SIB Policy and Procedures on Fraud

Author:	Brett Hannam / Sam Pringle
Version:	V3.9
Date:	01 Apr 2022
Content Manager Ref:	DF1/10/190918 – Restricted

The Strategic Investment Board

Contents

1 Fraud Prevention Policy

1.1 Introduction

Staff must be aware of their responsibility to safeguard public resources against the risk of fraud. The overall purpose of the Fraud Prevention Policy is to detail responsibilities regarding the prevention of fraud. The procedures to be followed in the event of a fraud being detected or suspected are detailed in Section 2 "*SIB Fraud Response Plan*" on page 11.

SIB requires all staff always to act honestly and with integrity, and to safeguard the public resources for which SIB is responsible.

Fraud is an ever-present threat to these resources and hence must be a concern to all. Fraud may occur internally or externally and may be perpetrated by staff, consultants, suppliers, and contractors, either individually or in collusion with others. SIB will not tolerate any level of fraud or corruption; consequently, SIB policy is to investigate thoroughly all suspected frauds and allegations (anonymous or otherwise) and, where appropriate, refer to the police at the earliest juncture. SIB is also committed to ensuring that opportunities for fraud and corruption are reduced to the lowest possible level of risk.

The purpose of this document is to set out the responsibilities of staff regarding fraud prevention, what staff should do if they suspect fraud and the action that will be taken by management in such circumstances under the following headings.

- SIB Fraud Prevention Policy, this section.
- SIB Fraud Response Plan, on page 11.

Note that, as there are personal details within Appendix 3, this document is marked as "restricted". It can be published provided Appendix 3 and any other personal information are redacted.

1.2 Definitions

The Fraud Act 2006 came into effect on 15th January 2007. The Act states that a person is guilty of fraud if he is in breach of any of the following:

- Fraud by false representation, i.e., if he dishonestly makes a false representation and intends by making the representation to make a gain for himself or another, or to cause loss to another or expose another to risk of loss.
- Fraud by failing to disclose information, i.e., if he dishonestly fails to disclose to another person information which he is under a legal duty to disclose and intends, by means of abuse of that position, to make a gain for himself or another, or to cause loss to another or expose another to risk of loss.
- Fraud by abuse of position, i.e., if he occupies a position in which he is expected to safeguard, or not to act against, the financial interests of another person, and he dishonestly abuses that position, and intends, by means of the abuse of that position, to make a gain for himself or another, or to cause loss to another or to expose another to a risk of loss.

The Bribery Act 2010 came into effect on 1st July 2011. It modernises the law on bribery and seeks to provide a revised framework of offences to combat bribery in the public and private sectors. It abolished the offence of bribery at common law and the statutory offences in the 1889 and 1906 Acts but defines four new criminal offences:

- offering or paying a bribe.
- requesting or receiving a bribe.
- bribing a foreign public official.
- failure of a commercial organisation to prevent bribery by persons associated with them.

Guidance on the applicability of the Act and procedures which an organisation can put in place to prevent bribery can be found in DAO (DFP) 09/11 Bribery Act 2010 on the Department of Finance (DoF) Accountability and Financial Management Division web-site.[1]

For practical purposes fraud may be defined as the use of deception with the intention of obtaining an advantage, avoiding an obligation, or causing loss to another party. The criminal act is the attempt to deceive, and attempted fraud is therefore treated as seriously as accomplished fraud.

Computer fraud is where information technology equipment has been used to manipulate programs or data dishonestly (for example, by altering, substituting, or destroying records, or creating spurious records), or where the use of an IT system was a material factor in the perpetration of fraud. Theft or fraudulent use of computer time and resources, including unauthorised personal browsing on the internet, is included in this definition.

The definition of staff in this document includes the following:

- Permanent staff (both full and part time)
- Temporary staff (including agency staff)
- Seconded staff
- Consultants, Associates, or variable hours staff working within the SIB operational structure

1.3 SIB's Responsibilities

The Chief Executive (CEO), as SIB's Accounting Officer, carries overall responsibility for the prevention of fraud, and is liable to be called to account by SIB's Board and The Executive Office (TEO) for specific failures. However, other responsibilities are set out below.

Irrespective of the amount involved, SIB's Financial Memorandum requires that SIB's CEO shall report to The Executive Office all cases of attempted, suspected, or proven

[1] https://www.finance-ni.gov.uk/sites/default/files/publications/dfp/daodfp0911-2.pdf

fraud. The Executive Office shall then report the frauds immediately to the Department of Finance (DoF) and the Comptroller & Auditor General (C&AG).

Further guidance beyond this policy can be found in the Northern Ireland Audit Office 2015 publication, "*Managing Fraud Risk in a Changing Environment: A Good Practice Guide*", the National Audit Office and HM Treasury 2017 publication, "*Good Practice Guide on Tackling External Fraud*", and the NIAO 2022 publication, "*Internal Fraud Risks*".

SIB staff should also be vigilant to the possibilities of money laundering (see The Money Laundering Regulations 2007 and the Proceeds of Crime Act 2002).

1.4 Chief Executive Officer's Responsibilities

The day-to-day responsibility for the prevention and detection of fraud rests with the Chief Executive Officer (CEO) who is responsible for:

- Developing a fraud risk profile and undertaking a regular review of the fraud risks associated with each of the key organisational objectives to keep the profile current.
- Establishing an effective anti-fraud policy and fraud response plan, commensurate to the level of fraud risk identified in the fraud risk profile.
- Developing and maintaining effective controls to prevent and detect fraud.
- Ensuring that controls are being complied with, through regular review and testing of control systems.
- Reassessing risks because of the introduction of new systems or amendments to existing systems.
- Reviewing controls and implementing new controls where a fraud has occurred or has been attempted, to reduce the risk of frauds recurring.
- Operating appropriate pre-employment screening measures.
- Establishing appropriate mechanisms for:
    - Reporting fraud risk issues.
    - Reporting significant incidents of fraud.
    - Coordinating assurances about the effectiveness of anti-fraud policies to support the Statement of Internal Control.
- Liaising with the Audit Committee and ensuring that the committee is kept informed of developments during an investigation.
- Liaising with the Executive Office and ensuring that the TEO is kept informed of developments during an investigation.
- Making sure that all staff are aware of the organisation's anti-fraud policy and know what their responsibilities are in relation to combating fraud and ensure that the organisation's Fraud Response Plan is up to date, and any changes communicated through the organisation.

- If appropriate, circulating lessons-learned documents throughout the organisation after a fraud has been identified and investigated.
- Operating appropriate pre-employment screening measures.
- Ensuring that anti-fraud awareness training is provided as appropriate and if necessary, more specific fraud prevention training and development opportunities are available to relevant staff.
- Ensuring that vigorous and prompt investigations are carried out if fraud occurs, is attempted, or is suspected.
- Ensuring where appropriate, legal and/or disciplinary action against perpetrators of fraud.
- Where appropriate, ensuring disciplinary action against staff who fail to report fraud or disciplinary action against supervisors where supervisory failures have contributed to the commission of fraud.
- Taking appropriate action to recover assets and losses.
- Quantifying fraud occurrences on an annual basis and updating the Risk Register to reflect the quantum of fraud within the business area. Where appropriate strategies should be devised to combat recurrence of fraud and targets set to reduce the level of fraud.
- Ensuring that appropriate action is taken to minimise the risk of similar frauds occurring in future.

In the event of an incident or suspicion of fraud, the CEO will consult within SIB as appropriate (e.g., with the Finance Manager, the Legal Director and the Information and Compliance Manager) and consider the course of action to be followed. In normal circumstances, this will include notifying the Board, Audit Committee, the SIB HR Manager and The Executive Office.

See Appendix 3 for a list of contacts.

