention of permanently depriving the rightful owner of it.

Note, a person can be guilty of fraud by attempting to make a gain or cause a loss even if their actions are not successful. This would obviously cover false applications, even if they were identified during processing.

Corruption

14. There are a number of definitions of corruption. For the purpose of this document, corruption can be defined as: Offering, giving, soliciting or accepting an inducement to influence the action of any person i.e. an abuse of position (officer or elected member) for personal gain.

    NB Although the third offence under the Fraud Act 2006 also includes 'abuse of position', this differs from corruption because:

- To be guilty of fraud by abuse of position, a person must be in a position where they are required to safeguard the financial interests of another party and fail to do so.

- Corruption implies the involvement of a third party who offers an inducement in return for personal gain.

15. Acts of fraud, theft and corruption are all considered to be gross misconduct under the Code of Conduct.

16. Advice regarding the categorisation of activity can be obtained via the Internal Audit Investigations Team 0114 2736060 or 0114 2735587.

Bribery

17. Bribery can be defined as "giving someone a financial or other advantage to encourage that person to perform their functions or activities improperly or to reward that person for having already done so."

18. The Bribery Act 2010 outlaws both giving (active bribery) and receiving bribes (passive bribery) and could extend to cover seeking to influence a decision maker by giving some kind of extra benefit which amounts to more than can legitimately be offered.

19. The Act creates four categories of offence that address the following:
    - paying or offering a bribe;

- receiving or requesting a bribe;
- bribing a foreign public official;
- the corporate offence of failing to prevent bribery.

20. Any acts of suspected bribery must be reported in accordance with this plan.

Impropriety

21. In the context of this document, the term impropriety may be used to describe an inappropriate act in place of theft, fraud or corruption, particularly as the actual offence may not be apparent until investigations are partially or fully complete.

MANAGEMENT RESPONSE

Responsibility for and Purpose of Investigation

22. The prime responsibility for the investigation of allegations of theft, fraud and corruption lies with the management of the particular service area affected. The objective of such investigations is to prove or disprove the initial suspicion/ allegation by obtaining and thoroughly evaluating all material evidence so as to establish the facts of the matter and, if the suspicions appear to be well founded, to be able to:

- identify all those involved

- support the findings of the investigation by the production of all relevant evidence

- present that evidence in an appropriate form for any subsequent disciplinary or criminal proceedings

23. The investigation should also identify assets which may be recovered, consider methods of recovery and address control weaknesses which may have contributed to the loss (to prevent subsequent occurrences).

Reporting Methods including Whistleblowing

24. Managers may become aware of concerns of impropriety within their service area via the following:

- Control mechanisms
- Report by an employee
- Report by a member of the public
- Report by a partner / contractor / supplier
- Report via the Police
- Report from Internal Audit (possibly due to a Fraud Hotline allegation)
- Their own observations

25. It is a requirement of all employees through the Officers' Code of Conduct to report any potential frauds or irregularities. Many allegations of fraud will come through the normal management processes. This can be in one to one's etc.

26. If anyone asks for a meeting to discuss 'concerns' they may have, managers should make time to discuss at the earliest possible opportunity. Failure to do so may lead to further impropriety, destruction of evidence and/or attempts by perpetrators to prevent the individual coming forward.

27. If the report is made by an employee, Managers must consider if the information is coming from the employee from the normal course of business, or if it is being reported through whistleblowing procedures. If the report is via whistleblowing, in the first instance, they should ensure that the Whistleblowing Monitoring Officer is informed so that the incident can be recorded (where appropriate).

28. Managers should also ensure that they are familiar with the principles of the Public Interest Disclosure Act (PIDA) 1998. Under this legislation, whistle-blowers are afforded legal protection if they have acted in good faith and their disclosure meets one of six qualifying criteria, one of which is **'that a criminal offence has been committed, is being committed or is likely to be committed'**.

29. In line with the SCC Whistleblowing Policy and PIDA, managers should assure employees reporting impropriety that they will be protected from victimisation and / or bullying and also provide them with an ongoing communication channel to report any such incidents.

30. Managers should treat **any** allegation seriously and should not attempt to pre-judge the validity of the allegation(s) based on perceptions of the alleged perpetrator's character or historic behaviour. Case law repeatedly shows that theft, fraud and corruption are often perpetrated by trusted, well respected and long-standing employees.

Reporting to Internal Audit

31. Before commencing any investigation, managers should report the allegations or suspicions to the 'Section 151 Officer'. This role is currently the responsibility of the Director of Finance and Commercial Services with the Head of Accounting and the Head of Fianncial and Commercial Business partnering acting as deputies of the Executive Director of Resources; with the Head of Strategic Finance taking day to day responsibility for this area. In practice managers should inform the Finance Manager – Internal Audit (responsible for investigations) who will brief the S151 officer as appropriate. This is a requirement under Financial Regulations and is important for two key reasons:

    - It allows the Finance Manager – Internal Audit (responsible for investigations) to assess the risks associated with any allegations and apply Internal Audit resource appropriately. Internal Audit involvement in any investigation will range from a simple monitoring function to taking full responsibility for the investigation if the risks identified are particularly significant.

- Internal Audit is responsible for maintenance of a central record of all fraud and corruption activity within the authority and for the reporting of these details to the Audit and Standards Committee.

32. If the investigation continues to be managed within the service area, managers should provide Internal Audit with periodic updates as the investigation progresses. Internal Audit are also able to provide advice and technical expertise if specific issues such as the extraction of data from systems is required.

33. In all eventualities Internal Audit will become involved at three key stages of the investigation process. These are:

- At commencement (see above) where Internal Audit can decide on the level of support required (to ensure that all investigations are recorded, as this is a statutory requirement).

- At the time when the investigation phase is complete. This is to ensure that support and challenge can be provided prior to the production of any statements of case. This is also to ensure along with HR, that all cases of a similar nature are dealt with consistently across the Council.

- At the end of any hearing or when the case is closed, so that the formal outcome of the allegation can be recorded.

HR Involvement and Disciplinary Process

34. If the allegations relate to an employee of the Council, it is important that Human Resources (HR) are notified at an early stage.

35. In such cases, managers investigating the allegation should ensure that the Council's Disciplinary Procedure is followed.

