Anti-Fraud Policy

Policy Number:
041-2016

Academic Year:
2024/2025 Onwards

Target Audience:
All Staff and Governors

Summary of Contents
Guidance on responsibilities regarding the prevention of fraud and the procedures to be used if fraud is suspected.

Enquiries
Any enquiries about the contents of this document should be addressed to:

Title: Deputy Chief Executive

Email: policies@serc.ac.uk

Review Information (responsible owner):
First Created: May 2016

Last Reviewed: June 2024

Next Review: June 2025

Change Type at last Review:

~~No~~/Minor/~~Significant~~ (delete as appropriate)

Approval/Noting By:
CMT: June 2024

Lead GB Committee: Finance & Staffing

Governing Body Approval: June 2024

Related Documents:
SERC Financial Governance Policy
SERC Risk Management Policy
Partnership Agreement between the Department for the Economy and the College
SERC Anti-Bribery Policy; Gifts & Hospitality Policy; Whistleblowing Policy; Conflicts of Interest Policy

Superseded Documents (if applicable):
Anti-Fraud Policy and Fraud Response Policy 29-2008

Date of Equality of Opportunity and Good Relations Screening (Section 75):
July 2016

Date of Last Accessibility Screening:
April 2024

1.0 Contents

1.0 CONTENTS 0
2.0 CHANGE HISTORY 1
3.0 BACKGROUND AND INTRODUCTION 1
4.0 SCOPE 1
5.0 DEFINITION OF FRAUD 1
6.0 COLLEGE RESPONSIBILITIES 2
7.0 HEADS OF SCHOOL / DEPARTMENT RESPONSIBILITIES 4
8.0 STAFF RESPONSIBILITIES 5
9.0 INTERNAL AUDIT 6
10.0 AUDIT AND RISK COMMITTEE 6
11.0 DEPARTMENT FOR THE ECONOMY ('THE DEPARTMENT') 6
12.0 FRAUD INVESTIGATION 7
13.0 NATIONAL FRAUD INITIATIVE 7
14.0 FRAUD RISK ASSESSMENTS 7
15.0 DISCIPLINARY ACTION 8
16.0 MALICIOUS ALLEGATIONS 9
17.0 CONCLUSION 9
18.0 RESPONSIBLE OWNER 9
19.0 COMMUNICATION PLAN 9
20.0 REVIEW 9
APPENDIX 1: DOCUMENT CHANGE HISTORY 10
APPENDIX 2: INDICATORS OF FRAUD 11
APPENDIX 3: COMMON METHODS AND TYPES OF FRAUD 13
APPENDIX 4: EXAMPLES OF GOOD MANAGEMENT PRACTICES/CONTROLS WHICH MAY ASSIST IN COMBATING FRAUD 15
APPENDIX 5: REDUCING OPPORTUNITIES FOR FRAUD 16
APPENDIX 6: GUIDANCE ON PERFORMING AN ASSESSMENT OF FRAUD RISKS 19
APPENDIX 7: CONTACT DETAILS 24

2.0 Change History

2.1 Changes to this SOP are documented in Appendix 1 of this document. When reading electronic copies of this document, you can click here to view the change history.

3.0 Background and Introduction

3.1 There is a continuing need to raise staff awareness of our responsibility to safeguard public resources against the risk of fraud.

3.2 Fraud is not a victimless crime. We are entrusted with taxpayers' money, and we must look after it in the same way that we look after our own, therefore we must be aware of:

- what constitutes fraud;
- the potential for fraud;
- steps to prevent fraud in the first instance; and
- what to do in the event of fraud or if we suspect fraud has occurred.

3.3 The College's Anti-Fraud Policy sets out the actions we must take and the responsibilities we have to prevent fraud.

3.4 This policy relates to fraud and loss within the College and applies to all monies for which the College is accountable, including expenditure through projects.

3.5 The College requires all staff, at all times, to act honestly and with integrity, and to safeguard the public resources for which they are responsible.

3.6 Fraud is an ever-present threat to resources and must be a concern to all members of staff.

3.7 The College takes a **zero-tolerance** approach and will not therefore tolerate any level of fraud or corruption; consequently, College policy is to thoroughly investigate all suspect frauds and allegations (anonymous or otherwise) and where appropriate, refer to the policy at the earliest juncture and seek recover of all losses, if necessary, through civil action.

3.8 The College is committed to ensuring that opportunities for fraud and corruption are reduced to the lowest possible level of risk.

4.0 Scope

4.1 This Policy applies to all staff and members of the Governing Body.

5.0 Definition of Fraud

5.1 Fraud is when someone obtains financial advantage or causes loss by implicit or explicit deception.

5.2 Fraud is not a victimless crime and is generally used to describe such acts as deception, bribery, money laundering, forgery, extortion, corruption, theft, conspiracy, embezzlement, misappropriation, false representation, concealment of material facts and collusion.