1.5 The SIB Audit Committee Responsibilities

The SIB Audit Committee will be responsible for advising the CEO (who is the SIB Accounting Officer) and the SIB Board on:

- Management's assessment of SIB's risk from fraud and the appropriateness of its response to it.
- SIB's fraud prevention policies and arrangements, procedures for raising a concern ("whistle blowing") and arrangements for investigations.

"Fraud (if required)" is a permanent Audit Committee agenda item under AOB (Any other Business).

1.6 Internal Audit

Internal audit is responsible for the provision of an independent and objective opinion to the Accounting Officer on risk management, control, and governance. The adequacy

of arrangements for managing the risk of fraud and ensuring SIB promotes and anti-fraud culture is a fundamental element in arriving at an overall opinion.

Internal Audit has no responsibility for the prevention or detection of fraud. However, internal auditors are alert in all their work to risks and exposures that could allow fraud. Individual audit assignments therefore are planned and prioritised to assist in deterring and preventing fraud by examining and evaluating the effectiveness of control commensurate with the extent of the potential exposure/risk. The risk register is also reviewed as a constituent part of each audit assignment to ensure that management have reviewed their risk exposures and, where appropriate, identified the possibility of fraud as a business risk.

1.7 Senior Management Responsibilities

A major element of good corporate governance is a sound assessment of the organisation's business risks. Senior management need to ensure that:

- Fraud risks have been identified within the SIB Risk Register[1] encompassing all operations for which they are responsible.
- Each risk has been assessed for likelihood and potential impact.
- Adequate and effective controls have been identified for each risk.
- Controls are being compiled with, through regular review and testing of control systems.
- Risks are reassessed as result of the introduction of new systems or amendments to existing systems.
- Where a fraud occurred, or has been attempted, controls are reviewed and new controls implemented, as necessary, to reduce the risk of fraud recurring.
- Fraud occurrences are quantified on an annual basis and the Risk Register updated to reflect the quantum of fraud within each business area. Where appropriate, strategies should be devised to combat recurrence of fraud and targets set to reduce the level of fraud.

In terms of establishing and maintaining effective controls, it is generally desirable that:

- There is regular rotation of staff, particularly in key posts.
- Wherever possible, there is a separation of duties so that control of a key function is not vested in one individual.
- Backlogs are not allowed to accumulate.
- In designing any new system, consideration is given to building in safeguards to prevent and/or detect internal and external fraud.

[1] Risk registers are filed in the CM Container DF1-13-16160 "*Strategic Investment - Audit and Accountability - Risk Management - SIB Risk Registers*".

1.8 Staff Responsibilities

All staff are responsible for:

- Acting with propriety in the use of SIB's resources and in the handling and use of public funds whether they are involved with cash or payment systems, receipts or dealing with contractors or suppliers.
- Conducting themselves in accordance with the seven principles of public life detailed in the "Nolan Committee's First Report on Standards in Public Life"[1], i.e. selflessness, integrity, objectivity, accountability, openness, honesty and leadership; and
- Being vigilant to the possibility that unusual events or transactions could be indicators of fraud and alerting their line manager where they believe the opportunity for fraud exists. (Annex A on page 27 provides examples of "*Indicators of Fraud*". In addition, Annex B lists "*Common Methods and Types of Fraud*" on page 29 and Annex C lists "*Good Management Practices*" on page 31.[2])

In addition, it is the responsibility of every member of staff to report details immediately to the CEO if they suspect that a fraud has been attempted or committed or see any suspicious acts or events. The Public Interest Disclosure (NI) Order 1998 protects the rights of staff who report wrongdoing. Your conversation will be treated in absolute confidence. The "*Strategic Investment Board Ltd (SIB) – Policy on Raising a Concern (Whistleblowing)*" (FI1/18/873641) is a separate policy document that is also available on the SIB Website.

Advice is additionally available through Protect – formerly Public Concern at Work.[3] This is an independent charity and is a leading authority on public interest whistleblowing.

Telephone:
Protect Advice Line: 020 3117 2520 (* option 1)
Business Support: 020 3117 2520 (*option 2)
Fax:
020 7403 8823
Email:
Protect Advice line: whistle@protect-advice.org.uk
Media enquiries: press@protect-advice.org.uk
Business support services: business@protect-advice.org.uk
Address:
The Green House
244-254 Cambridge Heath Road
London E2 9DA

Their lawyers can give free confidential advice at any stage regarding a concern about serious malpractice at work. An employee can, of course, also seek advice from a lawyer of their own choice, at their own expense.

[1] See the Committee on Standards in Public Life website.

[2] See also the NIAO 2022 publication, "*Internal Fraud Risks*".

[3] www.protect-advice.org.uk/

Section 5 of the Criminal Law Act (Northern Ireland) 1967 (Penalties for concealing offences etc.) also places the onus on individuals to report/pass evidence to the Police. The involvement of the Police Service of Northern Ireland (PSNI) is dealt with within the "*SIB Fraud Response Plan*" – Section 2 on page 11.

Staff should also assist any investigations by making available all relevant information and by co-operating in interviews. Any information provided by staff will be treated confidentially.

All staff are stewards of public funds. Therefore, all staff must have, and be seen to have, high standards of personal integrity. Staff should not accept gifts, hospitality, or benefits of any kind from a third party, which might be seen to compromise their integrity. (SIB's Gifts and Hospitality Guidelines can be found in the "*SIB Financial Policies & Procedures Manual*" DF1/11/239920) that is also available on the SIB Intranet and the SIB website.

It is essential that staff understand and adhere to laid down systems and procedures including those of a personnel/management nature such as submission of expense claims and records of absence and annual leave.

All SIB staff are required to declare any personal or business interests that may conflict with their responsibilities as employees of the company and as public servants. SIB's guidance on conflicts of interest can be found at FI1/21/1242715 "*SIB Guidance on Conflicts of Interest*", which is also available on the SIB Website on the "Policies and Procedures" page.

1.9 Investigation

Senior Management should be alert to the possibility that unusual events or transactions can be symptoms of fraud or attempted fraud. Fraud may also be highlighted because of specific management checks or be brought to management's attention by a third party.

It is SIB policy that there will be consistent handling of all suspected fraud cases without regard to position held or length of service.

Investigators should have free access to all staff, records, and premises to carry out investigations.

Irrespective of the source of suspicion, it is for the CEO to undertake an initial examination to ascertain the facts and to confirm or repudiate the suspicions, which have arisen so that further investigation may be instigated if necessary. After suspicion has been roused, prompt action is essential. **However, as detailed in the "*SIB Fraud Response Plan*" – Section 2 on page 11, it is imperative that such enquiries should not prejudice subsequent investigations or corrupt evidence; therefore, IF IN DOUBT, ASK FOR ADVICE.**

If it is the CEO who is suspected of fraud, the Chairman of the Audit Committee will take on the responsibilities designated to the CEO in this policy. He should inform the Chairman of the SIB Board. Where appropriate, staff should report their suspicions to the Chairman of the Audit Committee and/or the Chairman of the SIB Board.

In some cases (e.g., where fraud or suspected fraud has been perpetrated on SIB by a third party) and depending on the circumstances, an incident may be referred to the NICS Group Fraud Investigation Service (GFIS). Generally, this is done on the advice of TEO.[1]

1.10 Reporting Arrangements

If the initial examination confirms the suspicion that a fraud has been perpetrated or attempted, management should follow the procedures provided in Section 2 "*SIB Fraud Response Plan*" on page 11, which forms part of the SIB anti-fraud policy.

Figure 1: Reporting Fraud/Suspected Fraud on page 10 shows the process in diagrammatic form.

See also Appendix 3 for a list of contacts.

1.11 The National Fraud Initiative

The National Fraud Initiative (NFI) is an effective data matching exercise. It compares information held by different organisations and within different parts of an organisation to identify potentially fraudulent claims and overpayments. The Comptroller and Auditor General for Northern Ireland can undertake data matching exercises, requesting a data from a range of public bodies and the private sector, for the purposes of assisting in the prevention and detection of fraud.

