Special EU Programmes Body
Foras Um Chláir Speisialta An AE
Boord O Owre Ocht UE Projecks

STAFF NOTICE: (SEUPB) 05/11

(Last updated July 2017)

Contents **Page Number**

1. INTRODUCTION

1.1 There is a continuing need to raise staff awareness of their responsibility to safeguard public resources against the risk of fraud. The SEUPB requires all staff, at all times, to act honestly and with integrity, and to safeguard the public resources for which they are responsible. Fraud is an ever-present threat to these resources and must be a concern to all members of staff. The SEUPB has a zero tolerance to fraud and corruption. Our policy is to investigate all suspected frauds and allegations (anonymous or otherwise) and where appropriate, refer to the Police Service of Northern Ireland and/or An Garda Siochana and/or Police Scotland at the earliest juncture.

1.2 The purpose of the **Anti-fraud policy, SECTION A**, is to detail responsibilities regarding the prevention of fraud. **The SEUPB Fraud Response Plan**, **SECTION B,** details the procedures to be followed where a fraud is detected or suspected. Employees raising genuine concerns will be protected and their concerns looked into. SEUPB have in place avenues for reporting suspicions of fraud, without fear of prejudice or harassment, and these are detailed within **the SEUPB Whistle Blowing policy, SECTION C**.

2. DEFINITIONS

2.1 The term ‘fraud’ is used to describe such acts as deception, bribery, forgery, extortion, corruption, theft, conspiracy, embezzlement, misappropriation, false representation, concealment of material facts and collusion. However due to the existing over complicated array of deception offences the Fraud Act 2006 was established with a new general offence of Fraud. This Act supplements other legislation such as the Theft Act (NI) 1969 and the Theft (NI) Order 1978, which have traditionally been used to cover acts of fraud. In Ireland fraud is criminalised by the Criminal Justice (Theft and Fraud Offences) Act

2001 which creates the offences of theft and dishonesty. The Act also contains provisions on forgery and counterfeiting.

2.2 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 and dealt with as such.

2.3 The term 'Sponsor Departments; refers to the Department of Public Expenditure & Reform in Ireland and the Department of Finance in Northern Ireland.

SECTION A

3. ANTI-FRAUD POLICY

The Fraud Act 2006 became law in Northern Ireland in January 2007 (Criminal Justice (Theft and Fraud Offences) Act in Ireland in 2001). The Fraud Act states that a person is guilty of fraud if he is in breach of any of the following three areas:

- 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. A representation is false if it is untrue or misleading, and the person making it knows that it is, or might be, untrue or misleading;
- 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; and

- 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.

3.1 The Act also creates new offences to assist in the fight against fraud. These include an offence of possessing articles for use in fraud and an offence of making or supplying articles for use in fraud.

3.2 The Fraud Act requires that the person making the false representation, failing to disclose information or abusing their position must do so with the **intention** of making a gain or causing a loss or risk of loss to another. The gain or loss does not actually have to take place. Examples of frauds that may be perpetrated against the SEUPB include, but are not limited to:

- Theft, the misappropriation or misuse of assets for personal benefit;
- Bribery and corruption, offering, giving, soliciting or accepting an inducement or reward that may influence the actions taken by staff, for example, in the procurement of goods and services;
- False accounting and/or making fraudulent statements with a view to personal gain, for example falsely claiming overtime, travel and subsistence, sick leave or special leave (with or without pay);
- Dishonest use of a SEUPB credit card;
- Dishonest claims for reimbursement made by project promoters within the EU Programmes; or
- The dissemination of an email/correspondence to large groups of people falsely representing that the email/correspondence was sent by SEUPB;

4. SEUPB's RESPONSIBILITIES

4.1 The Chief Executive as Accounting Officer is responsible for developing and maintaining effective controls to prevent fraud and to ensure that if it does occur it will be detected without delay. The system of internal control is based

on an ongoing process designed to identify the principle risks, to evaluate the nature and extent of those risks, and to manage them effectively. This embraces all SEUPB activities and relationships and applies to fraud by the SEUPB's staff, members of the public and by contractors supplying goods/services to the SEUPB, or any other contractual or working relationships entered into by the SEUPB including EU Programme Promoters. Specific references are made in Agreements with third parties, the content of which is compatible with this policy.

4.2 The SEUPB must also investigate vigorously and promptly the circumstances in which fraud occurs. It must take the appropriate legal and/or disciplinary action in all cases where that would be justified; and make any necessary changes to systems and procedures to try to ensure that similar frauds will not happen again. Investigations must consider as a matter of course whether there has been a failure of supervision and, if appropriate disciplinary action will be taken (section 8 of this document refers).

4.3 Overall responsibility for managing the risk of fraud has been delegated to the Director of Corporate Services. Their responsibilities include:

- Developing a fraud risk profile and undertaking a regular review of the fraud risks associated with each of the key organisational objectives;

- Establishing an effective anti-fraud policy and fraud response plan, commensurate to the level of fraud risk identified in the fraud risk profile;

- Designing an effective control environment to prevent fraud commensurate with the fraud risk profile;

- Establishing appropriate mechanisms for:
    - Reporting fraud risk issues;
    - Reporting significant incidents of fraud to the Accounting Officer; and

    - Reporting to Department of Finance (DoF), Department of Public Expenditure and Reform (DPER), the Comptrollers and Auditors General, and all other relevant parties.