5.3 Computer fraud is where information technology (IT) equipment has been used to manipulate computer programs or data dishonestly (for example by altering or substituting records, destroying or suppressing records, duplicating or creating spurious records), or where the existence of an IT system was a material factor in the perpetration of fraud (i.e. where the fraud

was unlikely to have occurred if there had been no IT system). Theft or fraudulent use of computer facilities, computer programs and the Internet is included in this definition. The suspicion that any of these acts have taken place should be regarded as potentially fraudulent.

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

- **Fraud by false representation**, i.e. if someone dishonestly makes a false representation and intends, by making the representation, to make a gain for themselves or another, or to cause loss to another or expose another to risk of loss. A representation is false if it is untrue or misleading, and the person making it know that it is, or might be, true or misleading;
- **Fraud by failing to disclose information**, i.e. if someone 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; and
- **Fraud by abuse of position**, i.e. if someone 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.

5.5 Fraud by way of bribery is covered under The UK Bribery Act 2010, which came into effect on 1 July 2011. The Act modernises the law on bribery and seeks to provide a revised framework of offences to combat bribery in the public and private sectors. It abolishes the offences of bribery at common law and the statutory offences in the Public Bodies Corrupt Practices Act 1889 and the Prevention of Corruption Act 1906. The College has a detailed Anti-Bribery Policy to meet the requirements of the UK Bribery Act 2010, which is part of the measures to minimise the risk of fraud.

5.6 At a basic level four elements are normally necessary for a fraud to occur:

- People to carry out the fraud. They may be individuals within the organisation, outside the organisation, and/or a group of people working inside or outside the organisation.
- Assets of some form to acquire fraudulently.
- Intent to commit the fraud; and
- Opportunity.

5.7 Managers must ensure that the opportunities for fraud are minimised. Opportunities to commit fraud may be reduced by ensuring that a sound system of internal control, proportional to risk, has been established and that it is functioning as intended. While some people would never contemplate perpetrating a fraud, others may if they thought they could do it without being detected. A high chance of being caught will often deter such individuals.

6.0 College Responsibilities

6.1 The College's Accounting Officer (Principal and Chief Executive) is responsible for establishing and maintaining a sound system of internal control that supports the achievement of the College's policies, aims and objectives.

6.2 The system of internal control is designed to respond to and manage the whole range of risks that South Eastern Regional College (SERC) faces. The system of internal control is based on

an on-going process designed to identify the principal risks, to evaluate the nature and extent of those risks and to manage them effectively.

6.3 Managing fraud risk will be seen in the context of the management of this wider range of risks.

6.4 Overall responsibility for managing the risk of fraud has been delegated to the Deputy Chief Executive. Other College Directors also have a key responsibility to take steps, as are reasonably open to them, to prevent and detect fraud.

6.5 Responsibilities of the Deputy Chief Executive include:

a. Developing the College's Fraud Risk Register and overseeing regular reviews of the College fraud risk assessments in order to keep the Register current;
b. Establishing an effective anti-fraud policy and fraud response plan, commensurate to the level of fraud risk identified in the College's Fraud Risk Register;
c. Developing an effective control environment to prevent fraud commensurate with the level of fraud risk;
d. Assessing the risk of the College being used for money laundering;
e. Advising on the conduct of fraud investigations;
f. Ensuring that vigorous and prompt investigations are carried out if fraud occurs, is attempted, or is suspected and appropriate action is taken to recover assets and losses;
g. Establishing appropriate mechanisms for:
    - Reporting fraud risk issues;
    - Reporting all incidents of fraud to the Accounting Officer;
    - Staff to report all instances of suspected or actual fraud to line management/Head of Department who must then report to the Deputy Chief Executive;
    - Reporting, externally, to Department for the Economy and Northern Ireland Audit Office;
    - Coordinating assurances about the effectiveness of the anti-fraud policy and fraud response plan to support the College's annual Governance Statement;
    - Liaising with the Audit & Risk Committee;
    - Making sure that all staff are aware of the College's anti-fraud policy and know what their responsibilities are in relation to combating fraud; and
    - Ensuring that appropriate action is taken to minimise the risk of similar frauds occurring in future.

6.6 The Head of Human Resources also has specific responsibilities which include ensuring that:

a. Appropriate pre-employment screening measures are undertaken;
b. Anti-fraud awareness training is provided as appropriate and, if necessary, more specific anti-fraud training and development is provided to relevant staff;
c. Providing advice and support to management in implementing suspensions and any subsequent disciplinary investigation, including advising on the application of the College Disciplinary Policy;
d. Where appropriate, legal, and/or disciplinary action is taken against perpetrators of fraud;
e. Where appropriate, disciplinary action is taken against supervisors where supervisory failures have contributed to the commission of fraud; and
f. Where appropriate, disciplinary action is taken against staff who fail to report fraud.