SIB actively participates in NFI exercises providing trade creditor and payroll data sets and will continue to do so as a key strand in its fraud prevention policy.

1.12 Disciplinary Action

After full investigation of an alleged fraud SIB will, as appropriate:

- Notify the complainant and the subject of any complaint that the investigation concluded that there was no case to answer.
- Take legal and/or disciplinary action in all cases where it is considered appropriate. Any member of staff found guilty of a criminal act will be considered to have committed a serious disciplinary offence and is likely to be dismissed from SIB on the grounds of gross misconduct.

Where supervisory negligence is found to be a contributory factor, disciplinary action may also be initiated against those supervisors responsible.

It is SIB policy that in all cases of fraud, whether perpetrated or attempted by a member of staff or by external organisations or persons, the case will be referred to the police at the earliest possible juncture.

Losses resulting from fraud should be recovered, subject to the policy on write-offs and, if necessary, through civil action.

[1] An example would be cases of premium rate SMS scams that (in the past) have been perpetrated on individual SIB staff members' official smartphones. Either GFIS or TEO will provide a Case Referral Document that has to be completed.

1.13 Best Practice

The following best practice guidance should be applied during an investigation:

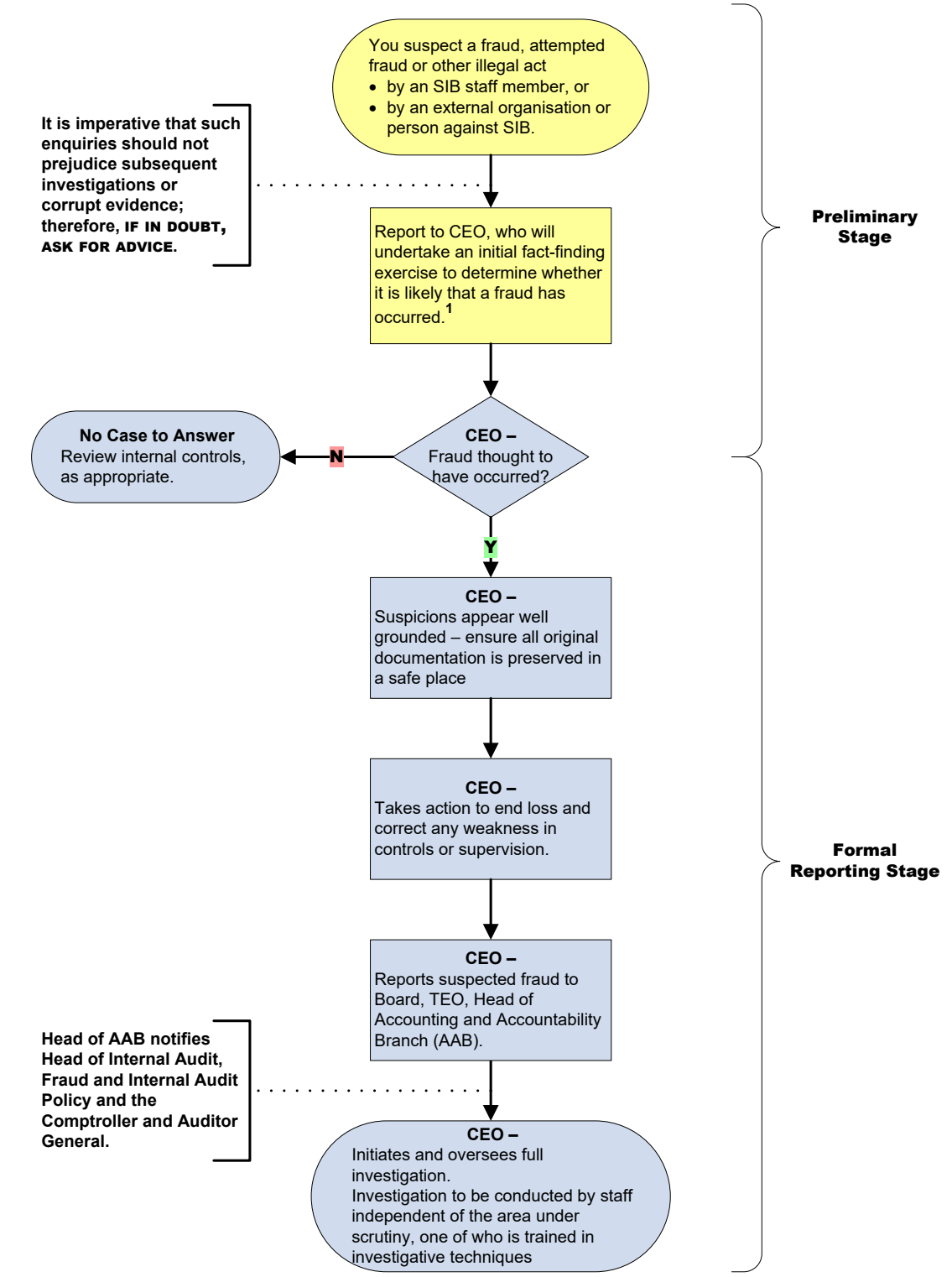
- All aspects of the suspected staff member's work should be investigated, not just the area where the fraud was discovered.
- The investigation will obviously cover the period the officer was responsible for the processes under investigation, but consideration should also be given to investigating earlier periods of employment.
- Potential evidence, including computer files and records of amendments relevant to the case, should be retained securely (in compliance with PACE requirements) and not disposed of under any normal or routine procedures for disposal of records.
- Control weaknesses discovered in procedures during the investigation should be strengthened immediately.
- The extent, if any, of supervisory failures should be examined.

1.14 Conclusion

It is appreciated that the circumstances of individual frauds will vary. SIB takes fraud very seriously and will ensure that all cases of actual or suspected fraud, including attempted fraud, are vigorously and promptly investigated and that appropriate remedial action is taken. Staff should be fully aware of their responsibility to protect public funds and as such, should always be alert to the potential for fraud.

Any queries in connection with this policy document should be directed to the CEO.

The Head of Internal Audit in the Department of Finance can offer advice and assistance on risk management or internal control issues. Appendix 3 has a list of contacts.



[1] *If you are concerned that the Chief Executive Officer may be involved in the suspected fraud, you should report it to the next appropriate level: i.e. the Chairman of the Board or the Chairman of the Audit Committee..*

Figure 1: Reporting Fraud/Suspected Fraud

2 SIB Fraud Response Plan

2.1 Introduction

SIB has prepared this Fraud Response Plan to act as a procedural guide and provide a checklist of the required actions, which **must** be followed, in the event of a suspected fraud, or attempted fraud.

Adherence to this plan will ensure that timely and effective action is taken to prevent further losses, maximise the recovery and minimise recurrence of losses, identify the fraudsters and maximise the success if any disciplinary/legal action taken.

Its purpose is to define authority levels, responsibilities for action and reporting lines in the event of suspected fraud, theft, or other irregularity.

A Memorandum of Understanding (MOU) between the Northern Ireland Public Sector and the PSNI was formally signed on 30 October 2006 and was updated and revised in September 2010. It can be found on the DoF website. The MOU sets out a basic framework for the working relationship between the PSNI and the Public Sector in respect of the investigation and prosecution of fraud cases. Its aim is to ensure consistency in the way fraud cases are investigated across the range of public sector bodies and a more targeted approach to criminal prosecution cases.

2.2 Preliminary Stage

In the event of a fraud, attempted fraud or other illegal act being suspected, the staff member should immediately report the matter to the CEO. If such action would be inappropriate (e.g., if the CEO himself were suspect), concerns should be reported upwards to the Chairman of the SIB Board and other Board members as appropriate.

It is for the CEO to undertake an initial fact-finding exercise (except where it is the CEO who is suspect, in which case the Chairman of the Board or his nominee will carry out the enquiry role normally assigned to the CEO). This discreet enquiry should be carried out as speedily as possible and certainly within 24 hours of the suspicion being raised.