36. The nature of the allegations or suspicions may require consideration of 'without prejudice suspension' of one or more officers. The Council's Legal Framework – Disciplinary Process & Dismissal states the following:

> *'There is no argument for not suspending from all employment if the issue is one of potential gross misconduct.'*

37. Acts of fraud, theft and corruption, if proven, are viewed by the Council as gross misconduct. HR can advise on the suspension process as well as assisting with investigative techniques, employment law and any later disciplinary action which may be necessary.

38. The following factors should be considered when deciding upon whether suspension(s) is appropriate:

- Do the suspected activities, if proven, constitute gross misconduct?

- Does the nature of the allegation(s) place service users/members of the public/officers at risk if the alleged perpetrator(s) remains in post?

- Could the authority suffer further losses if the alleged perpetrator(s) remains in post i.e. does the allegation/suspicion relate to a one-off incident or ongoing activities?

- If the alleged perpetrator(s) remains in post, to what extent could they damage or destroy evidence which would be needed in the investigation?

- Is the alleged perpetrator(s) capable of and/or likely to influence witnesses who may need to provide evidence pertinent to the investigation (including the person who made the allegation)?

39. **NB Managers should only proceed with suspension if initial enquiries suggest that the allegations / suspicions could be legitimate and the employee does not provide at the verification meeting, compelling information to suggest otherwise. However, as the act of suspending an employee is 'without prejudice', managers need not possess firm evidence of guilt in order to proceed with a suspension.**

40. Further guidance regarding suspension can be found on the Intranet under **Disciplinary Procedure Guidance**. This includes details of officers who must undertake the suspension.

41. In cases where suspension is appropriate, managers must ensure that any evidence or Council property in the possession of the employee, which could be pertinent to the investigation, is removed at the time of suspension e.g. laptop, Council phones, access passes, petty cash, procurement cardsMobile Phones (which may require managers to accompany an employee to their home immediately after the suspension meeting), desk contents etc. NB It may also be appropriate to suspend suspects' user accounts to prevent deletion / amendment of potential evidence via remote access. The Director of the Service should be made aware of all suspensions.

42. HR advisors will give the appropriate advice to the individual on contact with other employees and also be able to provide an independent contact to support the employee. In order to protect the employee and Council, it is important that staff in the department are suitably briefed whist maintain confidentiality and that communication to third parties is considered such as email out of office message on emails.

43. Suspensions have a cost and resource burden on the service and should be kept to as short a period as is reasonable to allow the investigation to take place. All suspensions will need to be reviewed at set periods and the employee informed in writing of any extensions.

Conducting the Investigation

44. The Director of Service should nominate a manager to lead the investigation and should produce a terms of reference for them to follow for the investigation. This should highlight the areas to be covered, the resources available and the key points where they expect to be informed of progress (this should either by on a time basis or at various points in the investigation).

45. It is essential that managers adopt a systematic approach to investigations. It is, however, equally necessary to ensure that the approach taken remains sufficiently flexible to ensure that the investigation is able to evolve in response to situations that may arise as evidence comes to light.

46. Managers should consider the fact that the extent of the perpetrator's impropriety may go beyond what is originally alleged / suspected. The fraud risks associated with the perpetrator's wider role should be considered and investigated as necessary. We refer to this technique as a 'holistic approach' (See Appendix A for suggested areas of consideration beyond the original allegation(s) in an investigation)

47. Once a decision has been made to commence an investigation, it is critical that a detailed record of all activity is maintained. As the nature of the investigation may lead to criminal proceedings and / or employment tribunal(s) at some time in the future, these records can prove invaluable. It is important that all meetings, interviews, removal/taking possession of evidence, telephone discussions, etc are documented. A more comprehensive note of any such event should be maintained in the form of a detailed file note which should be written up either during, or as soon after the relevant event as possible, and signed, dated and timed by the manager responsible. The investigation record should be supplemented with, and cross referenced to supporting documentation, which again could be called upon at a later stage due to future proceedings.

48. Dependent upon the scale of the investigation, it may be necessary for the manager responsible to establish a team or panel to conduct various elements of the investigation. Membership of this team should be carefully considered. It may be appropriate for managers to seek assistance from managers / officers from another service area as their expertise may assist proceedings and ensure that the investigation is completed in a timely manner. It may also be important to be able to demonstrate that managers independent to the service have been involved to counter allegations of victimisation. In certain circumstances, representatives from HR and / or Internal Audit may serve in this capacity.

Key Stages

49. Although the majority of investigations will be undertaken by service management. There is a need to ensure that all investigations by the Council are dealt with consistently. As a minimum Internal Audit and Human Resources should be involved at three key points in the investigations. These are:

- At the point where the initial allegations are made. This will ensure that support and advice can be given to the managers involved as to the way forward. This will also enable Internal Audit and Human Resources to determine their involvement in the investigation.

- In determining the outcomes (prior to the writing of the statement of case) this will ensure that the investigation can be challenged, to determine if any further areas need investigating. It will also ensure that there is consistency in the way that cases are handled (there will always be factors that impact on an individual case).

- At the conclusion of the case, to record the outcomes and to discuss any learning points for the future.

50. In complex cases or where further help and support is required the number of touch points will increase.

Resignations

51. During investigations, there are sometimes occasions where an individual may wish to tender their resignation during an investigation. The offering of a resignation does not infer guilt on the part of the employee and therefore the acceptance of a resignation cannot be used to place the employee on the Council's dismissals register. There is no reason for not accepting the resignation. The acceptance of a resignation does not prevent the conclusion of an investigation and the potential to hold a disciplinary hearing. In the event that gross misconduct is proven, the employee will still be recorded on the dismissal register, despite their resignation.

52. If a resignation is offered, this should always be discussed with Human Resources so that all of the options can be considered. As the Council has a zero tolerance to fraud, where practicable consideration should be made to concluding the investigation and holding a hearing.

Standards of Evidence

53. There are two basic evidential standards applied in UK courts which are relevant to this document:

- 'On the balance of probabilities'

- 'Beyond reasonable doubt'

54. In court, the first standard is applied in civil cases whilst the second is used for criminal cases.

55. In the case of fraud / theft case law has stated that for such cases to be proven, the level of evidence needs to be greater, ie beyond the balance of probabilities; however the actual level has not been prescribed.

56. If an investigation justifies disciplinary action against an employee, management is required to provide evidence which demonstrates 'on the balance of probabilities' that the person is guilty. This means that the quality / extent of the evidence of guilt obtained outweighs the likelihood of an innocent explanation.