6.7 Responsibilities of all Directors include:

a. Taking steps to provide reasonable assurance that the activities of the College are conducted honestly and that its assets are safeguarded, including assessing the fraud risk involved in the operations/area for which they are responsible;

b. Ensuring, that to the best of their knowledge and belief, financial information, whether used in the College's operations, business or for financial reporting, is reliable.
c. Establishing arrangements designed to deter fraudulent or other dishonest conductions and ensuring that these arrangements are complied with;
d. Where a fraud has taken place, implementing new controls to reduce the risk of similar fraud;
e. Reporting any instances of suspected or proven fraud to the Deputy Chief Executive as soon as they become aware of such instances;
f. Where appropriate overseeing the conduct of fraud investigations and liaising where necessary with the Deputy Chief Executive in accordance with the Fraud Response Plan;
g. Ensure that appropriate action is taken to recover assets and losses; and
h. Providing updates on open fraud cases.

7.0 Heads of School / Department Responsibilities

7.1 Heads of School / Department are responsible for ensuring that an adequate system of internal control exists within their areas of responsibility and that controls operate effectively.

7.2 Responsibility for the prevention and detection of fraud, therefore, rests primarily with Heads of School / Department.

7.3 A major element of good corporate governance is a sound assessment of the College's business risks. Heads of School / Department need to ensure that:

a. Fraud risks have been identified within risk registers based on a review of the operations/area for which they are responsible;
b. Each risk has been assessed for likelihood and potential impact;
c. Adequate and effective controls have been identified for each risk;
d. Controls are being complied with, through regular review and testing of control systems and continue to operate effectively;
e. Risks are reassessed as a result of the introduction of new systems or amendments to existing systems;
f. Where a fraud has occurred, or has been attempted, controls are reviewed and new controls implemented, as necessary, to reduce the risk of fraud recurring; and
g. Fraud occurrences are quantified on an annual basis and risk registers updated to reflect the quantum of fraud within the School/Department. Where appropriate, strategies should be devised to combat recurrence of fraud and targets set to reduce the level of fraud.

7.4 In terms of establishing and maintaining effective controls, Heads of Schools / Department should ensure:

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

7.5 As fraud prevention is the ultimate aim, anti-fraud measures should be considered and incorporated in every system and programme at the design stage, e.g. the design of application forms, regular monitoring of expenditure etc.

7.6 Advice is available from the Directors to Heads of School / Department on risk and control issues in respect of existing and developing systems/programmes.

8.0 Staff Responsibilities

8.1 Every member of staff has a duty to ensure that public funds are safeguarded and therefore, everyone is responsible for:

- Acting with propriety in the use of official resources and the handling and use of public funds in all instances. This includes cash and/or payment systems, receipts and dealing with suppliers;
- Conducting themselves in accordance with the seven principles of public life detailed in the first report of the Nolan Committee 'Standards in Public Life', 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. Appendix 2 provides examples of Fraud Indicators. In addition, Common Methods and Types of Fraud are included in Appendix 3, with Examples of Good Management Practices Which May Assist in Combating Fraud, are detailed in Appendix 4 and guidance on Reducing Opportunities for Fraud detailed in Appendix 5.

8.2 In addition, it is the responsibility of every member of staff to report details immediately to their line management/Head of School or Department, or the Deputy Chief Executive, if they suspect that a fraud has been attempted or committed or see any suspicious acts or events. More details on reporting are included in the College's Fraud Response Plan.

8.3 The Public Interest Disclosure (NI) Order 1998 protects the rights of staff who report wrongdoing. If you are in any doubt, you should speak to a member of the College Management Team.

8.4 Advice is also available through the independent charity Public Concern at Work on 020 7404 6609. 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.

8.5 Section 5 of the Criminal Law Act (Northern Ireland) 1967 (Withholding Information) 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 in the Fraud Response Plan.

8.6 Staff must also assist any investigations by making available all relevant information, by co-operating in interviews, and if appropriate provide a witness statement.

8.7 As stewards of public funds College staff must have, and be seen to have, high standards of personal integrity. Staff, including temporary staff or contractors, should not accept gifts, hospitality, or benefits of any kind from a third party, which might be seen to compromise their integrity (Refer to SERC's Gifts and Hospitality Policy).

8.8 It is also essential that staff understand and adhere to the College's Policies and SOPs including those such of a personnel/management nature such as submission of expenses claims and records of absence, flexi, and annual leave.

8.9 All staff are advised to consider their personal and business activities and whether these may be considered to conflict with their duty of office. Refer to the Conflicts of Interest Policy.

9.0 Internal Audit

9.1 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 the College promotes an anti-fraud culture is a fundamental element in arriving in overall opinion.

9.2 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 are planned to assist in deterring and preventing fraud by examining and evaluating the effectiveness of control commensurate with the extent of the potential exposure/risk.

9.3 Internal Audit will review Risk and Control Frameworks to ensure that management have reviewed their risk exposures and, where appropriate, identified the possibility of fraud as a College risk.

10.0 Audit and Risk Committee

10.1 The Audit & Risk Committee is responsible for understanding the College's strategy, control environment and risks, which includes an understanding of the College's fraud risk.

10.2 The Audit & Risk Committee is also responsible for:

- understanding the role of those charged with governance in relation to managing risk (including fraud risk);
- familiarisation with the College's policies and procedures relating to fraud risk;
- understanding the College's framework and allocation of responsibilities for risk management;
- being aware of the vulnerability of the College to changing conditions, such as economic pressures;
- critically reviewing and challenging the framework for managing risk, including fraud risk; and
- critically reviewing and challenging the control environment in place to mitigate risk, including fraud risk.