The purpose of the initial fact-finding exercise is to determine the factors that gave rise to suspicion and to clarify whether a genuine mistake has been made or if it is likely that a fraud has been attempted or occurred. This may involve discreet enquiries with staff or the examination of documents. **It is imperative that such enquiries should not prejudice subsequent investigations or corrupt evidence; therefore, IF IN DOUBT, ASK FOR ADVICE.**

If the preliminary enquiry confirms that a fraud has not been attempted nor perpetrated but that internal controls are deficient then management should review their control systems with a view to ensuring they are adequate and effective. The Risk Register should be updated if appropriate.[1]

[1] See the CM container DF1-07-6466 "*Strategic Investment - Audit and Accountability - Risk Management - Risk Assessment*".

The "Anti-fraud guidance"[1] section of the Department of Finance website provides information on good practice. Access to staff with the necessary training in investigation and interviewing can be arranged by the Director of Finance. See also "*DAO 09/16 (DoF) - Good Practice Procedures in Fraud Investigations*" filed at FI1/16/758123.

2.3 Formal Reporting Stage

If the preliminary enquiry confirms the suspicion that a fraud has been attempted or perpetrated, management must ensure that all original documentation is preserved in a safe place for further investigation. This is to prevent the loss of evidence, which may be essential to support subsequent disciplinary action or prosecution. The facts should be reported immediately to the CEO.

To remove any threat of further fraud or loss, management should immediately change/strengthen procedures and if appropriate, suspend any further payments pending full investigation.

2.4 Liaison with the Police Service of Northern Ireland (PSNI)

The CEO should ensure that legal and/or police advice is sought where necessary. The PSNI may be approached to give advice and/or guidance in cases where fraud is suspected but this approach must be made through TEO: that is, TEO should be asked first before any referral to PSNI is made by TEO. Where actual or attempted fraud is confirmed and is of a large or complex nature, the PSNI Fraud Squad can carry out investigations. Smaller cases may be referred to the local police.

If the evidence strongly suggests that a fraud may have occurred, the expert advice from the PSNI Fraud Squad is likely to include some or all the following actions:

- Secure the evidence and ensure the preservation of records, both paper and electronic.
- Ensure the procedures are strengthened and action has been taken to end the loss.
- Remove the suspect's access to the computer systems.
- Relocate the suspect in another building if immediate suspension is not warranted.

2.5 NICS Group Fraud Investigation Service (GFIS)

In some cases (e.g., where fraud or suspected fraud has been perpetrated on SIB by a third party) and depending on the circumstances, an incident may be referred to the NICS Group Fraud Investigation Service (GFIS). Generally, this is done on the advice of TEO.[2]

[1] https://www.finance-ni.gov.uk/publications/anti-fraud-guidance.

[2] An example would be cases of premium rate SMS scams that (in the past) have been perpetrated on individual SIB staff members' official smartphones. Either GFIS or TEO will provide a Case Referral Document that has to be completed.

2.6 Right of the Suspect to be Informed and be Accompanied

If fraud is suspected, investigators must secure evidence, ensure preservation of records, remove the suspect's access to computer systems, and suspend or relocate the suspect in another building. The suspect should not be informed before these steps are taken to avoid any attempt on their part to remove or destroy evidence. If it is necessary to inform the suspect earlier to get access to evidence or remove access to computers (e.g., it may be necessary to ask them to divulge passwords), the suspect's access to computer systems must be removed and the suspect should be relocated in another building if suspension is not warranted immediately. The suspect must be notified formally in writing at the earliest possible point in the investigation of the reasons for their suspension or relocation.

If it is decided to deal with the matter solely as a disciplinary issue, the suspect has the right to be accompanied during any investigation interviews. They are entitled to be accompanied by a colleague during any disciplinary hearing or appeal hearing. This method should only be followed if it is certain that SIB will not seek a criminal prosecution.

If the matter is dealt with under PACE[1], the suspect generally has the following rights, amongst others:

- For an interpreter to be provided as soon as practicable where there are doubts about hearing or speaking ability or ability to understand English.
- To be informed that they may at any time consult and communicate privately with a solicitor, whether in person, in writing or by telephone.
- On request to have that solicitor present when they are interviewed.
- To communicate with anyone outside the interview.

2.7 Post Event Action

Where a fraud, or attempted fraud, has occurred, management must make any necessary changes to systems and procedures to ensure that similar frauds or attempted frauds will not recur. Additionally, if a staff member is suspected of involvement, the CEO will consider the appropriate course of action. This may range from close monitoring/supervision to precautionary suspension; however, it should be noted that suspension does not in any way imply guilt.

2.8 Communication with the SIB Board and TEO

Irrespective of the amount involved, the Financial Memorandum requires that all cases of attempted, suspected, or proven fraud shall be reported to the Executive Office as soon as they are discovered.[2] The CEO will similarly immediately inform the Chairman of the Board and the Chairman of the Audit Committee.

[1] The Police and Criminal Evidence Act 1984 (Codes of Practice) Order 2008 (PACE).

[2] See https://www.dfpni.gov.uk/articles/national-fraud-initiative-notice

The CEO is responsible for preparation and submission of fraud reports to The Executive Office.

The CEO is responsible for bringing fraud reports to the attention of the internal and external auditors.

2.9 Report and Lessons Learned

A Fraud Report should be prepared for every incident and used to inform the Board, TEO, Auditors, etc. (see Section 2.8 above). The Fraud Report should include a lessons learned section to summarise shortcomings identified in the report and any actions needed and taken to avoid a repetition of the incident or a similar incident. In preparing "lessons learned", the report should be wide ranging and not confined simply to the current incident.

The lessons learned document should be circulated throughout SIB, if appropriate, and this "*SIB Fraud Response Plan*" should be reviewed to determine whether it needs updated and, if so, changes should be circulated throughout the organisation.

At the appropriate time, SIB should inform the Department of Finance Fraud Working Group and the Northern Ireland Civil Service Fraud Forum (or any successor organisations) of outcomes and lessons learned.

2.10 Dealing with the Media

Irrespective of whether the incident being investigated has become known to the media or whether there have been media enquires related to it, the CEO must consider arrangements for dealing with potential media enquiries, communications, and publications.

1. As he deems appropriate, the CEO should brief the SIB Press and Communications Director and ensure that she has access to any records relating to the incident.
2. The Press and Communications Director should brief or take advice from any other persons that she deems appropriate, clearing this with the CEO beforehand as necessary.
3. The Press and Communications Director will be responsible for preparing a briefing note or "lines to take". This note should be reviewed and updated as frequently as is needed to keep up with changing events or circumstances. The note should be precise on what information can be released (and what must not: e.g., for reasons of commercial confidentiality or sensitivity).
4. The briefing note will be made available to anyone who is likely to communicate with the media (but see 6 below).
5. In accordance with Section 2.8 above, and before it is used, this briefing note should be agreed with:
    a. The Executive Office
    b. The Chairman of the Board

c. The Chairman of the Audit Committee.

6. **The Press and Communications Director will handle all communications with the media or media enquiries, which must be referred to her by other staff.** The CEO may appoint someone else if the circumstances demand it.
7. Where media attention is anticipated, the CEO should send an email to all staff naming the key contact person to whom all media enquiries should be passed.
8. The Press and Communications Director will create a log, stored in HP Records Manager, that will record what information has been released (to the media), when it was released and to whom.
9. At the conclusion of the incident, the Press and Communications Director will ensure that any media lessons learned are included in the main lessons learned report – see Section 2.8 above.

2.11 Reporting Arrangements

The Head of Accounting and Accountability Branch (AAB) is responsible for notifications to Fraud and Internal Audit Policy in the Department of Finance (FIAP, DoF) and the Comptroller and Auditor General (C&AG) about all discovered fraud, proven or suspected, including attempted fraud, within Non-Departmental Public Bodies or Arm's Length Bodies. Therefore, the Head of Accounting and Accountability Branch should be notified immediately of all such frauds within SIB.