- Co-ordinating assurances about the effectiveness of anti-fraud policies to support the Statement on Internal Control;

- Liaising with the Audit and Risk Committee;

- 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;

- Ensuring fraud awareness training is provided as appropriate and, if necessary, more specific anti-fraud training and development is provided 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;

- Ensuring, where appropriate, disciplinary action against supervisors where supervisory failures have contributed to the commission of fraud;

- Ensuring, where appropriate, disciplinary action against staff who fail to report fraud;

- Taking appropriate action to recover assets and losses; and

- Ensuring that appropriate action is taken to minimise the risk of similar frauds occurring in future.

5 LINE MANAGERS' RESPONSIBILITIES

5.1 It is the responsibility of Senior Management (Chief Executive, Directors and Heads of Unit) to ensure that an adequate system of internal control exists and operates effectively. Line managers (i.e. staff at Clerical Supervisory level and above) are responsible for ensuring that the system of internal control within their areas of responsibility operates effectively. **The responsibility for the prevention and detection of fraud, therefore, rests primarily with managers.** There is a need for all managers to assess the types of risk involved in the operations for which they are responsible; to review and test regularly the control systems for which they are responsible ensuring that controls are being complied with; and to satisfy themselves that their systems continue to operate effectively.

5.2 A major element of good corporate governance is a sound assessment of the organisation's business risks. **Managers must ensure that**:

a) fraud risks have been identified within risk frameworks encompassing all operations 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

e) risks are reassessed as 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/Risk and Control Frameworks updated 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.

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

a) there is a regular rotation of staff, particularly in key posts;

b) there is a separation of duties so that control of a key function is not vested in one individual;

c) backlogs are not allowed to accumulate; and

d) in designing any new system, consideration is given to building in safeguards to prevent and/or detect internal and external fraud.

5.4 Senior Management (i.e. Director/Head of Unit level or above), as part of their overall responsibilities, are responsible for providing advice and assistance, where necessary, on risk and control issues. They, in turn, should utilise as appropriate, the services of professional Audit support or the advice of an appropriate source. As fraud prevention is the ultimate aim, anti-fraud measures should be considered and incorporated in every system and programme at design stage, for example the design of application forms.

5.5 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 the SEUPB promotes an anti-fraud culture is a fundamental element in arriving at an overall opinion.

5.6 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. Risk and Control Frameworks are 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.

6. STAFF RESPONSIBILITIES

6.1 The SEUPB's Code of Conduct sets out the duties and responsibilities of staff and states that "staff should endeavour to ensure the proper, economical, effective and efficient use of resources". Every member of staff has a duty to ensure that public funds are safeguarded, whether they are involved with cash or payments systems, receipts, assets, or dealings with contractors or suppliers.

6.2 Staff should alert their line manager or a more senior manager where they believe the opportunity for fraud exists because of poor procedures or lack of effective oversight.

6.3 Staff should be 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 I provides examples of Fraud Indicators). In addition, Common Methods and Types of Fraud are included in Appendix II, with Examples of Good Management Practices Which May Assist in Combating Fraud detailed in Appendix III.

6.4 In addition, it is the responsibility of every member of staff to report details immediately to their line manager or a more senior manager if they suspect that a fraud has been committed or see any suspicious acts or events. Staff must assist any investigations by making available all relevant information to the investigating officer(s) and by co-operating in interviews. Any information provided by staff will be treated confidentially. The Public Interest Disclosure (NI) Order 1998 (Whistle-blowing), the Employment Law Compliance Bill 2008 and the Prevention of Corruption (Amendment) Bill 2008 in Ireland protects the rights of staff who report wrongdoing (see Section C).

6.5 As stewards of public funds 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 that might be seen to compromise their integrity. There is further guidance on the acceptance of gifts and hospitality in the SEUPB Staff Guidance Note, or in DFP Finance Bulletin 02/10 (as amended 22 September 2010).

6.6 It is also essential that <u>all</u> staff understand and adhere to laid down systems and procedures including those of a personnel/management nature such as submission of expenses claims, records of absence, flexi and annual leave.

7. INVESTIGATION

7.1 Line managers should be alert to the possibility that unusual events or transactions could 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.

7.2 It is the SEUPB's policy that there will be consistent handling of all suspected fraud cases without regard to position held or length of service of the individual(s) involved.

7.3 The SEUPB has put in place a qualified investigations officer resource within the Managing Authority Directorate.

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

7.5 Irrespective of the source of suspicion, it is for the senior management in the office concerned (normally at Director/Head of Unit level), in conjunction with the MA investigations officer, to undertake an initial investigation to ascertain the facts. This investigation should be carried out as speedily as possible after suspicion has been aroused**: prompt action is essential.** The purpose of the initial investigation is to confirm or repudiate the suspicions that have arisen so that, if necessary, further investigation may be instigated. **However, as detailed in the Fraud Response Plan, It is imperative that such enquiries should not prejudice subsequent investigations or corrupt evidence, therefore, <u>IF IN DOUBT, ASK FOR ADVICE</u>.**

7.6 Once suspicion has been aroused that a fraud may have been perpetrated, management should follow the guidance provided in the attached Fraud Response Plan set out in **SECTION B**.