11.0 Department for the Economy ('the Department')

11.1 The College is responsible for reporting, immediately, to the Department all frauds (proven or suspected), including attempted fraud.

11.2 The Department is responsible for reporting any fraud reporting by the College, immediately, to the Department of Finance and the Comptroller & Auditor General (C&AG).

11.3 The Department's Fraud & Raising Concerns Branch is available to the College for advice and assistance if required.

11.4 The College is responsible for providing the Department with follow-up information as soon as it becomes available.

11.5 The Department is responsible for reviewing the College's Anti-Fraud Policy and Fraud Response Plan. The College shall notify the Department of any subsequent changes to the policy or response plan.

12.0 Fraud Investigation

12.1 All Heads of School/Department should be alert to the possibility that unusual events or transactions can be symptoms of fraud or attempted fraud. Fraud may also be highlighted as a result of specific management checks or be brought to management's attention by a third party. It is College policy that there will be consistent handling of all suspected fraud cases without regard to position held or length of service, and investigators should have free access to all staff, records, and premises in order to carry out investigations.

12.2 After suspicion has been roused, prompt action is essential, and all cases of suspected or actual fraud should be reported immediately to the Deputy Chief Executive who can provide advice on next steps.

12.3 Heads of School / Department **should not** undertake preliminary enquires until any suspicion has been reported to and advice taken from the Deputy Chief Executive. As detailed in the Fraud Response Plan, it is imperative that enquiries should not prejudice subsequent investigations or corrupt evidence, therefore, if in doubt, ask for advice.

12.4 If an initial examination confirms the suspicion that a fraud has been perpetrated or attempted, management should follow the procedures provided in the College's Fraud Response Plan.

13.0 National Fraud Initiative

13.1 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 data from a range of public bodies, for the purposes of assisting in the prevention and detection of fraud.

13.2 The College provides payroll, pensions, and trade creditors' data sets to identify cases of suspected fraud and overpayments.

13.3 Participation in the NFI represents a key strand of the College's Anti-Fraud Policy.

14.0 Fraud Risk Assessments

14.1 CIPFA's Code of Practice[1] states:
'Fraud risk identification is essential to understand specific exposures to risk, changing patterns in fraud and corruption threats and potential consequences to the organisation and its service users'.

14.2 The key to managing the risk of fraud is the same in principle as managing any other business risk and should be approached systematically at both the organisational and the operational level.

14.3 The key advantage of a Fraud Risk Assessment is that it improves an organisation's focus on its processes and controls with a view to minimising:

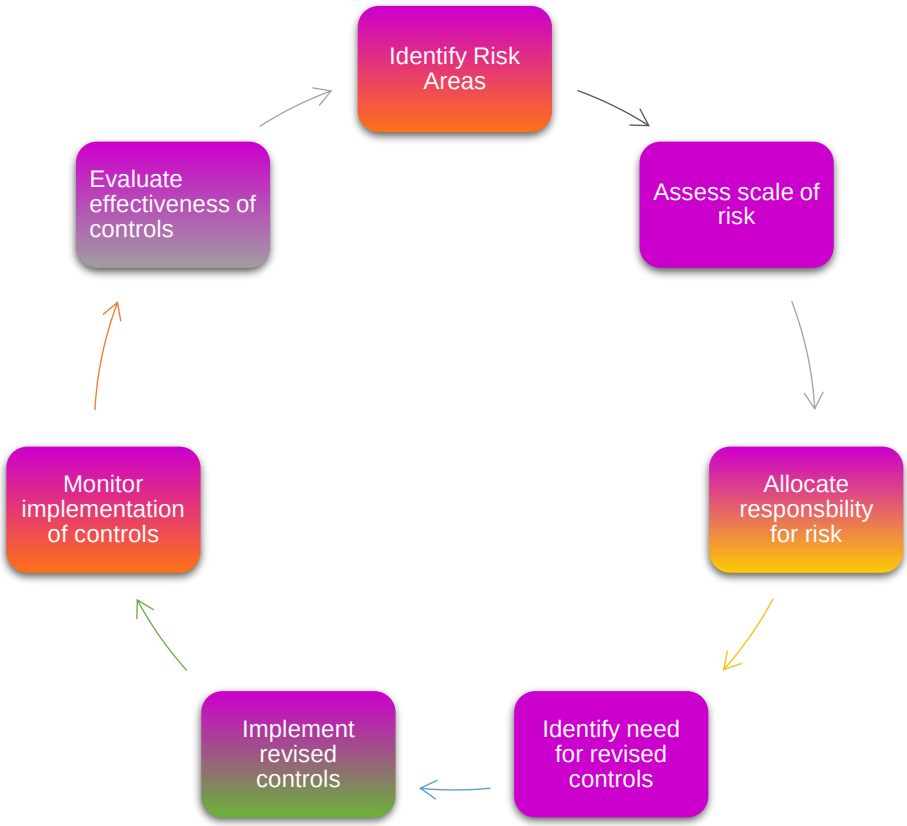
- The risk of loss through fraud;
- The opportunities for fraud; and
- The risk of reputational damage.