57. Managers should bear in mind that if the Police are informed of suspected theft or fraud, the Crown Prosecution Service must demonstrate that evidence proves 'beyond reasonable doubt' that the defendant is guilty. This means that the evidence indicates that the only logical explanation is that the person is guilty and that any remaining doubts held by the judge or jury are not reasonable.

58. If criminality is suspected, the above should not dissuade managers from involving the Police as they are best placed to assess the quality of the evidence obtained and therefore whether a criminal investigation is justified.

Investigation Process

59. No two investigations will be exactly alike. There is however a process which should be followed to ensure that each investigation is professionally and comprehensively conducted. The key investigation stages are detailed below:

60. Identify, obtain and review evidential information. This may take a number of forms:

- **Paper documents:** Unless it is absolutely not possible, evidential documents should be originals rather than copies. Documents should be maintained in the form in which they were obtained (where required, copies of the original documents should be placed in the working papers to allow processes to continue). They should be protected and stored securely during the investigation. Managers should not annotate or mark original evidential documents in any way. If copied documents must be used, they should be certified by the officer making the copy as a true image of the original.
- **Computer held data:** It is likely that certain information required in the course of the investigation will be stored on computer systems. Managers should ensure that any printouts used are annotated with the date and time they are obtained. If this type of information is likely to be used in court proceedings at a later date, managers are advised to contact Internal Audit and the Information and Knowledge Management team in the first instance for advice. There are specific procedures which must be taken in order that computer data is admissible in court. In certain circumstances, it may be necessary to enlist the services of a forensic specialist to obtain the data and provide a chain of evidence which is satisfactory to the court. Such forensic specialists may also be able to recover data which has been deleted by the perpetrator in an attempt to destroy evidence.
- **Surveillance Evidence:** It may be that covert surveillance is necessary to establish the legitimacy of the allegations. If a manager decides that this is the case he / she **must** refer to the Surveillance and Investigation section of the SCC Intranet. This course of action should also be discussed with Internal Audit before any surveillance is performed. Failure to adhere to proper processes could not only jeopardise the investigation but also place the Council and / or individual officers at risk of legal action for breach of an individual's Human Rights.

61. To establish whether allegations / suspicions are valid, it may be necessary to conduct fact finding interviews with appropriate persons. If this is the case, managers should produce an interview plan containing details of interviewees, the reason for interviewing each officer, the order in which the interviews will be conducted and the reasoning behind this order. The suspect(s) should be the last person(s) interviewed to enable any evidence gained from previous interviews to be put to them. Interviewees should be given reasonable notice in advance of the interview and should be offered the opportunity to be accompanied during the interview. This will normally be a Trade Union Representative or other Sheffield City Council employee. If in particular circumstances these arrangements are not appropriate, the employee may request alternative representation although this should not be allowed to delay proceedings. Managers should establish the identity of the accompanying person in advance and ensure that this is appropriate in the context of the investigation e.g. the person accompanying an officer in a fact-finding interview should not have a personal relationship with the suspect(s).

62. Interviews should ideally be conducted by two officers for corroboration purposes. Managers must ensure that interview venues are appropriate and take reasonable steps to ensure that interviewees are comfortable. This could take the form of providing hot drinks or water, ensuring rooms are not excessively hot / cold and providing periodic comfort breaks depending on the length of the interview. Interviewers should obtain information via responses to questions rather than by eliciting statements through leading questions or oppression. Interviewees are entitled to refuse to answer any questions put to them and should not be pressurised if they choose to do this. All interviews must include a final question: "Are you satisfied with the way in which this interview has been conducted". This provides a defence against subsequent complaints of unfair treatment. All interviews should be recorded in the form of either summary or contemporaneous notes. These should be finalised as soon as possible either during or after the interview and Interviewees should be provided with a copy and asked to sign it show that it is an accurate reflection of the meeting.

63. Before conducting interviews with suspects, managers should consider the possibility that the interviewee may admit to a criminal act during the interview. If this were to occur the Council would be required to consult the Police in order to consider whether a criminal investigation should be instigated. The Police and Criminal Evidence Act 1984 (PACE) requires that suspects be formally cautioned and allowed access to legal representation before being questioned in regard to criminal offences. Managers are advised to contact Internal Audit for advice prior to interviews in which it is believed that this situation may arise.

64. Following completion of the interviews it may be necessary to follow up explanations of circumstances provided by interviewees to ensure that all pertinent information has been obtained and considered. It is important that all leads are followed up where they could disprove the case rather than those that would only prove the case.

65. If evidence of impropriety has been established, managers may apply the 'holistic approach' and expand the investigation into other areas of risk associated with the individual's role. Internal Audit has produced a document detailing areas of fraud

risk for consideration. This is referred to Appendix A of the Fraud Response Guidance. Again, it is important to keep a detailed record of the actions taken and to gather and protect relevant evidence. If further evidence is discovered, it is acceptable to re-interview potential witnesses if necessary. **NB If the evidence identified during the original investigation, including that obtained via fact finding interviews, does justify the adoption of the holistic approach, managers may wish to postpone interviews with the suspect(s) until the full extent of the suspected impropriety is established.**

66. If managers have adopted a holistic approach, upon completion of these investigations, they should again consider the possibility of criminality and whether the Police should be consulted.

67. When the investigation is complete, it should be apparent whether the original allegation(s) / suspicion(s) were valid. If no evidence has been found to support the allegations, then the investigation can be concluded. Managers should inform Internal Audit that this is the case so that the outcome can be recorded on the Internal Audit database. If there is evidence to support the original allegation(s) / suspicion(s), managers should consider whether criminality is involved and if so the Police should be consulted. Managers may wish to seek advice from Internal Audit before taking this action.

68. Once all the above actions have been completed, dependent upon circumstances, it may be appropriate to produce a report (separate to the statement of case) detailing the findings of the investigation and the actions which will be taken as a result. HR representatives will advise on whether and what disciplinary action is appropriate. Internal Audit should be informed of the outcome of the investigation and of any subsequent disciplinary action. The report should also consider the circumstances which allowed the impropriety to occur, the adequacy of existing controls and, in particular, whether any changes are necessary to prevent such occurrences in future. For further information, refer to the Statement of Case section of the Managers' Disciplinary Procedures Guidance document.

INITIATION OF RECOVERY ACTION

69. The Council will take appropriate steps, including legal action if necessary, to recover any losses arising from fraud, theft, irregularity or misconduct. This may include action against third parties involved in the fraud or whose negligent actions contributed to the fraud.