8. DISCIPLINARY ACTION

8.1 After a full investigation the SEUPB will take legal and/or disciplinary action in all cases where it is considered appropriate. Where supervisory negligence is found to be a contributory factor, disciplinary action may also be initiated against those managers/supervisors responsible. 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 the SEUPB on the grounds of gross misconduct.

8.2 The Director of Corporate Services may suspend or redeploy any officer involved, pending the outcome of an investigation. Suspension or redeployment itself does not imply guilt.

8.3 It is the SEUPB's 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 Service of Northern Ireland and/or An Garda Siochana and/or Police Scotland as appropriate at the earliest possible juncture.

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

9. CONCLUSION

9.1 It is appreciated that the circumstances of individual frauds will vary but it is important that all are vigorously and promptly investigated and that appropriate remedial action is taken. Management should be conscious of

their responsibility to protect public funds and as such, should always be alert to the potential for fraud.

9.2 The SEUPB's Internal Audit Service will be available to offer advice and assistance on risk management/internal control issues.

9.3 Any queries in connection with this guidance should be directed to the Director of Corporate Services.

Gina McIntyre
Chief Executive

SECTION B

FRAUD RESPONSE PLAN

1 Introduction

The SEUPB has prepared this fraud response plan to act as a guide and provide a checklist of action that must be followed in the event of a fraud, or attempted fraud, being suspected.

The objective of the plan is to 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 of any disciplinary/legal action.

2 Initial Investigation

It is for the Director concerned and the investigations officer to undertake an initial investigation to ascertain the facts. This discreet investigation must be carried out and documented as quickly as possible and certainly within 24 hours of the suspicion being raised.

The Director concerned and investigations officer should contact the Director of Corporate Services who will be able to provide advice and support on the conduct of the investigation. The Director of Corporate Services may wish to seek advice and support from the Head of Internal audit. A flowchart is attached at Appendix IV outlining the required steps for reporting a fraud.

2.1 The Director of Corporate Services will inform the Chief Executive that an attempted or suspected fraud has been discovered (irrespective of the amount involved) and that an investigation is underway. The CEO should subsequently be kept fully informed of any developments.

2.2 The factors which give rise to the suspicion should be determined and examined to clarify whether a genuine mistake has been made or an irregularity has occurred. An irregularity may be defined as any incident or action which is not part of the normal operation of the system or the expected

course of events. An initial investigation may involve discreet enquiries with staff or the examination of documents.

2.3 If the initial investigation confirms the suspicion that a fraud has been perpetrated (or attempted), management must ensure that all original documentation and IT equipment 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.

2.4 **EU PROGRAMME FRAUD** - Where the irregularity involves co-financed expenditure from the European Union then these irregularities or suspected irregularities should be reported as set out in Regulations (EC) No 1303/2013, 1970/2015 and 1974/2015. In such cases the Body should adhere to SEUPB Designation Procedure 11: Procedure on the Treatment of Irregularities.

2.5 If further investigation is required in either Internal or EU Programme related instances, Internal and/or External Auditors may be appointed to conduct an investigation or provide advice.

3 Action Required for Internal Fraud

The facts should be reported immediately to the Director of Corporate Services, such notification to be followed up in writing. The Director of Corporate Services will inform the SEUPB's Internal Audit Service, the Corporate Accountant, and Chief Executive.

3.1 Senior Management within the SEUPB will decide on the appropriate course of action including the full investigation arrangements. The latter should be conducted by at least two senior officers, preferably one of whom is trained in investigative techniques i.e. PACE - Police and Criminal Evidence Act (NI Order), and independent of the area under scrutiny. 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.

3.2 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.**

3.3 If the preliminary enquiry confirms that a fraud has not been attempted nor perpetrated, however, internal controls are deficient, then management should review their control systems with a view to ensuring they are adequate and effective. The relevant Risk Register should be updated and, where appropriate, Internal Audit is available to offer advice and assistance on matters relating to internal control, if required.

FORMAL INTERNAL NOTIFICATION PROCEDURE

3.4 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 may require engagement with an external forensic expert in instances where digital/electronic data may need to be recovered. The purpose of 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 Director of Corporate services, who will report to the Chief Executive.

NOTIFICATION RESPONSIBILITIES OF SEUPB

3.5 The Chief Executive will immediately write to:

- Accounting Officers of the Sponsor Departments
- Head of Internal Audit (Department of Finance)
- NI Audit Office and the Comptrollers and Auditors General, in Northern Ireland and Ireland
- Audit & Risk Committee Members

4 EU PROGRAMME FRAUD INCLUDING ACTION REQUIRED FOR FRAUD WITHIN EXTERNAL BODIES

Formal Programme Rules have been issued to all Lead Partners for the EU Programmes 2014-2020 to guide Lead Partners on the steps to take upon discovering a suspected fraud or other irregularity. These Programme Rules detail what actions should be taken by the Lead Partner and when/how to inform the SEUPB. The most up to date version of these Programme Rules are available on the SEUPB website.