[1] Code of Practice on Managing the Risk of Fraud and Corruption, CIPFA, December 2014

14.4 The assessment of risk should be part of a continuous cycle rather than a one-off event: as systems and the environment change, so do the risks to which the College and College departments will be exposed.

14.5 Figure 1 below sets out the key stages of a risk management cycle to help deal with fraud:

Figure 1 - Risk Management Cycle



14.6 SERC's fraud risk assessments will be reviewed every 2 years or when there is organisational change, to ensure that any new fraud risks are identified and addressed. SERC's Audit Committee will review the corporate fraud risk assessment when updated.

14.7 Colleges will share their strategic risk registers and fraud risk assessments annually via the Northern Ireland Finance Officers' Network (NIFON) for information and discussion.

14.8 Internal Audit is available to offer advice and assistance on risk management/ internal control issues along with DfE's Fraud and Raising Concerns Branch.

14.9 Appendix 6 provides Guidance on Performing a Fraud Risk Assessment.

15.0 Disciplinary Action

15.1 After full investigation, the College will take legal and/or disciplinary action in all cases where it is considered appropriate. A member of staff found guilty of a criminal act will be considered to have committed a serious disciplinary offence and will be sanctioned under the Disciplinary Policy.

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

15.3 It is College policy that, where appropriate, all cases of fraud, whether perpetrated or attempted by a member of staff or by external organisations or persons, will be referred to the PSNI at the earliest possible juncture.

15.4 Appropriate steps will be taken to **recover all losses** resulting from fraud, if necessary, through civil action.

16.0 Malicious Allegations

16.1 If an allegation is made frivolously, in bad faith, maliciously or for personal gain, disciplinary action may be taken against the person making the allegation.

17.0 Conclusion

17.1 It is appreciated that the circumstances of individual frauds will vary. The College takes fraud very seriously, taking a **zero-tolerance** approach, 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, including recovery of losses. Managers should be fully aware of their responsibility to protect public funds and as such, should always be alert to the potential for fraud.

17.2 Any queries in connection with this Anti-Fraud Policy should be directed to the Deputy Chief Executive.

17.3 Current contact details are provided in Appendix 7.

18.0 Responsible Owner

18.1 It is the responsibility of Deputy Chief Executive to ensure that this policy is implemented, adhered to, and reviewed.

19.0 Communication Plan

19.1 This Procedure will be uploaded to the College intranet and referred to in staff induction and training.

20.0 Review

20.1 This procedure will be reviewed annually, or when the need for change has been identified.

Appendix 1: Document Change History

Version	Date	Change Detail
1.0	May 2016	Created
1.1	June 2020	Update title of Audit & Risk Committee Update of Appendices 1, 2 & 3 to include categorisation and further examples of: - Indicators of fraud; - Methods of fraud; and - Controls to combat fraud.
1.2	June 2021	Updated contact details of Internal Audit following contract change.
1.3	March 2022	Fraud Risk Assessment section amended Section 9 created to detail role/responsibility of the Department for the Economy.
1.4	June 2023	Reviewed and no changes required.
1.5	April 2024	Accessibility Checked
1.6	June 2024	Update job titles to reflect new College structure. Reference to Management Statement and Financial Memorandum changed to Partnership Agreement.

Appendix 2: Indicators of Fraud

Fraud indicators are clues or hints that a closer look should be made at an individual, area or activity.

Examples of issues that could be investigated to ensure fraud is not taking place include:

Organisational Indicators

- Lack of effective Board oversight.
- No fraud risk assessment.
- Lack of Anti-Fraud Policy and Fraud Response Plan.
- Lack of clear financial delegations.
- Climate of fear or an unhealthy corporate culture.
- Management frequently overriding internal controls.
- Lack of established code of ethical conduct.
- Lack of thorough investigations of alleged wrongdoing.
- Strained relationships between management and internal/external auditors.

Operational Indicators

- Inadequate recruitment processes and absence of staff screening (including casual staff, contractors, consultants).
- Lack of segregation of duties.
- Lack of rotation of duties.
- Lack of management supervision of staff.
- Excessive staff turnover in key control areas.
- Dissatisfied staff in key control areas.
- Significant workforce reductions/redundancies.
- Inadequate monitoring to ensure that controls work as intended (periodic testing and evaluation).
- Absence of key controls and audit trails.
- Consistent failures to correct major weaknesses in internal control.
- Missing expenditure vouchers and unavailable official records.
- Documentation that is photocopied, altered, or lacking essential information.
- Use of ‘rubber stamp’ signatures.
- Missing authorisation signatures.
- Bank reconciliations not maintained or balanced.
- Other control account reconciliations not maintained or balanced.
- Extensive use of suspense accounts and journal entries.
- Unauthorised changes to systems or work practices.
- Excessive control of all records by one officer.
- Subordinates by-passing managers.
- Suppliers/contractors who insist on dealing with one particular member of staff.
- Multiple cash collection points.
- Remote locations.
- Poor physical security of assets.
- Unexplained differences between inventory checks and stock records.
- Poor access controls to physical assets.
- Poor access controls to IT security systems.
- Poor IT security practices e.g. sharing or displaying passwords.
- Breaches in data security.
- Systems being accessed outside normal working hours.
- Control/audit logs being switched off.
- Crisis management coupled with a pressured business environment.