70. Use of the Proceeds of Crime Act 2002, where appropriate, will also be considered to maximise the penalty and level of recovery by the Council.

71. If the authority has suffered a loss as a result of the impropriety identified, managers should take action to attempt to recover the loss. This can be achieved via a number of methods:
    - Internal recovery – agreement to repay / issue of a debtor account
    - Civil recovery – seek advice from Legal Services

72. The Council's Insurance Officer must be informed as soon as possible of any loss. It is the responsibility of the Service Manager to do so. Where it is possible, details of the case should be given together with some indication of the likely loss and what recovery action is being attempted. This information has to be passed to the Council's insurers promptly to keep open the possibility of making a claim.

FURTHER INFORMATION

73. The information contained in this document is intended to cover all essential elements of a management investigation however it cannot cover every circumstance or eventuality; Managers are advised to discuss individual circumstances with Internal Audit / HR / Legal Services if further advice is required.

Intentionally left blank

Appendix A

Sheffield City Council

Finance and Commercial Services

MANAGERS GUIDANCE

FRAUD THEFT AND CORRUPTION RESPONSE PROCEDURE

HOLISTIC APPROACH TO FRAUD INVESTIGATION

Revised
July 2022

INDEX

Introduction

This document is intended to assist managers who are undertaking investigations into suspected impropriety. The following sections identify potential fraud risks areas which may need to be covered is a “holistic” approach is to be adopted.

Fraud Investigation Area 1: Budgets

If the suspect has budget management responsibilities, the opportunities for them to commit fraud may be increased. The management of budgets, may also allow staff to more easily cover up fraudulent activity. Scrutiny of the activities surrounding the management of these budgets can provide clues to specific areas of potential fraud.

Questions

1. Does / did the individual have responsibility for budget management?
2. What is / was the extent of this responsibility in terms of number / value of budgets and specific access rights? (E.g. virements, transfers, allocation etc.)
3. Does / did the individual have access to suspense accounts?
4. Is / was the individual able to set up new budget heads / sub codes?
5. Is / was the individual solely responsible for management of certain budgets? (theoretically and practically)
6. Is / was the individual required to provide budget monitoring reports to a higher authority? (such as a governing body or committee)

Suggested Testing

1. Review the budget to see that it correlates to the service provision. Check that staffing, non-staffing, income and capital expenditure agrees to the activity that is being undertaken.
2. Does the range of budget codes being used appear reasonable; review the transactions to the code descriptions? Using a few codes and putting large quantities of unrelated items through those codes could be used to cover up issues.
3. Review current and previous budgets to assess overspend situation.
4. Identify specific cost codes which are being overspent and validate a sample of individual charges.
5. Ensure that regular budget monitoring reports have been produced / submitted.
6. Check that budget monitoring reports accurately reflect position at time of production. (Variances may give pointers to ‘areas of concern’)
7. Identify and investigate any transfers / virements made / authorised by the individual. Are they justified and appropriate? (Again, excessive virements / transfers may identify ‘areas of concern’)
8. Interview other staff with theoretical budget management responsibilities. Establish whether they were actually allowed to be involved in practice.
9. Consider a review of budget management activities purportedly carried out by other individuals. Compare these to independent leave / sickness information to identify discrepancies.
10. Review suspense account transactions. Do transactions appear appropriate? Are suspense accounts cleared regularly? Do budget monitoring reports incorporate suspense account balances?

11. Identify budgets set by the individual. How were they formulated i.e. supporting documentation? Do they seem appropriate i.e. variance from previous years, unusually large apportionments to particular areas?
12. Contact the relevant Finance Business Partner for further information.

Fraud Investigation Area 2: Staffing

Staffing costs are often the biggest area of expenditure in any service and are therefore worthy of scrutiny when attempting to identify potential fraud. Likewise, fraudsters will often seek to 'recruit' or exploit people around them to assist with their activities. It is worthwhile exploring the individual's relationships with colleagues to assess whether this is the case.

Questions

1. Does / did the individual have the authority to appoint new staff or process changes to existing salaries?
2. Is / was the individual particularly friendly with any other members of the team?
3. Does / did the individual manage / monitor staffing budgets?

Suggested Testing

1. Review staffing charges. Are all staff charges accounted for? Check starters and leavers to ensure pay arrangements are correct i.e. salaries have been correctly entered and pay has been started / stopped on appropriate dates?
2. Consider whether it is appropriate to review recruitment and selection process for employees appointed by the individual. Were all appropriate processes followed? Do appointments seem fair i.e. is there evidence of favouritism? Were all necessary propriety checks undertaken?
3. Review any salary changes made by the individual. Is there apparent justification and a satisfactory management trail present?
4. Is there evidence of collusion, i.e are the same employees always involved in signing off transactions.
5. Are there any employees on the payroll with no-pay; is there a specific reason for this?

Fraud Investigation Area 3: Statements of Accounts

If an individual is relied upon to produce statements of accounts, it may be that he / she could have hidden fraudulent activity via misrepresentation of the true financial position of the account or service.

Questions

1. Is / was the individual responsible for the production of any statements of accounts including balance sheets, profit & loss accounts etc?
2. How long has / had the individual held this responsibility?
3. Are / were accounts prepared by the individual subject to any independent scrutiny?

Suggested Testing

1. Identify all statements of accounts prepared by the individual. Carry out an independent reconciliation to ensure that accounts prepared are a fair representation of the financial position at the appropriate date.
2. Where accounts were required to be presented to a higher authority, check that presented figures correspond with actuals. (Variances could indicate 'problem areas')
3. Where accounts have been verified by a third party, check whether the same person was used consistently. Where this is the case, and irregularities have been identified, consider whether this person acted in collusion with the individual. Consider whether these findings justify further investigations into the activity of the third party.

Fraud Investigation Area 4: Procurement

This is one of the most common areas to be targeted by fraudsters both internal and external. Given the sheer number of creditor payments processed across a wide range of service areas, opportunities for fraud are diverse and should be considered in any fraud investigation.

Questions

1. Does / did the individual have the authority to order goods / services?
2. What is / was the individual's authority level?
3. Is / was the individual in a position to grant contract work or specify which suppliers / service providers were used?
4. What level of authority does / did the individual have in relation to granting of contracts?
5. Has the individual completed a declaration of interests?
6. Have any interests been declared?