4.1 Where the suspected fraud is in connection with programme expenditure or technical assistance funds, the Chief Executive will notify the Accounting Officers of the relevant accountable Departments, as agreed in the Service Level Agreements, and copy this notification to the Head of Internal Audit for the Department of Finance. The Chief Executive will provide details of the fraud (or attempted fraud), along with results of the initial and subsequent investigation and any initial action taken. The SEUPB will ensure all paperwork is safeguarded for the Sponsor Departments inspection. The SEUPB will also copy any notification to the NI Audit Office and the Comptrollers and Auditors General, in Northern Ireland and Ireland. The SEUPB will also report to the Audit & Risk Committee on those suspected fraud cases being progressed.

4.2 The Chief Executive will seek Audit advice and assistance, from the Departments and externally if required. Advice sought will be on control issues, identifying what further enquiries need be made and on any action which may be necessary to prevent further loss. Following consultation with the Finance Departments and the relevant Audit Bodies, the SEUPB will contact the Police Service of Northern Ireland and/or An Garda Siochana and/or Police Scotland, as appropriate.

4.3 The SEUPB will co-operate fully with police enquiries. Following a police investigation the offender(s) may be prosecuted. In the event of the Police Service of Northern Ireland and/or An Garda Siochana and/or Police Scotland requesting the SEUPB's advice on prosecution, the request should be passed to the Chief Executive in the first instance who will seek the advice of the

relevant Audit Bodies and the Sponsor Departments. In such circumstances the SEUPB will seek appropriate legal advice as to the extent of any notification pending legal or other procedures that may remain extant.

4.4 Where a fraud is suspected involving an external organisation or individual, it is the Chief Executive's responsibility, with the assistance of the SEUPB investigations officer, to determine if there is sufficient evidence to notify the Police Service of Northern Ireland and/or An Garda Siochana and/or Police Scotland.

4.5 In such circumstances, investigation and reporting arrangements as documented above will apply and appropriate legal advice will be sought as to the extent of any notification pending legal or other procedures that may remain extant.

5 Post Event Action

When all the necessary investigations have been completed the results will be reported to the Director of the office concerned, the Director of Corporate Services, the Corporate Accountant, the Chief Executive and the Finance Departments (as outlined in 3.5). The Managing Authority and the Controller should be kept informed throughout the process.

5.1 The investigations may have revealed a failure of supervision, and/or a breakdown in or an absence of control. Where a fraud has occurred, management must make any necessary changes to systems and procedures to ensure that similar frauds will not recur. Audit Services will be utilised, as appropriate, to investigate the area where the fraud occurred to provide assurance that systems and procedures have been improved and are operating effectively. Internal Audit would be available to offer advice and assistance on matters relating to internal control, if considered appropriate.

6 Reporting Arrangements

The SEUPB will be required to ensure the following reporting arrangements are applied in all cases:

- The Audit & Risk Committee should be kept informed of developments during the investigation;
- The SEUPB provide an annual return of frauds for the Sponsor Departments, by end of May each year;
- The SEUPB Fraud response plan should be reviewed to determine if updates/changes are required; and
- A lessons learnt document should be circulated within the SEUPB if appropriate.

7 Conclusion

Any queries in connection with this response plan should be made to the Director of Corporate Services. Current contact details for the appropriate officers are provided in Appendix V.

SECTION C

SPECIAL EU PROGRAMMES BODY POLICY FOR REPORTING SERIOUS CONCERNS AT WORK (WHISTLE BLOWING POLICY)

1. Introduction

This Policy for Reporting Serious Concerns at Work takes account of the Public Interest Disclosure (Northern Ireland) Order 1998 (Employment Law Compliance Bill 2008 and the Prevention of Corruption (Amendment) Bill 2008 in Ireland) and provides a procedure which enables employees to raise concerns about what is happening at work, particularly where those concerns relate to unlawful conduct, financial malpractice or dangers to the public or the environment. The object of this policy is to ensure that concerns are raised and dealt with at an early stage and in an appropriate manner. The SEUPB is committed to its Policy for Reporting Serious Concerns at Work. If an employee raises a genuine concern under this policy, he or she will not be at risk of losing their job, nor will they suffer any form of detriment as a result. As long as the employee is acting in good faith and in accordance with this policy, it does not matter if they are mistaken.

2. How the Policy for Reporting Serious Concerns at Work Differs from the Grievance Procedure

This policy does not apply to raising grievances about an employee's personal situation. These types of concern are covered by the SEUPB's grievance procedure. The Policy for Reporting Serious Concerns at Work is primarily concerned with where the interests of others or of the SEUPB itself are at risk. It may be difficult to decide whether a particular concern should be raised under the Policy for Reporting Serious Concerns at Work, under the grievance procedure, or under both. If an employee has any doubt as to the correct route to follow, the SEUPB encourages the concern to be raised under this policy and will decide how the concern should be dealt with.

3. How to Raise a Concern Internally

Step 1

If an employee has a concern about malpractice, he or she should consider raising it initially with their line manager. This may be done orally or in writing. An employee should specify from the outset if they wish the matter to be treated in confidence so that appropriate arrangements can be made.

Step 2

If an employee feels that they are unable to raise a particular matter with their line manager, for whatever reason, they should raise the matter with their Director or the HR Manager.