- Large payments to individuals.
- Defining needs in ways that can only be met by specific contractors.
- Splitting up requirements to get under small purchase requirements or to avoid prescribed controls.
- Vague procurement specifications.

Personal Indicators

- Employees apparently living beyond their means.
- Employees with outside business interests or other jobs.
- Employees with drink, drug, or gambling problems.
- Employees suffering financial hardship, e.g. borrowing from fellow employees.
- Employees who are first to arrive in the morning and last to leave at night.
- Egoistical employees, e.g. scornful of system controls.
- Marked character changes in employees.
- Employee secretiveness.
- Employees working unusual hours on a regular basis.
- Employees who refuse to comply with normal rules and practices.
- Employees not taking leave or working excessive overtime.
- Employees socialising with contractors or suppliers, accepting meals, drinks, or holidays.
- Disgruntled employees.

Appendix 3: Common Methods and Types of Fraud

Staff Fraud

- Claiming for overtime not worked.
- Secondary employment during working hours.
- Abuse of flexible working.
- Working while on sick leave.
- Over claiming expenses (including travel and subsistence).
- Skimming odd pence and rounding.
- Running a private business with official assets.
- Selling waste and scrap.
- Stolen equipment and supplies.

Payroll Fraud

- False persons on payroll.
- Change of employee account details (external fraudster purporting to be an employee).
- Delayed terminations from payroll.

Supplier Fraud

- Payment for work not performed.
- Forged endorsements (e.g. in order to win contracts).
- Collusive bidding for contracts.
- Overcharging.

Cyber Fraud

- Bank mandate fraud (requests to change bank details).
- Ransomware.
- Account hacking.
- Using imaging and desktop publishing technology to produce apparent original invoices.

Documentation Fraud

- Altering stock records.
- Altering sales records.
- Altering amounts and details on invoices/documents.
- Cheques made out to false persons.
- Supplies not recorded at all.
- False official identification used.
- Damaging/destroying documentation.
- Lack of documentation.

Accounting fraud

- Writing off recoverable assets or debts.
- Unauthorised transactions.
- Transactions (expenditure/receipts/deposits) recorded for incorrect sums.
- Theft of official purchasing authorities such as order books.
- Unrecorded transactions.
- Transactions (expenditure/receipts/deposits) recorded for incorrect sums.
- Cash stolen.
- Using copies of records and receipts.

Other

- Charging incorrect amounts with amounts stolen.
- Transferring amounts between accounts frequently.
- Bribes.
- False compensation and insurance claims.
- Stealing of discounts.
- Selling information.

Appendix 4: Examples of Good Management Practices/Controls Which May Assist in Combating Fraud

Organisational Controls

- Ethical culture and 'tone from the top'.
- An effective Board.
- Code of conduct for all staff.
- Sound working practices.
- A strong internal audit presence.
- Well defined procedures for reporting fraud or other concerns.
- Effective investigation of fraud and application of sanctions.
- Regular fraud awareness training for all staff.

Operational Controls

- Effective controls and controls testing.
- Prompt implementation of audit recommendations to rectify control weaknesses.
- Effective segregation of duties, particularly in financial accounting and cash handling.
- Rotation of staff, particularly in key posts.
- Adherence to authorisation limits.
- Prompt recording of all income.
- Regulations governing contracts and the supply of goods and services are properly enforced.
- Effective contracts management for supply of goods and services.
- Effective security of all physical assets (including premises, equipment, financial stationery etc.).
- Effective security of IT systems (access controls, passwords, audit trails).
- Up-to-date financial regulations and accounting instructions.
- Prompt issue of accounts payable and follow-up of any non-payments.
- Periodic review of large and unusual payments.
- Periodic analytical reviews to highlight variations to the norm.

Good Practices

- Conduct regular staff appraisals.
- Review work practices open to collusion or manipulation.
- Review large and unusual payments.
- Develop well defined procedures for reporting fraud, investigating fraud, and dealing with perpetrators.
- Perpetrators should be suspended from duties pending investigation.
- Proven perpetrators should be dismissed without a reference and prosecuted.
- Set achievable targets and budgets, and stringently review results.
- Ensure staff take regular leave.
- 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.

Appendix 5: Reducing Opportunities for Fraud

Introduction

The absence of proper control and the failure to observe existing control procedures are the main contributory factors in most frauds.

Managers must ensure that the opportunities for fraud are minimised. Separation of duties, effective procedures and checks should prevent or deter fraud from occurring.

Opportunities to commit fraud may be reduced:

- By ensuring that a sound system of internal control proportional to risk has been established and that it is functioning as intended;
- Through the “fear factor” (i.e. the risk of being caught or the severity of the consequences);
- By changing attitudes to fraud; and
- By making it too much effort to commit.