Suggested Testing

1. Cross reference the individual's bank account details from payroll system against creditor payment account details. Investigate matches.
2. Review orders placed by the individual.
    a. Are goods / services appropriate in nature in respect of the service area? Investigate any anomalies.
    b. Have inventory type items been entered on the appropriate inventory / asset register?
    c. Consider a physical inspection of a sample of items.
    d. Where works / services have been provided, consider physical inspection to ensure that this appears to be genuine e.g. repair or maintenance works.
    e. Are there a significant number of transactions, just below the authorisation limits or the limits where quotations are required? Check that this is appropriate.
    f. Have authority levels been adhered to or have 'split orders' been used?
    g. Have approved suppliers been used?
    h. Has a significant amount of 'business' been given to a particular supplier / service provider?
    i. Have the correct number of quotations been obtained where relevant?
    j. Do supplies / services seem excessive given the nature of the service area?
    k. Has a particular employee regularly 'counter-signed' for some part of the procurement process? Is there any correlation with a particular supplier or type of goods / services?
    l. Do costs appear to represent value-for-money?
    m. Do any of the suppliers appear to have links to the individual?
3. Review contracts for goods / services granted by the individual.
    a. Were appropriate tendering processes used?

b. Has all appropriate documentation been retained?
c. Have multiple contracts been granted to the same supplier?
d. Is there evidence of favouritism in any contracts granted?
e. Do any of the contractors appear to have links to the individual?
f. Where works / services have been provided, consider physical inspection to ensure that this appears to be genuine e.g. repair or maintenance works.

Fraud Investigation Area 5: Income Collection

Although high value fraud is often non cash-related, cash is perhaps the most tempting to small scale fraudsters as it has immediate physical value. Employees with access to cash often handle significantly larger sums on behalf of their employer than they do in their private lives. The consideration of the fraud or theft opportunities involving cash are important in any investigation.

Questions

1. Does / did the individual have the responsibility of collecting income or have access to collected income?
2. What is / was the extent of this responsibility / access?
3. Does / did the individual have custody of collected funds?
4. Is / was the individual responsible for the reconciliation of income collected?
5. Does / did the individual have access to receipt books, tickets or other stationery which could have financial value?
6. Are all possible sources of income identified?
7. Have any concerns been raised in regard to income collected by the service historically?

Suggested Testing

1. Carry out reconciliations of income to banking for a sample period.
2. Ensure that all monies are banked intact.
3. Ensure that monies have been banked promptly (within banking regulations if applicable).
4. Check that cheques have not been substituted for cash.
5. Ensure that all possible sources of income are accounted for.
6. Ensure that ticket sales or other receipts reconcile with monies collected.
7. Account for all stationery with a financial value.
8. Reconcile any residual cash / cheques held to outstanding collections.

Fraud Investigation Area 6: Bank Accounts/ Treasury Management

Controls around treasury management and bank accounts tend to be stringent due to the high values of transactions that are processed through them. The values and volumes, however means that they are susceptible to serious and organised crime as the rewards could also be significant.

Questions

1. Is / was the individual responsible for the management of any bank accounts?
2. Is / was the individual a cheque signatory?
3. Do / did all bank accounts require 2 signatories on each cheque?
4. Do / did all bank accounts require 2 signatories on each cash withdrawal?
5. Are there any known links or suspicions of links between the individual and any other signatories?
6. What were the reconciliation / reporting requirements for the accounts?

Suggested Testing

1. Reconcile banking records to actual bank statements for a suitable period.
2. Review cheque expenditure to ensure amounts and type of expenditure is reasonable given the nature of the service area.
3. Consider requesting a sample of cheques from the bank to ensure that cheques were made out to stated payees and were actually signed by 2 employees.
4. If other signatories remain in post, confirm that they did actually countersign the cheques obtained i.e. that the individual did not forge signatures.
5. Review bank accounts to establish whether non-service related cheques have been deposited i.e. personal cheques for cash.
6. Ensure that any cheques written for cash were justified and that the cash was entered into appropriate records.
7. Review bank statements for direct debits, standing orders, loan repayments or other suspicious transactions.
8. Ensure that all procurement / credit cards are accounted for and that the individual is / has been removed as a signatory.

Fraud Investigation Area 7: Procurement Cards/Credit Cards

The use of procurement cards in the Council is limited. These are mainly used for emergency items, but need to be signed off similarly to petty cash. All purchases through the cards must be fully compliant with the procurement regulations of the Council.

Questions

1. Does / did the individual have responsibility / access to a procurement card?
2. In what capacity i.e. administrator / user / authorising officer?
3. Does the service have adequate supervision over the use and verification of the cards and transactions?
4. Are assets purchased using the purchasing card always physically verified (where appropriate)?
5. Are statements always checked authorised and retained?
6. Is the card kept securely?
7. Has the card been retained on suspension or has it been cancelled?

Suggested Testing

1. Obtain the copies of all statements from the bank/ Treasury Mangement?
2. Verify the transactions to actual activity or to physical goods?
3. Why have normal ordering processes not been used?
4. Are the goods items that are required by the service?
5. Have the goods been bought from non-standard suppliers?
6. Have contract requirements been met?
7. Was authorisation sought?
8. Does the supplier offer additional items such as free gifts? Can these be accounted for?
9. Have VAT receipts been obtained?
10. Where goods cannot be verified (such as food) can these be verified in other ways?
11. Are there patterns to usage? i.e. there is always an increase before the month end.
12. Is card usage excessive?

Fraud Investigation Area 8: Petty Cash

Petty Cash although small in value is often susceptible to both theft and also manipulation. This is often referred to as “teeming and ladling” or the payday loan where money is taken with the supposed intention of repayment. It is explicit that staff should not under any circumstances; “borrow” money from petty cash and therefore any missing funds should always be treated as theft.

Questions

8. Does / did the individual have responsibility / access to petty cash?
9. In what capacity i.e. administrator / signatory / authorising officer?
10. Does the petty cash system have adequate internal controls to prevent mis-use / misappropriation?
11. Are periodic reconciliations required to be presented to a higher authority for review?
12. Is / was the individual the sole key-holder for the petty cash tin / receptacle?