2.12 Conclusion

Any queries in connection with this response plan should be made to the CEO.

Internal Audit in the Department of Finance can offer advice and assistance on risk management or internal control issues. Contacts are listed in Appendix 3.

3 SIB Whistle-blowing Policy

SIB's whistleblowing policy is contained in a separate policy document, FI1/18/873641 "*Strategic Investment Board Ltd (SIB) – Policy on Raising a Concern (Whistleblowing)*", which is also available on the SIB Intranet and the SIB website.

All whistleblowing reports made to SIB should be documented and summarised using the template available at FI1/18/872728 "*[Template] SIB Public Interest Disclosure Form*".

Appendix 1 Guidance on the Prevention of Conflicts of Interest

SIB's guidance on the prevention of conflicts of interest was moved into a separate document in October 2021, FI1/21/1242715 "*SIB Guidance on Conflicts of Interest*". This brings the SIB guidance into line with the Department of Finance guidance published on the Department of Finance website as DAO (DoF) 07/21 att (29 Sept 2021) - Conflicts of interest guidance.[1] It is also publicly available on the SIB Website on the "Policies and Procedures" page.

[1] https://www.finance-ni.gov.uk/sites/default/files/publications/dfp/daodof0721att.pdf

Appendix 2 Changes from the Previous Version

Table 1: Version History

VERSION NUMBER	VERSION DATE	SUMMARY OF CHANGES
		The previous versions of this document are: • DF1/07/89731 "SIB Fraud Policy - 2007" • DF1/07/163093 "SIB Whistle-blowing Policy" (now incorporated into the main document at Section 3 on page 17). • DF1/10/24837 "Guidance on Conflicts of Interest" (now incorporated into the main document at Appendix 1 on page 19).
3.0	31-May-10	Major revision and recast. **General Changes** • Reviewed against DF1/09/484179 "OFMDFM Fraud Policy and Response Plan" and updated as necessary. • Checked and updated as necessary all cross-references and footnotes. **Specific Non-trivial Changes** • Incorporated the "SIB Whistle-blowing Policy" as Section 3 rather than it being a separate policy document (following the OFMDFM model). • Incorporated the SIB "Guidance on Conflicts of Interest" as Appendix 1 rather than it being a separate policy document • Document completely reordered and re-numbered to make it more consistent. • Reference to staff responsibilities on conflicts of interest added at Section 1.8 "Staff Responsibilities" on page 6 (including a cross-reference to Appendix 1 on page 19). • Added Section 1.13 "Best Practice" on page 9. • Section 1.14 "Conclusion" on page 9 – added reference to Internal Audit in the Department of Finance. • Updated Section 2.4 "Liaison with the Police Service of Northern Ireland (PSNI)" on page 12. • Added Section 2.6 "Right of the Suspect to be Informed and be Accompanied" on page 13. • Section 2.12 "Conclusion" on page 15 – added reference to Internal Audit in the Department of Finance. • Update on declarations of interest.
3.1	Feb-12	Sections C–2 "Fraud Prevention in Supplier payments" and C–3 "Grants" were added to reflect the same additions in DF1/11/239920 "*SIB Financial Policies & Procedures Manual*".
3.1	Apr-12	Added footnote in Section 2.7 "Post Event Action" for link http://www.afmdni.gov.uk/pubs/FMG/fddfp0412.doc
3.11	Oct-12	Changes from an interim review: • Amendments consequent on SIB no-longer having a Chief Operating Officer (all references to COO changed to CEO as appropriate)

VERSION NUMBER	VERSION DATE	SUMMARY OF CHANGES
		• Amendments to Sections 2 and 3 to deal with the possibility that the CEO is suspected of Fraud and the consequence of not being able to report suspicions to the COO. • Minor changes such as changes in staff at OFMDFM.
3.11	4-Mar-13	Added, revised copy of declaration of interests form (DF1/08/316258) added
3.12	13-Dec-13	Added, following Internal Audit recommendations (see DF1/13/806122): • Section 2.10 "Dealing with the Media" on page 14. • Appendix 3 "Key Contacts for Advice, etc." on page 25. **Note that, as there are personal details within the new Appendix 3, the document is marked as "restricted". It can be published provided Appendix 3 is redacted.**
3.13	19-Sep-14	Review, check and general update. No substantial changes. **18-Mar-15** Added paragraph to refer to DAO (DFP) 02/15.
3.14	13-Mar-16	Review, check and general update. No substantial changes other than reformatting the document to match the new SIB styles and branding. A few broken links that appear to have been removed from the DFP website have also been removed.
3.14a	23-Jun-16	Review, check and general update. No significant changes. Changes to reflect changes in Departmental names and email addresses (e.g. OFMDFM has become TEO). In a few cases links to legislation have changed and been corrected.
3.15b	14-Jul-16	Reviewed against the "TEO Departmental Fraud Prevention Policy and Fraud Response Plan" issued in July 2016 (TEO ref: EO1/16/0037283). Changes to: • Section 1.2 Bribery Act 2010 • Section 1.3 Additions to bring the SIB policy in line with the TEO policy • Added Section 1.10 on the National Fraud Initiative • Section 2.1 Update on the Memorandum of Understanding (MOU) between the Northern Ireland Public Sector and the PSNI • Section 2.2 Added reference to the DoF Fraud Management Guidance • Appendix 4 update contacts
3.15b	10-Oct-16	Reviewed against the Updated TEO Fraud Prevention Policy & Fraud Response Plan - -September 2016 (copy filed at FI1/16/494583). No changes required.
3.2	22-Mar-17	Updated for points identified by the SIB Audit Committee on 16-Mar-17. • Section 1.4 on page 3 Added, *"Liaising with the Executive Office and ensuring that the TEO is kept informed of developments during an investigation."* • Section 1.9 on page 7 – Clarification if CEO is a suspect and the role of the Chair of the Audit Committee. • Section 1.12 on page 8 – Clarified text to avoid perception of prejudicing the expected outcome.

VERSION NUMBER	VERSION DATE	SUMMARY OF CHANGES
		• Figure 1 on page 10 – Added Chairman of Audit Committee as person to whom to report suspicions about CEO. • Section 2.4 on page 12 – Clarified that liaison with PSNI should be through TEO, who should be contacted first. • Section Expanded to cover time limit and keeping whistle blower informed. • Appendix 3 on page 25 – Changed contact details for Internal Auditor. (note that individual contact names are outstanding). • New Annex C–1 on page 32 created from FI1/17/194720, "*Examples of risks and controls in specific systems for reducing opportunities for fraud*". • Annex C–3 on page 34 "*Grants*" amended to note that 100% of invoices are checked. A review against the TEO guide on Grants Expenditure is outstanding (and has to wait until TEO has finalised the guide).
3.2a	16-Jan-18	Review and check. No significant updates needed other than… • Updated a facsimile conflicts form to the latest template in HPRM. • Some changes to contacts.
3.5	20-Aug-18	Review and check. The SIB whistleblowing policy removed into a separate policy document and cross-referenced.
3.6	1-Feb-19	Review and check. FI1/19/126304 "*DAO (DoF) 04/18 [Fraud Proofing]*" incorporated and reflected in policy as a new Annex D. Minor corrections to contact details and changes of contacts.
3.7	16-Apr-21	Reviewed, checked, and updated as necessary. Corrections to contact details and changes of contacts.
3.7	Sep-21	Whistleblowing policy moved to a separate document.
3.8	Nov-21	Revised following the removal of the guidance on declarations of interest into a separate document.
3.9	Apr-22	Revised and updated.

Appendix 3 Key Contacts for Advice, etc.