Step 3

If these channels have been followed and the employee still has concerns, or if the employee feels that the matter is so serious that they cannot discuss it with any of the above, they should discuss it with the Director of Corporate Services.

Step 4

If the employee has exhausted the above steps, they may contact the Chair of the Audit & Risk Committee (contact details at section 10).

4. When are Disclosures Protected?

The Order does not introduce a general protection for a worker who reports a wrongdoing in all circumstances. A disclosure will qualify for protection if, in the reasonable belief of the worker making it, it tends to show that one or more of the following has occurred, is occurring or is likely to occur:

a. a criminal offence;
b. a failure to comply with a legal obligation;

c. a miscarriage of justice;
d. the endangering of an individual's health and safety;
e. damage to the environment; or
f. deliberate concealment of information tending to show any of the above.

5. What Protection Does the Order Give?

5.1 A qualifying disclosure will be protected under the Order if it is made:

a. in good faith to the SEUPB (either directly or through internal procedures authorised by SEUPB), or to another person whom the worker reasonably believes is solely or mainly responsible for the failure in question;
b. to a legal adviser in the course of obtaining legal advice;
c. in good faith to a Government Minister by a worker employed in a Government-appointed organisation such as a non-departmental public body; or
d. to a person or body prescribed in Statutory Rule 1999 No. 401 ("a prescribed person"), e.g. the Health and Safety Executive for Northern Ireland.

In the last case the worker must make the disclosure in good faith, reasonably believe that the information and any allegation in it are substantially true, and reasonably believe that the matter falls within the description of matters for which the person has been prescribed.

5.2. Qualifying disclosures will also be protected if they are made other than described in paragraph 4.1, provided that the worker makes the disclosure in good faith, reasonably believes that the information and any allegation contained in it are substantially true, and does not act for personal gain. One or more of the following conditions must also apply:

a. the worker reasonably believed that he or she would be victimised if he or she had made the disclosure to the employer or to a prescribed person;
b. there was no prescribed person and the worker reasonably believed that disclosure to the employer would result in the destruction or concealment of evidence; or

c. the worker had already disclosed substantially the same information to the employer or a prescribed person.

It must also be reasonable for the worker to make the disclosure. In deciding the reasonableness of the disclosure, an industrial tribunal will consider all the circumstances. This will include the identity of the person to whom the disclosure was made, the seriousness of the concern, whether the failure is continuing or likely to occur, whether the disclosure breached a duty of confidentiality which the employer owed to a third party, what action has been taken or might reasonably be expected to have been taken if the disclosure was previously made to the employer or a prescribed person, and whether the worker complied with any approved internal procedures if the disclosure was previously made to the employer.

6. Protecting the Employee

The SEUPB will not tolerate harassment or victimisation of anyone raising a genuine concern under the Policy for Reporting Serious Concerns at Work. If an employee requests that their identity be protected, all possible steps will be taken to prevent the employee's identity becoming known. If the situation arises where it is not possible to resolve the concern without revealing the employee's identity (e.g. if the employee's evidence is needed in court), the best way to proceed with the matter will be discussed with the employee. Employees should be aware that by reporting matters anonymously, it will be more difficult for the organisation to investigate them, to protect the employee and to give the employee feedback. Accordingly, while the Office will consider anonymous reports, this policy does not cover matters raised anonymously. It should be noted that there is no automatic right to anonymity guaranteed under this policy.

7. How the Matter Will Be Handled?

Once an employee has informed the SEUPB of his or her concern, the concerns will be examined and the SEUPB will assess what action should be

taken. This may involve an internal enquiry or a more formal investigation. The employee will be told who is handling the matter, how they can contact him/her and whether any further assistance may be needed. If the employee has any personal interest in the matter, this should be declared by the employee at the outset. If the employee's concern falls more properly within the grievance procedure, then they will be told this.

8. Independent Advice

If an employee is unsure whether to use this procedure or wants independent advice at any stage, they may contact the independent charity Public Concern at Work on 020 7404 6609 or email helpline@pcaw.co.uk. Their lawyers can give free confidential advice at any stage about how to raise 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.

9. Who is this policy for?

This policy is for employees of the SEUPB, and, for the purpose of this policy only, will include temporary staff, independent consultants and contractors and suppliers of services to the SEUPB. The policy also applies to the general public who wish to report a reasonable suspicion of malpractice within an EU funded project relative to the SEUPB.

10. Audit Committee

The SEUPB has an Audit Committee and has appointed internal auditors. Staff may contact members of the Audit Committee or the internal auditors to raise concerns. The appropriate contact points are:

Name:	*Designation / Located at:*	*Telephone No.:*
Mr Brendan Mullan	Chairman, Audit & Risk Committee	028 9083 2311
Mr Joe Campbell	Independent member of Audit & Risk Committee	07713 068543
Corporate Services Director	Special EU Programmes Body attendee of Audit Committee	028 9026 6660
Mr. Brian O'Neill	Northern Ireland Audit Office, attendee of Audit Committee	028 9025 4323
Mr Michael Matthews	Head of Internal Audit, attendee of Audit Committee	028 9037 8603

11. External Contacts

It is intended that this policy should give employees the reassurance they need to raise concerns internally. However, the SEUPB recognises that there may be circumstances where employees should properly report matters to outside bodies, such as regulators or the police. If an employee is unsure as to whether this is appropriate and does not feel able to discuss the matter internally, Public Concern at Work will be able to give advice on such an option and on the circumstances in which an employee should contact an outside body rather than raise the matter internally.