Suggested Testing

13. Reconcile the petty cash.
14. Review expenditure from petty cash. Is it reasonable in value (within guidelines) and appropriate in terms of the service area?
15. Are receipts retained to evidence expenditure?
16. Do receipts appear to be legitimate or have ‘generic’ receipts been submitted i.e. no establishment / date / VAT no. stated?
17. Is petty cash usage excessive?
18. Are there patterns to usage? i.e. there is always an increase before the month end.
19. Has the individual made an unusually high number of petty cash purchases?
20. Where large purchases have been made via petty cash, consider verifying items / date with supplier.
21. If ‘inventory type’ items have been purchased, verify their physical existence.
22. If transactions require a counter-signatory, can trends be identified?
23. Is there evidence that signatures have been forged?
24. Reconcile previous petty cash returns to ensure that they accurately represent the position at the time.

Fraud Investigation Area 9: Non Official Funds

Non official funds are funds that are not the Council's or clients, such as school funds, collections etc. These are funds for which we have no official duty, but which may have been in the possession of a Council employee. The loss of such funds although not attributable to the Council could still damage its reputation.

Questions

1. Does / did the individual have responsibility / access to non official funds?
2. What was the extent of this access?
3. Are / were these funds subject to independent review / scrutiny?
4. Is there any evidence or suspicion of links with these independent reviewers?
5. Are reconciliations of these funds required to be submitted to a higher authority?

Suggested Testing

Testing in this area may be inappropriate as we may have no right to do so. However, if irregularity is proven in other areas, the relevant authority should be informed that a review of these funds is recommended.
If we are able to review the funds, the testing detailed in bank accounts, petty cash, income and statement of accounts may be used.

Fraud Investigation Area 10: Service Users' Funds / Property

The Council manages funds and property on behalf of a number of vulnerable clients. These relationships by their very nature can be difficult. The controls in place are to protect the client and the officers who operate these systems were these to fail; the reputational damage would be significant.

Questions

1. Does / did the individual have responsibilities in relation to / access to funds / property belonging to service users?
2. What is / was the extent of this access i.e.
    a. access to service users' homes
    b. specific duties in managing service users' financial affairs
    c. access to bank accounts / cash within Council establishment
    d. access to service users' property within Council establishment
3. Do systems in place to manage the above contain adequate internal controls to prevent abuse?
4. Have there been previous concerns relating to service users funds / property?

Suggested Testing

1. Where funds are retained on behalf of service users, reconcile any cash / bank accounts held.
2. Select a sample of transactions from service users' funds in which the individual has been involved. Check the following:
    a. expenditure seems reasonable
    b. receipts have been provided and appear genuine
    c. transactions have been countersigned
    d. in cases where large / expensive items have been purchased, that they actually exist / have been given to the service user
    e. any monies which are claimed to have been banked were actually deposited in the appropriate bank account
    f. monies claimed to have been banked were deposited promptly i.e. no un-necessary delays
    g. cash which was claimed to have been banked was deposited as cash i.e. not substituted by cheques
3. Examine records of previous reconciliations of service users' funds. Is the individual the person who usually carries out reconciliations (i.e. the primary signatory)?
4. Have such reconciliations been counter signed?
5. Can these counter signatories verify that they actually checked the funds?
6. Check with banks to establish whether the individual has been set up as a signatory on the accounts of any service user inappropriately. Remove as necessary.
7. Where the individual visited service users in their own homes, consider interviewing other staff who visited the same clients to establish whether there have been concerns raised by service users over missing cash or property.

8. Reconcile records of property retained on behalf of service users to ensure that it remains in storage.
9. Check property records to establish whether the individual has signed to claim that property has been returned to service users. Check that all transactions of this nature are countersigned. Attempt to verify that property has been returned independently.

Fraud Investigation Area 11: Council Property

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.

Questions

1. Does / did the individual have access to council property (i.e. items which could be transportable / valuable / desirable)?
2. If particular items of property had been assigned to the individual (e.g. laptop, mobile, blackberry, tools, vehicles etc.) have there been any previous claims that such items have been stolen?
3. Have any items assigned to the individual been returned and accounted for?
4. Does the individual have the ability to access to Council property out of hours? i.e. do they have keys/passes etc.?
5. Would the individual have the ability to loan out Council property?

Suggested Testing

1. Carry out an inventory check of items to which the individual had access.
2. Examine documentation regarding previous claims of loss / theft for patterns / validity.
3. Check whether the individual has ever written off inventory / asset items. Does the age of the items suggest that write-offs are appropriate? How have the items been disposed of? Can this be independently verified?

Fraud Investigation Area 12: Stocks, Stores and Controlled Stationary (certificates/ permits etc)

Stocks, stores and certificates / permits 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, birth certificates and blue badge permits etc.

Questions

1. Does / did the individual have access to / responsibility for SCC stocks, stores, the issue of certificates / permits?
2. What is / was the extent of this access / responsibility (i.e. simple 'access' to stock / store rooms / buildings / receptacles / certificates / permits or involved in stock control system, recording goods in / out, stock ordering / issue etc.)?
3. What is the process for periodic reconciliation of stocks / stores / certificates / permits?
4. Does the above incorporate independent involvement?
5. Is / was the individual involved in stocks / stores / certificate / permit reconciliations?
6. What is the process for writing-off obsolete, damaged or out-of-date stocks / stores.

Suggested Testing

1. Identify stocks / stores / certificate / permit records and carry out sample checks to ensure that stocks held agree to stock records.
2. Select a sample of stock / stores orders / deliveries and ensure that goods received were entered accurately on stock records.
3. Identify unusually frequent orders and / or unusually high numbers / values of stocks / stores ordered / retained. Ascertain trends / justifications (This may require independent specialist advice.)
4. Check reconciliation records for the following:
    a. Have reconciliations been carried out in accordance with instructions?
    b. Has the individual carried out reconciliations?
    c. If so, have reconciliations been counter checked?
    d. If reconciliations have been counter-signed, is there any evidence to suggest the forging of signatures?
5. Examine documentation covering the requisition of stocks / stores. Ascertain the following:
    a. Are all requisitions signed by employees other than the individual?
    b. Are job numbers included?
    c. Can these be independently verified against specific jobs (e.g. by comparison to timesheets, other systems etc.)?

    d. If so, carry out sample checks to ensure that all stocks / stores were requisitioned appropriately.
    e. Check that stocks / stores requisitioned are appropriate for jobs. (This may require independent specialist advice.)
    f. Check to ensure that requisitions amounts have not been amended.
6. For a sample of jobs for which stocks / stores have been requisitioned, ensure that unused items have been returned to stores. (i.e. check that records exist to demonstrate the quantity of stocks / stores used on the job and record details of unused stocks / stores.)
7. For a sample of returned stocks / stores, ensure that returned quantities are recorded back into stocks / stores records promptly and accurately.
8. Identify any write-offs of stocks / stores. Check the following:
    a. Do they seem appropriate? (This may require independent specialist advice.)
    b. Have they been authorised by the individual or another employee / manager?
    c. Have write-offs been counter-signed?
    d. Consider whether it is possible to independently verify disposal of the written-off stocks / stores.