[REDACTED]

Annex A Indicators of Fraud

- Missing expenditure vouchers and unavailable official records
- Crisis management coupled with a pressured business climate
- Excessive variations to budgets or contracts
- Refusals to produce files, minutes or other records
- Related party transactions
- Increased employee absences
- Borrowing from fellow employees
- An easily led personality
- Covering up inefficiencies
- Lack of Board oversight
- No supervision
- Staff turnover is excessive
- Figures, trends or results which do not accord with expectations
- Bank reconciliations are not maintained or can't be balanced
- Excessive movement of cash funds
- Multiple cash collection points
- Remote locations
- Unauthorised changes to systems or work practices
- Employees with outside business interests or other jobs
- Large outstanding bad or doubtful debts
- Employees suffering financial hardships
- Placing undated/post-dated personal cheques in petty cash
- Employees apparently living beyond their means
- Heavy gambling debts
- Signs of drinking or drug abuse problems
- Conflicts of interest (see Appendix 1 on page 19)
- Lowest tenders or quotes passed over with scant explanations recorded
- Employees with an apparently excessive work situation for their position
- Managers bypassing subordinates
- Subordinates bypassing managers
- Excessive generosity
- Large sums of unclaimed money
- Large sums held in petty cash
- Lack of clear financial delegations
- Secretiveness
- Apparent personal problems
- Marked character changes
- Excessive ambition
- Apparent lack of ambition
- Employees suffering financial hardships
- Poor morale
- Excessive control of all records by one officer

- Poor security checking processes over staff being hired
- Unusual working hours on a regular basis
- Refusal to comply with normal rules and practices
- Personal creditors appearing at the workplace
- Non taking of leave
- Excessive overtime
- Large backlogs in high risk areas
- Lost assets
- Unwarranted organisation structure
- Absence of controls and audit trails.
- Socialising with clients – meals, drinks, holidays
- Seeking work for clients
- Favourable treatment of clients – e.g. allocation of work
- Altering contract specifications
- Contract not completed to specification
- Contractor paid for work not done.
- Grants not used for specified purpose – e.g. leasing capital equipment instead of purchasing them

A–1 Corporate Fraud

- Lack of thorough investigations of alleged wrongdoing
- Pecuniary gain to organisation – but no personal gain

Annex B Common Methods and Types of Fraud

- Payment for work not performed
- Forged endorsements
- Altering amounts and details on documents
- Collusive bidding
- Overcharging
- Writing off recoverable assets or debts
- Unauthorised transactions
- Selling information
- Altering stock records
- Altering sales records
- Cheques made out to false persons
- False persons on payroll
- Theft of official purchasing authorities such as order books
- Unrecorded transactions
- Transactions (expenditure/receipts/deposits) recorded for incorrect sums
- Cash stolen
- Supplies not recorded at all
- False official identification used
- Damaging/destroying documentation
- Using copies of records and receipts
- Using imaging and desktop publishing technology to produce apparent original invoices
- Charging incorrect amounts with amounts stolen
- Transferring amounts between accounts frequently
- Delayed terminations from payroll
- Bribes
- Over claiming expenses
- Skimming odd pence and rounding
- Running a private business with official assets
- Using facsimile signatures
- False compensation and insurance claims
- Stealing of discounts
- Selling waste and scrap

Annex C Good Management Practices

The following are examples of good management practices that may assist in combating fraud

- All income is promptly entered in the accounting records with the immediate endorsement of all cheques
- Regulations governing contracts and the supply of goods and services are properly enforced
- Accounting records provide a reliable basis for the preparation of financial statements
- Controls operate which ensure that errors and irregularities become apparent during the processing of accounting information
- A strong internal audit presence
- Management encourages sound working practices
- All assets are properly recorded and provision is made known or expected losses
- Accounting instructions and financial regulations are available to all staff and are kept up to date
- Effective segregation of duties exists, particularly in financial accounting and cash/securities handling areas
- Close relatives do not work together, particularly in financial, accounting and cash/securities handling areas
- Creation of an agency climate to promote ethical behaviour
- Act immediately on internal/external auditor's report to rectify control weaknesses
- Review, where possible, the financial risks of employees
- Issue accounts payable promptly and follow-up any non-payments
- Set standards of conduct for suppliers and contractors
- Maintain effective security of physical assets; accountable documents (such as cheque books, order books); information, payment and purchasing systems
- Review large and unusual payments
- Perpetrators should be suspended from duties pending investigation
- Proven perpetrators should be dismissed without a reference and prosecuted
- Query mutilation of cheque stubs or cancelled cheques
- Store cheque stubs in numerical order
- Undertake test checks and institute confirmation procedures

- Develop well defined procedures for reporting fraud, investigating fraud and dealing with perpetrators
- Maintain good physical security of all premises
- Randomly change security locks and rotate shifts at times (if feasible and economical)
- Conduct regular staff appraisals
- Review work practices open to collusion or manipulation
- Develop and routinely review and reset data processing controls
- Regularly review accounting and administrative controls
- Set achievable targets and budgets, and stringently review results
- Ensure staff take regular leave
- Rotate staff
- Ensure all expenditure is authorised
- Conduct periodic analytical reviews to highlight variations to norms
- Take swift and decisive action on all fraud situations
- Ensure staff are fully aware of their rights and obligations in all matters concerned with fraud

C–1 Examples of risks and controls in specific systems for reducing opportunities for fraud

Risk	Control
PURCHASING	
Unauthorised expenditure	Ensure all expenditure is ***verified*** by the appropriate person/ team. Expenditure can only be ***authorised for payment*** by the Accountant, Finance Manager or Chief Executive. On-line banking must be approved by two individuals; Accountant and Finance Manager do not have authority (or access) to approve on-line banking.
Misuse of accounts/ fraudulent transfers into bank accounts.	Ensure that payment runs are reviewed by the Accountant or Finance Manager prior to on-line banking authorisation.
Misuse of Cheques	Store cheques in a safe place in numerical order. Make a record of any cancelled cheques.
Review large and unusual payments	Ensure that all payments have adequate business case cover. All invoices over £5,000 must be countersigned by SIB's Chief Executive.

PAYROLL	
Lack of job segregation and independent checking of key transactions.	Payroll amendments and contract variations (including starters and leavers) must be verified by HR personnel. Associate Advisor timesheets are authorised by the Strategic Support Unit or appropriate project manager. The Finance Officer collates all payroll information. Monthly salary calculations and appropriate deductions are calculated by the Finance Officer and entered onto Opera. All Payroll information is securely saved on CM. When the payroll process is complete, all payroll reports (and supporting documentation) are reviewed by the Accountant.
Lack of clear management control of responsibility, authorities, delegation.	All payroll data is reviewed by the Accountant. Any changes to contract; daily rate staff calculations and/ or any other variance are reviewed by the Finance Manager. Excel reports are matched to Opera and matched to the on-line bank payment by Accountant and Finance Manager. Payroll is approved by HR Manager and Chief Executive prior to the on-line payment authorisation.
Fictitious (or ghost) employees on the payroll.	All payroll data is reviewed by the Accountant, Finance Manager and Human Resource Manager.
Falsifying work hours to achieve fraudulent overtime payments	All overtime must be approved in advance by SIB's Chief Executive.
Improper changes in salary levels	Payroll amendments and contract variations (including starters and leavers) are verified by HR. The Finance Manager will have access to this information via business case and Investment Committee.
TRAVEL AND SUBSISTENCE	
Inadequate controls in the processing of travel and subsistence claims	SIB's Financial Policies and Procedures are available to all staff and are kept up to date. The Finance Administrator will refer to the policies when verifying claims. All travel and subsistence claims are reviewed prior to payment by the Accountant or Finance Manager.
Adding private expenses to expense claims.	The Finance Administrator verifies 100% of claims to ensure that errors and irregularities become apparent during the processing of travel and subsistence claims.