12. Matters Raised Maliciously

Employees who maliciously raise a matter that they know to be untrue will be subject to the disciplinary policy.

13. Guiding Principles

To ensure this policy is adhered to, the SEUPB will:

- Not allow the person raising the concern to be victimised for doing so;
- Treat victimisation of whistle blowers as a serious matter, that may lead to disciplinary action that may include dismissal;
- Not attempt to conceal evidence of poor or unacceptable practice;
- Take disciplinary action if an employee destroys or conceals evidence of poor or unacceptable practice or misconduct; and

  Ensure confidentiality clauses within employment contracts do not restrict, forbid or penalise whistle blowing.

14. Contacts

To make a disclosure to the SEUPB write to:

Paul Sheridan
Director of Corporate Services
The Special EU Programmes Body
The Clarence West Building
2 Clarence Street West
Belfast
BT2 7GP

Or telephone 02890 266660

APPENDIX I

INDICATORS OF FRAUD

THESE INCLUDE, BUT ARE NOT LIMITED TO:

- 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
- Covering up inefficiencies
- 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 unexplained movement of cash funds
- Unauthorised changes to systems or work practices
- Employees with outside business interests or other jobs
- Excessive overtime
- Large backlogs in high risk areas
- Lost assets
- Absence of controls and audit trails
- Lack of thorough investigations of alleged wrongdoing
- Pecuniary gain to organisation – but no personal gain
- 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
- Lowest tenders or quotes passed over with scant explanations recorded
- Managers bypassing subordinates
- Subordinates bypassing managers
- Large sums held in petty cash
- Lack of clear financial delegations
- Secretiveness
- Marked character changes
- Excessive ambition
- Apparent lack of ambition
- 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

APPENDIX II

COMMON METHODS AND TYPES OF FRAUD

THESE INCLUDE, BUT ARE NOT LIMITED TO:

- 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
- 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 with inappropriate authorisation documentation
- 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

APPENDIX III

EXAMPLES OF GOOD MANAGEMENT PRACTICES WHICH MAY ASSIST IN COMBATING FRAUD

THESE INCLUDE, BUT ARE NOT LIMITED TO:

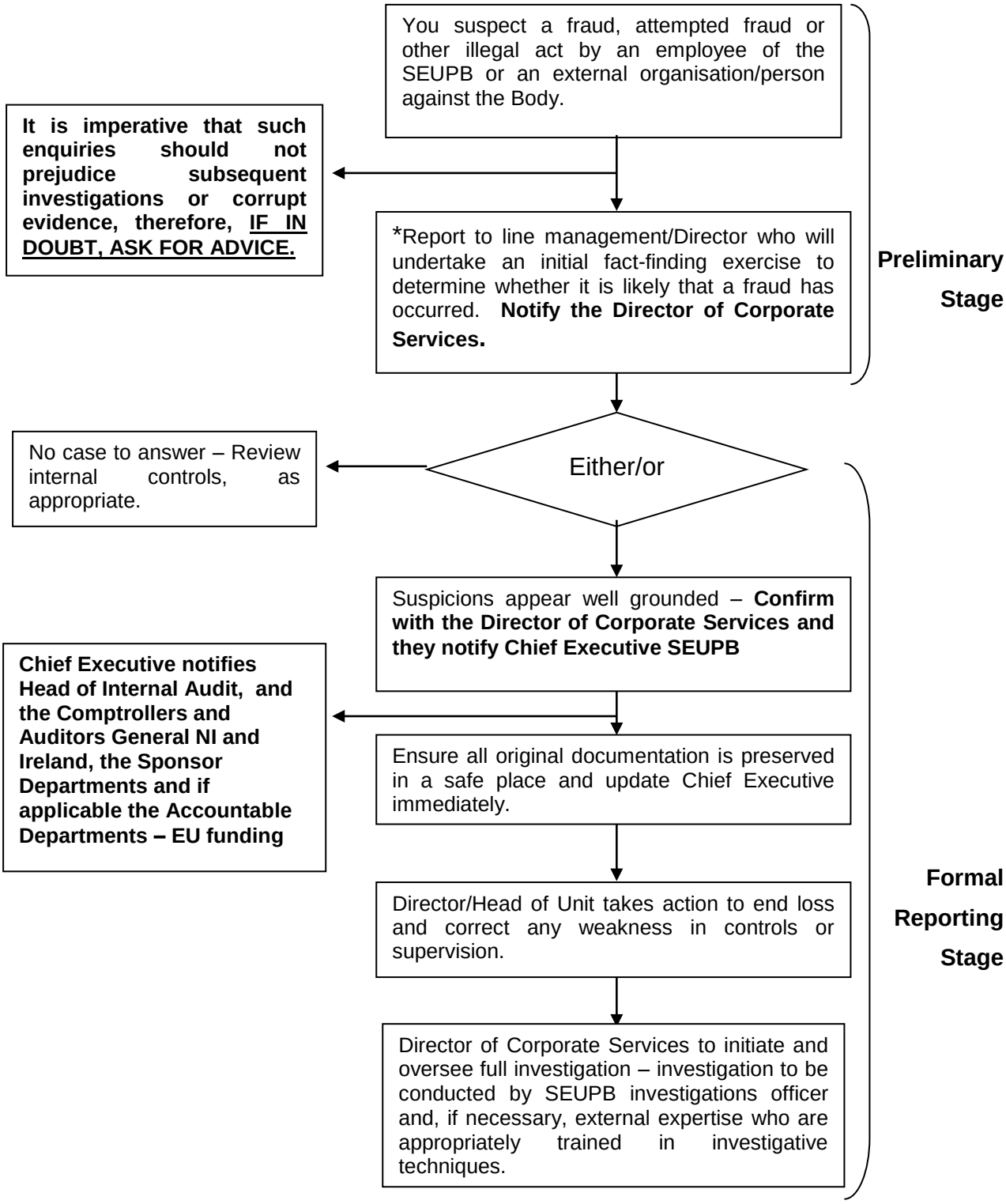
- All income is promptly entered in the accounting records with the immediate endorsement of all cheques
- Regulations governing contracts and the supply of goods and services are properly enforced
- Accounting records provide a reliable basis for the preparation of financial statements
- Controls operate 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 studs in numerical order