Fraud Investigation Area 13: Provision of Services

This area is increasingly significant. The Council provides a number of services which have significant benefits attached both to the rightful recipients, but also to individuals who do not have a right to them. This is a growing area for organised crime. The types of services susceptible is wide spread, but covers the provision of council housing, blue badges, residents parking permits, licences and the provision of school places.

Questions

1. Does / did the individual have access to / responsibility for processing or approving applications?
2. What is / was the extent of this responsibility (i.e. are they processing or do they allocate or approve transactions.)?
3. What is the process for verification of processing?
4. Does the above incorporate independent involvement?
5. Are reviews of processing carried out?
6. What controls are there to prevent processing of applications for family and friends?
7. Is all income reconciled to the provision of service? (licences etc.)

Suggested Testing

1. Identify the transactions carried out by the individual?
2. Are there system contols? Can items be processed in another's name?
3. Verify any transactions carried out by leavers from the service? (particular after their leaver date)
4. Check any transactions with the same address, the same name or individuals known to be associated with the individual?
5. Carry out a sample check of transactions undertaken by the individual? Have these been completed correctly?
6. Verify the validity of the transactions to original documentation? Ensure that these appear genuine.
7. Have all transactions been checked and authorised independently?
8. Identify unusually frequent transactions by individuals or to an address?
9. Check reconciliation records for the following:
    - Have reconciliations been carried out in accordance with instructions?
    - Has the individual carried out reconciliations?
    - If so, have reconciliations been counter checked?
    - If reconciliations have been counter-signed, is there any evidence to suggest the forging of signatures?
10. Are complaints independently received and dealt with?

Fraud Investigation Area 14: Mileage / expenses claims

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

Questions

1. Has the individual claimed expenses from SCC?
2. Are these expenses of material value?
3. What is the process for authorisation / verification within the service area?
4. Where and for what period are receipts retained?

Suggested Testing

1. Obtain and review expense forms submitted by the individual. Check the following:
    a. Receipts were provided for each expense
    b. Receipts appear to be valid (rather than generic)
    c. Dates of receipts agree to dates of expense
    d. Amounts claimed are reasonable / within guidelines / prescribed limits
    e. Expenses are claimed for legitimate purposes only (requires independent verification)
    f. Mileage / fares are accurate (via web search: route planner, fare sites etc.)
2. Check that expense claims have been authorised by a suitable individual (consider individual's involvement if expenses are found to be fraudulent.)
3. Check leave records to ensure that individual has not claimed expenses whilst not working (e.g. whilst on annual leave / sick leave).

Fraud Investigation Area 15: Authorisation Responsibilities (including confirmation of 'qualification criteria')

This area covers a multitude of possible responsibilities and fraud opportunities because the Council is responsible for granting / authorising a wide variety of 'entitlements' (for example benefits, allowances, grants, approvals)

Questions

1. What duties / responsibilities are associated with the individual's post?
2. Does / did the individual have the authority to 'sign-off' or significantly contribute to the 'signing-off' of any benefit, certificate, grant, application, claim, permit, licence, entitlement, service, cost etc. which could qualify as a gain either personally or to a third party?
3. Could the individual speed up, fast track or queue jump any of the above examples, which could effectively cause a loss to another by nature of the fact that their application etc. would be slowed down or refused due to actions in 2 above?
4. Is / was the individual in a position to prevent / refuse any of the examples listed in 2 above, to which an applicant or other individual would be otherwise entitled, in order to cause a loss to an individual?

Because of its varied nature, suggested testing in this section is generic. For the purposes of this document, transactions of the nature referred to above will be referred to as 'approvals' or 'rejections'.

Suggested Testing

1. For a sample of approvals made by the individual, independently assess the 'application' to ensure that it meets normal qualification criteria. (This should include the provision of any documentation required as part of the process and the validation of such documentation.)
2. For the above sample, establish whether the application for the approval has been processed / granted within expected timescales / in accordance with approved processes. Check that the approvals have not been fast-tracked.
3. If the transaction relates to a financial entitlement, settlement, payment etc. check that this has been calculated correctly.
4. For a sample of rejections made by the individual, independently assess the 'application' to ensure that qualification criteria are not met and therefore that the rejection is appropriate.
5. For a sample of approvals / rejections, ensure that correct details have been entered on supporting systems i.e. to ensure that false information has not been entered to achieve either approval or rejection.
6. For a sample of approvals / rejections, examine original application documentation to ensure that amendments have not been made in order to gain approval / rejection.

Fraud Investigation Area 16: Data Access

Data is an asset:

- Names and contact information for individuals has a monetary value to unscrupulous companies involved in telemarketing or spam email selling
- Customer information has a monetary value to competitors
- Criminals may offer large sums for information of particular use to their enterprises.

The Council holds an enormous amount of data, much of it extremely sensitive, for example relating to children and vulnerable service users, but also in relation to the details of many thousands of bank accounts relating to staff, council tax payers, benefit claimants etc.
This section deals with an individual's ability to access that data either piecemeal or en masse for immoral and/or dishonest purposes.

Questions

1. Does / did the individual have access to SCC systems?
2. Do these systems contain 'sensitive data'?
3. Does / did the individual's access level allow him / her to access sensitive data?
4. (In relation to each individual system if access was available to more than one): Does the system incorporate an audit trail which records user activity? (Obtain reports for the individual's activity)
5. If the system does incorporate an audit trail facility, is this adequately protected from amendment (by for example parties with the individual's level of access)? [If this is not the case, testing in this area is likely to be unproductive]
6. Does the individual have access to a PC / laptop?
7. Has this been interrogated as part of the investigation?

Suggested Testing

1. Review the audit trail for each system to ascertain the individual's system activity.
2. Identify any 'unusual' activity i.e. activity which does not appear to be associated with his/ her day-to-day duties. (Investigate further if found.)
3. Review PC interrogation data. Did this identify data files which were unusual or inappropriate to the individual's role? Is there any evidence that the individual downloaded the files to a memory stick, burned them to CD/DVD or printed them?
4. Don't forget to check any server drives, to which only the individual had access, for evidential data.
5. (See also section 15) Review email server logs to ascertain whether data files have been sent outside SCC by the individual.