Applying for multiple reimbursements of the same expenses.	Original receipts should be provided. On occasion, scanned receipts will be permitted. The Finance Administrator will check previous claims to ensure expenses are not being claimed in error.
Submitting inflated or false expense claims.	All expense claims must be signed by the employee's Line Manager or Project Manager.
PETTY CASH	
Theft of cash	Maintain good physical security of cash. Only SIB's Finance team have access to the Petty Cash tins. Effective segregation of duties exists. Cash on-site to be kept to a minimum.
False payment requests	Ensure all expenditure is authorised prior to reimbursement.
Petty Cash transactions should be kept to a minimum.	Payment via on-line banking is always preferable.

C–2 *Fraud Prevention in Supplier payments*

Following the publication of **FD (DFP) 19/11,** SIB Finance staff must follow the guidelines below with respect to verifying supplier bank details and requests for changes:

- Closely scrutinise all requests for changes in payment details, no matter how minor.
- As part of standard procedures suppliers should be independently contacted to verify that any change of bank details or contact details is genuine.
- Verification should **not** be made using the document/letter which has been received requesting the change (which may contain false contact information) but should be done using existing contact details held on file or information obtained from directory enquiries. It may also be useful to check details provided via an Internet search of the company name. It may also be necessary, and prudent, to follow up this initial verbal contact by obtaining further written confirmation from a known contact in the supplier's firm before making changes.
- Finance staff and others dealing with any changes to suppliers' details should be made aware of this fraud risk. Staff should also be advised that they must be careful about the information they give out to callers regarding the organisation's payment processes and any unique supplier identifiers, etc. which may be held. Such callers may not be genuine and may help the fraudsters by making their subsequent requests more authentic looking.

C–3 *Grants*

Offers of Grant aid from SIB must be made using the official SIB Grant Letter of Offer template (DF1/11/138355 *"SIB Letter of Offer Template"*).

Risk of fraud or error can be reduced by following the guidelines below when issuing Grants and vouching expenditure.

- Ensuring that sufficiently detailed letters of offer are developed.
- Conducting regular inspection/verification visits.
- Vouching of expenditure back to source documentation including obtaining original cheques from banks to confirm payee details, and
- Checks are made to confirm that all invoices (i.e. 100%) provided in support of claimed expenditure are bona fide. This can include checking VAT registration numbers are genuine and are for the supplier stated; checking that suppliers do indeed exist; and seeking confirmation from suppliers that goods/services have indeed been supplied as invoiced.

Annex D Fraud Proofing Guidance (DAO (DoF) 04/18)

D–1 Introduction

1.1 Fraud is an ever-present threat and may occur internally or externally. It can be perpetrated by staff, consultants, suppliers, contractors, development partners, members of the public, users and recipients of services, and organisations. This can be done at an individual level or in collusion with other parties.

1.2 The consistent application of management controls is the most effective way of mitigating against fraud, therefore, it is vital that the controls established address the fraud risks within policies, programmes and systems (hereafter collectively referred to as systems).

1.3 It is therefore important when developing new systems that potential fraud risks are identified at an early stage and effective countermeasures developed and integrated into the design and subsequent operation.

1.4 This process is commonly referred to as 'fraud proofing'.

Fraud Risk Assessment

1.5 The more fraud risks that are identified and measures taken to address them at the outset, the less chance there is that such systems/activities are at risk of being open to fraud. When assessing fraud risks organisations need to consider all the different ways a fraudster could exploit the system/activity. This can be difficult when organisations or individuals are not used to thinking in that way.

1.6 Many new systems will be common or standard, or have common elements and there is a wealth of information available regarding the types of risks and controls which should be considered for such systems. This information is a good starting point, however, thought should also be given to whether risks exist beyond those already identified in similar systems. The Managing the Risk of Fraud guide contains some examples of risks within systems and controls that can be put in place to prevent such risks occurring.

1.7 Fraud risks in new, innovative or completely different systems/activities may point to other risks needing to be considered. It is therefore worth trying to think creatively or unconventionally to see if other, previously unidentified or unimagined risks can be identified.

1.8 Innovative schemes may be particularly vulnerable to fraud as there may be no previous information about the potential risks and the risks themselves may be hard to envision. In this situation, thinking creatively or unconventionally may be particularly important to help identify potential fraud risks. In addition it is good practice to undertake a pilot exercise in relation to complex or innovative systems, policies or programmes to help ensure that fraud risks are comprehensively identified.

1.9 Programmes with complex rules of entitlement can increase the risk of fraud as it can be difficult for staff to police effectively and it may be easier for fraudsters

to misrepresent their circumstances and, if discovered, claim that it was a genuine error. Where the level of complexity cannot be reduced, it is vital that clear guidelines are established to ensure the public and particularly staff understand the requirements.

1.10 As part of the fraud risk assessment, organisations should consider all the different parities who could commit fraud as the type of controls put in place may be different depending on the nature of the perpetrator. The list of potential external perpetrators will include those who directly interact or benefit but may also include representatives, agents and others who may try to impersonate legitimate clients.

1.11 While it may not be comfortable to consider that colleagues could be capable of committing fraud, when assessing fraud risks it is important to consider how fraud could be committed internally, including how members of staff could collude with external parties to commit fraud.

Addressing Risks

1.12 Once fraud risks have been identified, the next step is to determine how best to how to address these risks. In designing control it is important that the controls put in place are proportional to the risk. In most circumstances it is sufficient to design control to provide reasonable assurance that the risk will be mitigated.

1.13 The Orange Book : Management of Risk – Principles and Concepts highlights that there are 5 aspects to addressing risk (including fraud risk):

- Treat – This is where action is taken to manage the risk to an acceptable level. The greatest number of risks will be addressed this way.
- Tolerate – The risk may be tolerable without any action being taken. Even if the risk is not tolerable, the ability to do anything about some risks may be limited or the costs disproportionate to the potential benefit.
- Transfer – The best way to respond to some risks may be to transfer them, for example through insurance.
- Terminate – Some risks will only be containable through terminating the activity. The option of termination may be limited in overall terms, however, this may be a useful consideration in relation to specific aspects of a new system.
- Take the opportunity – this is something which should be considered when tolerating, treating or transferring risk – does an opportunity arise to exploit positive impacts?

1.14 There are different types of controls which can be utilised, depending on the nature of the risk:

- Preventative – limit the possibility of an undesirable outcome.
- Detective and Corrective – identify and correct undesirable outcomes which have been realised.

- Directive – designed to ensure a particular outcome is achieved.

1.15 The Orange Book contains further guidance on identifying, assessing and addressing risks.

Monitor and Review

1.16 It is important to recognise that control measures may not be wholly effective in preventing fraud. Therefore, on-going monitoring and review is an important aspect of any system. It is vital that new systems are subject to monitoring and review at an early stage. This will help determine whether the controls established have been effective in countering the fraud risks identified during development. Early review is particularly vital in relation to complex or innovative schemes.

1.17 During the development of new systems, consideration should be given to how the effectiveness of the system will be monitored and reviewed with appropriate arrangements established and embedded within the system. Specifically in relation to fraud prevention and detection this could include:

- Management checks;
- Exception reporting;
- Analysis to identify anomalies;
- Trend analysis; and
- On-going risk analysis.

Sources of Help

1.18 When considering fraud risks within new areas there are a range of teams/individuals who will be able to provide advice:

- Counter fraud specialists;
- Internal audit;
- Subject matter experts (e.g. procurement, grants,); and
- Teams operating similar policies, programmes or systems.

1.19 Input from these team/individuals should be sought during the development of the system to ensure that any insight they have to offer can be incorporated within system design during the development.

1.20 There is also a range of guidance available to assist with identifying, assessing and addressing fraud.

1.21 A basic checklist is also attached at which can be used by organisations when establishing or creating a new system, policy of programme. It is good practice to consider the "fraud proof-ness" of such new systems/activities and to formally record this assessment and any actions arising from it.