EXAMPLES OF GOOD MANAGEMENT PRACTICES WHICH MAY ASSIST IN COMBATING FRAUD (CONTINUED)

- 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 (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

APPENDIX IV

Reporting Fraud/Suspected Fraud



* If you are concerned that line management may be involved in the suspected fraud, you should report it to the next appropriate level, i.e. Head of Unit, Director, CEO. Alternatively, at any stage in the process, you can contact the CEO, Head of Internal Audit for advice.

APPENDIX V

Contact details for relevant officers

Name	Designation	Telephone Number
Ms Gina McIntyre	Chief Executive, SEUPB	02890 266663
Paul Sheridan	Director of Corporate Services, SEUPB	02890 266660
Mr Michael Matthews	Head of Internal Audit	02890 378603 (x88603)

ANNEX 1

Definitions for the Identifying and Reporting Irregularities, per Regulations (EC) No: 1299/2013, 1303/2013, 1970/2015 and 1974/2015.

"Irregularity": Article 2(36) of Regulation (EC) No 1303/2013 defines an 'irregularity' as "any breach of Union law, or of national law relating to its application, resulting from an act or omission by an economic operator involved in the implementation of the ESI Funds, which has, or would have, the effect of prejudicing the budget of the Union by charging an unjustified item of expenditure to the budget of the Union.

"Suspected Fraud": An irregularity that gives rise to the initiation of administrative or judicial proceedings at national level in order to establish the presence of intentional behaviour, in particular fraud, as referred to in Article 1(1)(a), of the Convention on the protection of the European Communities' financial interests. Fraud can only be classed as suspected fraud at the outset of an enquiry. Cases should be indicated as suspected fraud if the details suggest intent to deceive or misappropriate funds. Poor management, financial control or record keeping is not suspected fraud.

"Fraud": The term 'Fraud' is used to describe such acts as deception, bribery, forgery, extortion, corruption, theft, conspiracy, embezzlement, misappropriation, false representation, concealment of material facts and collusion. However due to the existing over complicated array of deception offences, the Fraud Act 2006 was established, creating a new general offence of fraud which can be committed in three defined ways – by false representation; by failure to disclose information; and by abuse of power. This Act supplements other legislation such as the Theft Act (NI) 1969 and the Theft (NI) Order 1978, which have traditionally been used to cover acts of fraud. The Act also contains provisions on forgery and counterfeiting. In Ireland fraud is criminalised by the Criminal Justice (Theft and Fraud Offences) Act 2001 which creates the offences of theft and dishonesty.

"Bankruptcy" means:

- winding up by or subject to the supervision of the Court;
- creditors' voluntary winding up (with confirmation by the Court);
- administration;
- voluntary arrangements under insolvency legislation; and
- bankruptcy or sequestration.

“Economic operator” means any natural or legal person or other entity taking part in the administration of assistance from the Funds, with the exception of Member States exercising their prerogatives as a public authority.

“Primary administrative or judicial findings” means a first written assessment by a competent authority, either administrative or judicial, concluding on the basis of specific facts that an irregularity has been committed, without prejudice to the possibility that this conclusion may subsequently have to be revised or withdrawn as a result of developments in the course of the administrative or judicial procedure.

ANNEX 2

Common Types of Irregularity (this list is not exhaustive)

Ineligible costs:

- Use of ineligible costs to obtain grant.
- Non-compliance with procurement guidance.
- Inflated project costs.
- Activities already funded from other sources.
- Charging costs to a project already used in another Structural Funds project.
- Claiming for work done before the Letter of Offer start date.
- Fees, overhead costs not allowed under the regulations.
- Incorrectly calculated overheads/staff salaries.

False claim/false supporting documents – suspected fraud.