Internal Control

“Control” is any action, procedure or operation undertaken by management to increase the likelihood that activities and procedures achieve their objectives. Control is a response to risk – it is intended to contain uncertainty of outcome.

Some frauds arise because of a system weakness such as a lack of proper control over e.g. placing of purchase orders. Other frauds are the result of failures to follow proper control procedures. It may be the result of carelessness in carrying out a check, or it may be that too much trust has been placed in one individual with no effective separation of duties. Frauds that result from collusion may be more difficult to detect and prevent as these types of fraud tend to operate within the normal control environment.

In designing control, it is important that the control put in place is proportional to the risk. In most cases it is normally sufficient to design control to give a reasonable assurance of confining loss within the risk appetite of the organisation. Every control action has an associated cost, and it is important that the control action offers value for money in relation to the risk that it is controlling. Generally speaking, the purpose of control is to contain risk to a reasonable level rather than to remove it entirely.

When risks and deficiencies in the level of control are identified it is necessary to choose the most appropriate type of controls within the above guidelines. In respect of fraud risks prevention is almost always preferable to detection. Strong preventive controls should therefore be applied wherever possible.

The following range of controls should be considered always ensuring that a balance between identified risk and value for money is maintained:

Physical security*:* this is a preventive measure which controls or monitors access to assets, documentation, or IT systems to ensure that there is no unauthorised use, loss, or damage.

Assets can range from the computer terminal that sits on the desk to the cheques sent out to pay suppliers. As a general principle all assets should be held securely and access to them restricted as appropriate. The control should apply not only to the premises but also to computers, databases, banking facilities, documents and any other area that is critical to the operation of the individual organisation. It may even be appropriate to restrict knowledge of the existence of some assets.

Access to computer systems is an important area that should be very tightly controlled, not only to prevent unauthorised access and use, but also to protect the integrity of the data - the Data Protection Act requires computer and data owners to secure information held on their systems which concerns third parties. This threat may increase with the introduction of systems designed to meet current and future Government targets (e.g. to allow the public to do business electronically with government departments, to link public sector computer systems etc.). Computers are also vulnerable to theft, both in terms of hardware and software. This type of theft also has the potential to cause major disruption, significant financial loss or even serious reputational damage to the core operations of an organisation.

***Organising**:* organising involves the allocation of responsibility to individuals or groups so that they work together to achieve objectives in the most efficient manner. Major principles in organising relevant to fraud are:

- Clear definition of the responsibilities of individuals for resources, activities, objectives, and targets. This includes defining levels of authority. This is a preventive measure which sets a limit on the amounts which may be authorised by individual officers. To be effective, checks need to be made to ensure that transactions have been properly authorised;
- Establishing clear reporting lines and the most effective spans of command to allow adequate supervision;
- Separating duties to avoid conflicts of interest or opportunities for abuse. This is also largely a preventive measure which ensures that the key functions and controls over a process are not all carried out by the same member of staff (e.g. ordering goods should be kept separate from receipt of goods); similarly, authorisation and payment of invoices; and
- Avoiding undue reliance on any one individual.

***Supervision and checking of outputs**:* supervision is the function by which managers scrutinise the work and performance of their staff. It provides a check that staff are performing to meet standards and in accordance with instructions. It includes checks over the operation of controls by staff at lower levels. These act as both preventive and detective measures and involve monitoring the working methods and outputs of staff.

These controls are vital where staff are dealing with cash or accounting records. Random spot checks by managers can be an effective anti-fraud measure.

***Audit trail**:* this is largely a detective control, although its presence may have a deterrent effect and thus prevent a fraud. An audit trail enables all transactions to be traced through a system from start to finish. In addition to allowing detection of fraud it enables the controls to be reviewed.

***Monitoring**:* management information should include measures and indicators of performance in respect of efficiency, effectiveness, economy, and quality of service. Effective monitoring, including random checks, should deter and detect some types of fraudulent activity.

***Evaluation**:* policies and activities should be evaluated periodically for economy, efficiency, and effectiveness. The management of the operation may perform evaluations, but they are usually more effective when performed by an independent team. Such evaluations may reveal fraud.

***Staffing**:* adequate staffing is essential for a system to function effectively. Weaknesses in staffing can negate the effect of other controls. Posts involving control of particularly high

value assets or resources may need the application of additional vetting procedures. Rotation of staff between posts can help prevent or detect collusion or fraud.

***Asset accounting**:* asset registers used for management accounting purposes can help detect losses that may be caused by fraud.

***Budgetary and other financial controls**:* use of budgets and delegated limits for some categories of expenditure and other accounting controls should ensure that expenditure is properly approved and accounted for by the responsible manager. This should limit the scope for fraud and may result in some types of fraud being detected.

***Systems development**:* controls over the development of new systems and modifications to existing systems or procedures are essential to ensure that the effect of change is properly assessed at an early stage and before implementation. Fraud risks should be identified as part of this process and the necessary improvements in control introduced.