Orange book

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/220647/orange_book.pdf

Managing the Risk of Fraud (NI)

https://www.finance-ni.gov.uk/sites/default/files/publications/dfp/daodfp0611att.pdf

Managing the Risk of Fraud in a Changing Environment

https://www.finance-ni.gov.uk/sites/default/files/publications/dfp/fddfp0915att.pdf

Fraud Proofing Checklist

Questions	Free text to be completed by business area
Have we identified and understood what the new system /policy /programme actually is?	
Have we identified the risks associated with such an activity?	
Have we identified who may try to abuse /defraud the system /activity?	
Have we considered the controls that we need to put in place to prevent this?	
Have we engaged with relevant experts to assist us in this process?	
Has this process been formally documented and approved?	
Have the risks associated with the system /activity been included in relevant registers?	
Has the need to run a pilot been sufficiently considered?	
Has responsibility for reviewing the activity been allocated: • to a specific post holder? • within a specific timeframe?	
Has feedback from pilots or short term operation of the activity been considered and remedial action taken where required?	
Are there arrangements in place for the results of such reviews in place to report back to senior management?	

Annex E Public Interest Disclosure (NI) Order 1998[1]

E–1 What Type Of Disclosure Will Qualify For Protection?

A disclosure will qualify for protection ("a qualifying disclosure") if, you reasonably believe, it tends to show one or more of the following has occurred, is occurring or is likely to occur:

- A criminal offence (e.g. theft and fraud).
- A failure to comply with a legal obligation.
- A miscarriage of justice.
- Endangering of an individual's health and safety.
- Damage to the environment.
- Deliberate concealment of information tending to show any of the above.

E–2 When Are Disclosures Protected?

A qualifying disclosure will be protected under the Act when it is made in good faith:

- To your employer.
- To a body or person other than your employer.[2]
- To a legal adviser in the course of obtaining legal advice.
- To a Minister of the Crown.
- To a prescribed body or person, provided that you reasonably believe that the relevant failing falls within matters prescribed to that body or person and that the information is substantially true. For a list of prescribed persons, please see Annex F on page 45.

E–3 Circumstances in Which Disclosures Are Not Protected

The legislation does not introduce a general protection for whistle-blowers in all circumstances. Individuals who make disclosures will not be protected by the Act if they commit an offence by making the disclosure.

E–4 Further Information

For further information see the Whistle-blowing Disclosures page on the Northern Ireland Audit Office website.

[1] http://www.legislation.gov.uk/nisi/1998/1763/contents/made

[2] Provided that you reasonably believe that the relevant failure relates solely or mainly to the conduct of that body or person, or relates to a matter over which the body or person has legal responsibility.

Annex F Prescribed Persons

This table is extracted from the Schedule to Statutory Rule 1999 No. 401, Public Interest Disclosure (Prescribed Persons) Order (Northern Ireland) 1999.

COLUMN (1) PERSONS AND DESCRIPTIONS OF PERSONS	COLUMN (2) DESCRIPTIONS OF MATTERS
Building Societies Commission	The operation of building societies.
Certification Officer for Northern Ireland	Fraud, and other irregularities, relating to the financial affairs of trade unions and employers' associations.
Chief Executive of the Criminal Cases Review Commission	Actual or potential miscarriages of justice.
Civil Aviation Authority	Compliance with the requirements of civil aviation legislation, including aviation safety.
Commissioners of Customs and Excise	Value added tax, insurance premium tax, excise duties and landfill tax. The import and export of prohibited or restricted goods.
Commissioners of the Inland Revenue	Income tax, corporation tax, capital gains tax, petroleum revenue tax, inheritance tax, stamp duties, national insurance contributions, statutory maternity pay and statutory sick pay.
Comptroller and Auditor General for Northern Ireland	The proper conduct of public business, value for money, fraud and corruption in relation to the provision of centrally funded public services.
Data Protection Registrar	Compliance with the requirements of legislation relating to data protection.
Department of Agriculture	Acts or omissions which have an actual or potential effect on the flows in rivers or on drainage of land.
	Acts or omissions which have an adverse or potentially adverse effect on fish in the sea, inland fisheries, or on migratory salmon or trout.
Department of Economic Development	Fraud and other misconduct in relation to companies. Compliance with the requirements of consumer protection and fair trading legislation.
Department of the Environment	Acts or omissions which have an actual or potential effect on the environment or

COLUMN (1) PERSONS AND DESCRIPTIONS OF PERSONS	COLUMN (2) DESCRIPTIONS OF MATTERS
	the management or regulation of the environment including those relating to pollution.
Department of Health and Social Services and auditors appointed by that Department	The proper conduct of public business, value for money, fraud and corruption in health service bodies.
Director General of Electricity Supply for Northern Ireland	The generation, transmission, distribution and supply of electricity and activities ancillary to these matters.
Director General of Fair Trading	Matters concerning the sale of goods or the supply of services which adversely affect the interests of consumers. Matters relating to consumer credit and hire, estate agency, unfair terms in consumer contracts and misleading advertising. The abuse of a dominant position in a market and the prevention, restriction or distortion of competition.
Director General of Gas for Northern Ireland	The conveyance, storage and supply of gas, and activities ancillary to these matters.
Director General of Telecommunications	The provision and use of telecommunication systems, services and apparatus.
Director of the Serious Fraud Office	Serious or complex fraud.
District Councils	Matters which may affect the health or safety of any individual at work; matters, which may affect the health or safety of any member of the public, arising out of or in connection with the activities of persons at work.
	Compliance with the requirements of consumer safety legislation.
Financial Services Authority	The carrying on of investment business or of insurance business; the operation of banks, deposit-taking businesses and wholesale money market regimes; the functioning of financial markets, investment exchanges and clearing houses; the functioning of other financial regulators; money laundering, financial crime, and other serious financial misconduct, in

COLUMN (1) PERSONS AND DESCRIPTIONS OF PERSONS	COLUMN (2) DESCRIPTIONS OF MATTERS
	connection with activities regulated by the Financial Services Authority.
Fisheries Conservancy Board for Northern Ireland	Acts or omissions which have an adverse or potentially adverse effect on inland fisheries or on migratory salmon or trout.
Foyle Fisheries Commission	Acts or omissions which have an adverse or potentially adverse effect on inland fisheries or on migratory salmon or trout.
Friendly Societies Commission	The operation of friendly societies and industrial assurance companies.
Health and Safety Executive for Northern Ireland	Matters which may affect the health or safety of any individual at work; matters, which may affect the health or safety of any member of the public, arising out of or in connection with the activities of persons at work.
Investment Management Regulatory Organisation	The activities of persons regulated by the Investment Management Regulatory Organisation.
Local government auditors appointed by the Department of the Environment	The proper conduct of public business, value for money, fraud and corruption in district councils, the Northern Ireland Housing Executive, the Fire Authority for Northern Ireland, the Northern Ireland Local Government Officers' Superannuation Committee and the Local Government Staff Commission for Northern Ireland.
Occupational Pensions Regulatory Authority	Matters relating to occupational pension schemes and other private pension arrangements.
Personal Investment Authority	The activities of persons regulated by the Personal Investment Authority.
Registrar of Credit Unions for Northern Ireland	The operation of credit unions and industrial and provident societies.
Securities and Futures Authority	The activities of persons regulated by the Securities and Futures Authority.
The competent authority under Part IV of the Financial Services Act 1986[2]	The listing of securities on a stock exchange; prospectuses on offers of transferable securities to the public.
Treasury	The carrying on of insurance business.

COLUMN (1) PERSONS AND DESCRIPTIONS OF PERSONS	COLUMN (2) DESCRIPTIONS OF MATTERS
A person ("person A") carrying out functions, by virtue of legislation, relating to relevant failures falling within one or more matters within a description of matters in respect of which another person ("person B") is prescribed by this Order, where person B was previously responsible for carrying out the same or substantially similar functions and has ceased to be so responsible	Matters falling within the description of matters in respect of which person B is prescribed by this Order to the extent that those matters relate to functions currently carried out by person A