Fraud Investigation Area 17: Internet / Email Usage

This section deals with the internet and email usage of the individual. This is important as not only could these give clues to the type and extent of his / her fraudulent activity, it will also give an insight into their personality and provide information to you concerning the time spent on non-work-related emails and internet use.

Questions

1. Does the individual have access to email?
2. Does the individual have access to the internet?
3. Has the individual signed a form / confirmed agreement via MyHR to the conditions of the SCC Electronic Communication Policy
4. (For I.T.) Is all internet and email activity logged centrally i.e. via a firewall or proxy-server
5. For what period is the above data stored?
6. Was the individual's PC confiscated before he / she was aware that allegations / suspicions had been raised?

Suggested Testing

1. Examine the individual's emails (sent / received / deleted etc.) for evidence of 'unusual' activity. If you suspect that the individual has deleted relevant emails, they may be saved centrally on a firewall or proxy server. Contact BCIS to check this.
2. Was the individual in contact with an email contact (either internal or external) unusually often? Pay particular attention to the content of such emails as the recipient may be a 'confidante' or may also be involved in inappropriate activities.
3. Examine the individual's internet access (via temporary internet files on his / her PC or via interrogation of the firewall or proxy server.)
    a. What proportion of his / her time is spent on the internet whilst at work? Compare internet access to timesheet details, clock cards etc. to establish any 'on-the-clock' usage.
    b. What sites have been visited? Are any 'inappropriate' or give clues as to the individual's activities?
4. Establish whether any of the individual's email or internet usage contravenes SCC's Electronic Communications Policy?

Fraud Investigation Area 18: Flexi-time / Time-keeping

One of the most common types of fraud is employees who claim time whilst not at work. This type of activity usually starts with small anomalies i.e. just a few additional minutes claimed however, it can escalate significantly if it goes un-checked.

Questions

1. How many hours is / was the individual contracted to work?
2. What are the procedures for recording times in and out of work?
3. Is / was the individual subject to specific working schedules or were flexible working hours available?
4. Does the individual's normal place of work operate a security system such as swipe-cards or CCTV which could be used to independently verify time claimed?
5. Are / were the individual's timesheets subject to independent scrutiny / authorisation?
6. To what extent did authorising officers check / authorise time claimed?
7. If the individual worked away from base regularly, what controls are in operation to ensure that times claimed are accurate?

Suggested Testing

1. Attempt to validate a sample of timesheets via reference to external sources e.g. swipe card records, CCTV etc.
2. If the individual spent considerable time away from base, consider independently checking security systems at a sample of establishments e.g. signing in / out books, CCTV, Visitors passes etc.
3. If the individual used a SCC vehicle, establish whether it was fitted with a tracker (as most SCC vehicles are). Consider checking tracker records to establish whether they can validate or disprove times claimed / locations visited.
4. Interview authorising officers to establish to what extent checks were undertaken when authorising the individual's time / flexi sheets.

Fraud Investigation Area 19: Propriety

Whilst this is an area which has always been of concern, during periods in which competition for employment is particularly tough, job applicants are more likely to make false claims about their qualifications and / or experience. Equally importantly, they may cover up previous employments from which they were dismissed or left under unexplained circumstances in order to prevent employers from identifying their intentions or risks associated with employing them.

Questions

1. Is a copy of the individual's application form / CV available? (Obtain a copy)
2. Is there evidence to demonstrate what (if any) checks were undertaken to establish his / her propriety during the application / appointment process? (e.g. were original certificates seen / copied etc.)
3. What qualifications / experience are necessary to carry out the role? (e.g. an applicant requires QTS to qualify for a teaching role.)
4. What are the risk exposures to the authority if the individual has falsified experience or qualifications? (e.g. is the individual in a role with particular authority, control or trust?)

Suggested Testing

1. Attempt to independently verify the following:
    a. All results / passes if relevant i.e. if in recent past or where they have not been superseded by 'higher' qualifications (i.e. if individual claims to have 3 A' levels and a degree, verify the degree.)
    b. Specific qualifications / memberships via requests to governing organisations. (Even if these are not 'necessary' for the role, any fabricated qualifications give an insight into the individual.)
    c. Career history. (It is only practical to go back so far with this testing i.e. if the individual has been in various employment for 30 years, it may not be practical to contact all previous employers.)
2. In certain cases, it may be appropriate to check the individual's right to work / immigration status.

Fraud Investigation Area 20: External Activities / Information

With the rise in popularity of the internet and particularly social networking, investigators are turning to the World Wide Web to help.

Sites such as Facebook, MySpace, Twitter, YouTube etc. can be successfully utilised to identify key fraud indicators.

For example, the individual may have written blogs about his / her dissatisfaction at work, the state of his/her finances or even bragged or hinted about theft or fraud. He / she may be showing off expensive possessions or holidays on YouTube which could indicate a lifestyle beyond his / her apparent means, or may be advertising stolen SCC property on sales / auction sites such as ebay.

Whilst you may not have access to some of these types of sites at work, certain individuals have been provided with access. If you have suspicions in this area, contact Internal Audit for advice on how you can search for this type of activity.

Aside from these restricted sites, a simple web search of an individual's name (along with a location if appropriate) can assist your investigation. The individual may have been involved in activities that he / she has not informed the authority about.

The individual may be running a business 'on the side', the activities of which may conflict with Council standards or individual responsibilities. This could be worthy of further investigation.

Fraud Investigation Area 21: Refunds and Write offs

This area is often overlooked but can be significant. In certain areas, the level of income is significant and so is the level of write off. The individual with the ability to undertake refunds can undertake fraud in one of three ways. They could refund legitimate payments to their own accounts. They could write off debts to accounts for payment or use the writing off of debts to cover other transactions that they have already put in.

Questions

1. Can the individual under take refunds?
2. Do refunds need to be matched to payments?
3. Can refunds only be made to the original payment source, bank account/ payment card?
4. Is there an independent process for authorising write offs?
5. Are all write-offs reported and agreed?

Suggested Testing

1. Review the value of write offs and write backs?
2. Examine if the individual is undertaking these write offs?
3. Is there a separation of duties in who authorises the write offs?
4. Examine a sample of write offs to see if the reason is correct and they tie back to accounts?
5. Obtain the bank details from payroll for the individual and check if any refunds have been made to that account?

This page is intentionally left blank