The “Fear Factor”
Major deterrents to perpetrating fraud are the risk of being caught and the severity of the consequences. The most important fact about deterrence is that it derives from *perceived* risk and not *actual* risk. Organisations may manage to increase the actual risk of detection, but it will only achieve a deterrent effect if it ensures that *perceptions* of risk change too.

Ways in which organisations can do this include:
- Warnings on forms such as: “false statements may lead to prosecution”;
- General publicity;
- Increasing the severity of penalties; and
- Always taking appropriate action against known perpetrators of fraud.

Changing Attitudes to Fraud
The most effective strategies designed to change attitudes rely on motivation rather than fear. They aim to persuade people of the undesirability of a particular behaviour. Attitude changing strategies rely to a large extent on publicity campaigns to achieve their effect, so it is important that departments carry out a full appraisal of the benefits of any proposed advertising campaign and to establish some way of measuring the outcomes of such campaigns. Organisations need to be clear about the objectives and targets of their campaigns.

Appendix 6: Guidance on Performing an Assessment of Fraud Risks

This appendix provides guidance on how to perform an assessment of fraud risks using the template provided. This appendix also provides detailed guidance from the Department of Finance of fraud proofing within policies, programmes, and systems.

1. General

Business Area:	[Insert name of business area]
Fraud Risk Assessment of:	[Insert a description of the area being assessed e.g. branch, process, type and value of transactions, nature of expenditure, any risks realised, any internal audit or external audit recommendations or concerns.
Assessment completed by:	[Insert name of officer completing the assessment]
Assessment reviewed and agreed by:	[Insert name of line manager reviewing and agreeing the assessment]
Assessment agreed on:	[Insert date assessment is agreed]
Next assessment due on:	[Insert date for completion of next fraud assessment]

1	**2**	**3**	**4**	**5**	**6**	**7**
FRAUD RISK	**IMPACT (H, M, L)**	**LIKELIHOOD (H, M, L)**	**KEY CONTROLS**	**RESIDUAL RISKS**	**PLANNED ACTION**	**ACTION TAKEN**

How to complete the assessment

1. Identify the key fraud risks facing your business and detail these in **Column 1**. Examples might be:
   - fraudulent subsidy/grant claims;
   - payment made on false documentation;
   - theft of assets;
   - misappropriation of cash;
   - false accounting;
   - contract fraud;
   - procurement fraud;
   - collusion;
   - computer fraud;
   - fraudulent encashment of payable instruments;
   - travel and subsistence fraud;
   - false claims for hours worked;
   - bribery.

2. Assess the impact of the identified fraud risk should it occur – High, Medium, or Low (**Column 2**). What damage could be done in relation to achievement of objectives, financial loss, reputation etc.?

3. Assess the likelihood of the identified fraud risk occurring – High, Medium, or Low (**Column 3**). High would be probable/likely, low would be improbable/unlikely.

4. Identify the key controls already in place to address each identified risk (**Column 4**).

Examples might be:
- segregation of duties;
- payment authorisation levels;
- payment/lodgement reconciliations;
- management checks and reviews;
- tendering process;
- transparent approval process;
- inter-system checks;
- physical controls such as safes, key safes etc.;
- logical access controls;
- physical access controls;
- asset register and inventory checks;
- audit logs;
- project monitoring;
- performance monitoring;
- independent/unannounced inspections;
- post-payment checks;
- training;
- manuals;
- staff rotation;
- irregularity recording, investigation, and reporting process etc.

5. Determine if any risk still exists after the application of the identified controls (**Column 5**). For example, the original risk detailed in Column 1 will probably still be a risk post-control although the effective application of the controls detailed in Column 4 will reduce the likelihood of occurrence.

6. Detail in **Column 6** what further action you are going to take to address the residual risk. It may be that control over the risk lies elsewhere and as a consequence you will have to accept the risk. If this is the case, justify why you are accepting the risk.

7. If you are planning further action to treat the risk, state what this is, who will be responsible for the action and when it is to be implemented.

8. **Column 7** will be used by you for internal reviews of the risk management framework.

2. Fraud Proofing Policies, Programmes and Systems (DoF Guidance)

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

Fraud Risk Assessment

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.

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.

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.

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.

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.

As part of the fraud risk assessment, organisations should consider all the different parties 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.

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
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.

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?

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.

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

Monitor and Review
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.

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
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.

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.

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

A basic checklist is also attached at which can be used by organisations when establishing or creating a new system, policy or 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.

Fraud Proofing Checklist

Questions	**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?	

Appendix 7: Contact Details

Contact	Position	Contact Details
Mr Ken Webb	Principal & Chief Executive Accounting Officer	kwebb@serc.ac.uk
Mr Tommy Martin	Deputy Chief Executive	tmartin@serc.ac.uk
Mrs Heather McKee	Deputy Principal Student Support Services	hmckee@serc.ac.uk
Mr Gary Ritchie	Deputy Principal Curriculum	gritchie@serc.ac.uk
Mrs Emma Carson	Head of Human Resources	ecarson@serc.ac.uk
RSM Northern Ireland (UK) Limited	Internal Auditors	028 90 234343