Inadequate supporting documentation:

- Lack of documents to support expenditure.
- Lack of documents to support progress against targets and objectives.
- No invoice or only a copy invoice.
- No timesheets.
- Incomplete timesheets.
- Insufficient tenders or quotes.
- Incomplete assessment of tenders / quotes.
- Assessment of quotes not in line with terms of reference.
- No independent evidence of exchange rates.
- No evidence of compliance with publicity.

Incorrectly completed supporting documents – often down to poor management skills.

Misleading description of project – project not proceeding as in the Letter of Offer.

Non-existing or incorrect match funding.

Administrative errors:

- Incorrectly completed claim form.
- Database inputting errors.

- Failure to maintain records – lack of clear audit trail.
- Awarding contracts/committing funds after programme closure date.

Breach of Terms and Conditions of Letter of Offer:

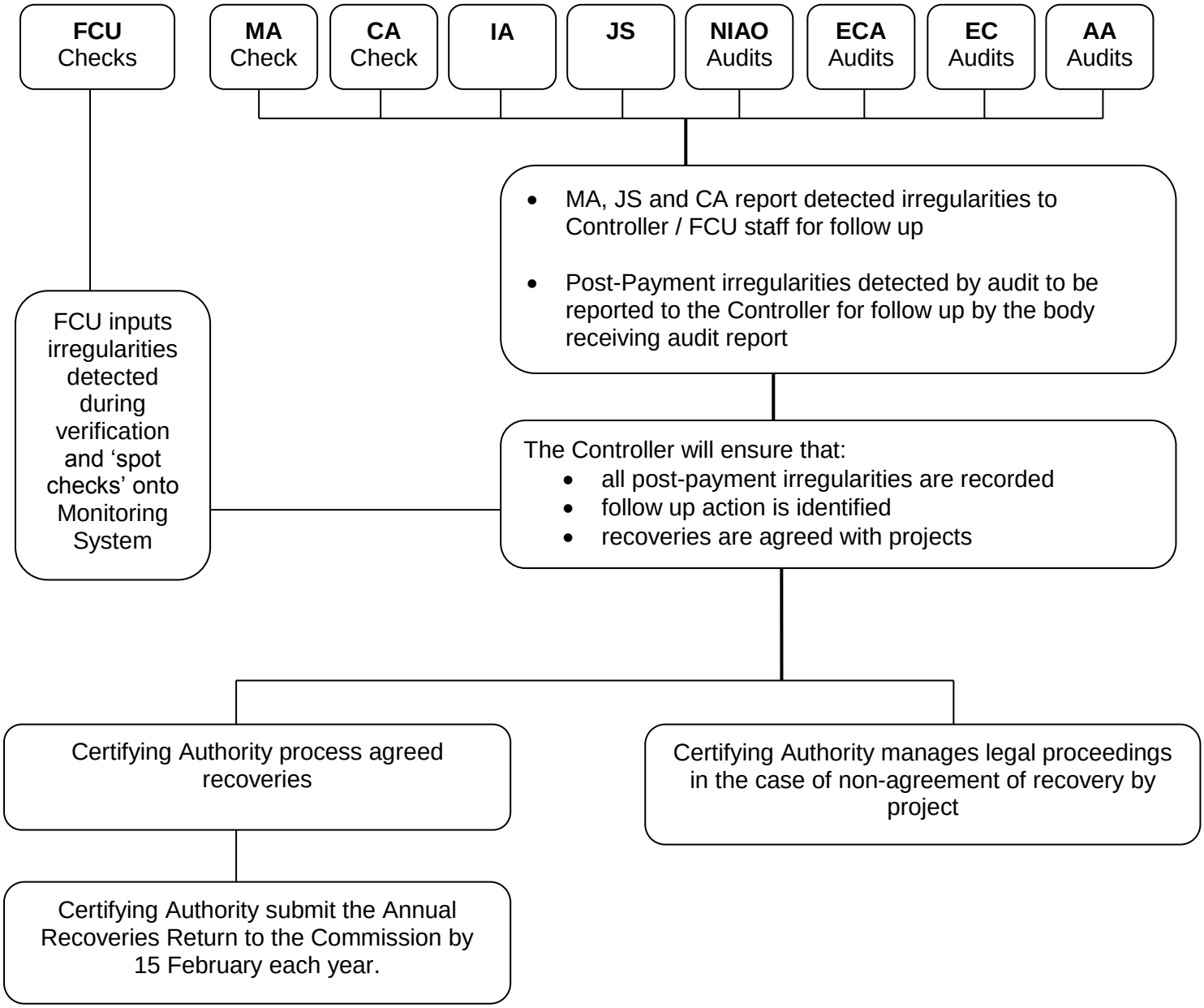
- Failure to respect deadlines.
- Claiming for expenditure not defrayed.
- Failure to retain relevant / adequate supporting documentation.
- No evidence of compliance with publicity.
- Unapproved budget variances.
- Failure to achieve targets and objectives.

Annex 3

Irregularities Process: Flowchart of responsibilities

Post-payment Irregularities

Bodies Detecting Irregularities



Bodies Detecting Irregularities:

FCU – Financial Control Unit **MA** – Managing Authority
CA – Certifying Authority **IA** – Internal Audit
JS – Joint Secretariat
NIAO – Northern Ireland Audit Office **ECA** – European Court of Auditors
EC – European Commission Audit **AA** – Audit Authority