

Counter Fraud Guide

April 2022

Foreword

We all face difficult challenges and growing resource pressures in our day-to-day work. As civil servants we must ensure the economic, efficient and effective use of public resources in everything that we do.

It is essential to have a proactive approach to countering fraud, bribery and corruption, to ensure that public funds are safeguarded and we are protecting frontline services as a result.

The main purpose of this guide is to:

* ensure there is a greater level of awareness of the risk of fraud no matter what role you undertake,
* ensure we all understand our responsibilities and the procedures for dealing with and reporting an incident should it occur in our own areas, or the organisations we work with,
* foster a culture where we are able to prevent such incidents from occurring.

This guide outlines the approach for the prevention, detection, reporting and handling of fraud, bribery and corruption. The documentation is designed to be accessible to all Food Standards Scotland (FSS) staff.

Contents

[**Protecting Public Resources - Strategy** 3](#_Toc166576756)

[**What is Fraud?** 5](#_Toc166576757)

[**Types of Fraud** 6](#_Toc166576758)

[**The Signs of Fraud** 7](#_Toc166576759)

[**Fraud Prevention** 8](#_Toc166576760)

[**Responding to Fraud** 10](#_Toc166576761)

[**Roles and Responsibilities** 11](#_Toc166576762)

[**Fraud Investigations - Fraud Response Plan** 14](#_Toc166576763)

[**Conclusion** 19](#_Toc166576764)

# **Protecting Public Resources - Strategy**

Food Standards Scotland (FSS) ambition is to improve the approach to counter fraud across the organisation to safeguard services and improve performance: working together across the organisation to protect public resources from the risk and impact of fraud, bribery and corruption.

Countering fraud, bribery and corruption is an individual responsibility, with corporate support and training provided. It is every employee’s responsibility to be alert to and prevent fraudulent activity being perpetrated against FSS.

FSS has five strategic objectives to deter, disable, prevent, detect and deal with fraud, bribery and corruption:

Awareness: We will deter fraud, bribery and corruption by raising awareness of the risk and impact of fraud, bribery and corruption with FSS staff, and our stakeholders.

Prevention: We will disable fraud, bribery and corruption through improving our systems and controls and being proactive in analysing data to identify areas at risk to reduce the opportunity and ease of fraudulent activity.

Teamwork: We will prevent fraud, bribery and corruption by working together across FSS and the public sector to share information and develop collaborative approaches.

Investigation: We will detect fraud, bribery and corruption by investigating allegations quickly, impartially and professionally and by maintaining a whistle blowing procedure that is seen to be independent and protective of those reporting potential fraud.

Enforcement: We will deal with fraud, bribery and corruption by enforcing the policy on fraud through disciplinary action and prosecution where appropriate.

Zero Tolerance Approach

Our approach to countering fraud, bribery and corruption is one of zero tolerance.

There is a role for all members of staff in establishing an effective counter fraud culture by engaging and being alert to the risk of external and internal fraud; identifying suspicious activities and control weaknesses; and reporting any suspicions quickly and appropriately.

This can be achieve and effectively managed at all levels of public service delivery as follows:

* Promoting clear ethical standards through this counter fraud guide.
* Communicating our commitment to deter fraud, bribery and corruption by raising awareness of this counter fraud guide to all staff.
* Supporting all staff and stakeholders in their responsibilities in preventing and detecting fraud, bribery and corruption through guidance and training.
* Providing managers with specialist support in designing, operating and reviewing internal controls.
* Maintaining comprehensive procedures for disabling and detecting fraud that must be carefully followed and monitored.
* Protecting members of staff through a robust process for reporting suspicions of fraud, bribery and corruption.
* Effectively dealing with fraud by implementing a comprehensive fraud response plan, including professional investigation by skilled staff.
* Using data, and technology, efficiently in the systems in place to combat fraud.
* Sharing knowledge of vulnerabilities and lessons learned through strong communication channels.

# **What is Fraud?**

Fraud is wrongful or criminal deception intended to result in financial or personal gain.

Fraud is committed when someone achieves a practical result by the means of a false pretence.

This can sometimes be where someone is caused to do something they would not otherwise have done by use of deception.

All FSS staff are required at all times to act honestly and with integrity and to safeguard the public resources for which they are responsible, line with the [Civil Service Code.](https://www.gov.uk/government/publications/civil-service-code/the-civil-service-code) FSS will not accept any level of fraud or corruption; consequently, any case will be thoroughly investigated and dealt with appropriately.

Fraud can be used to describe a wide variety of dishonest behaviour such as forgery, false representation and the concealment of material facts. The fraudulent use of IT resources is included in this definition, where its use is a material factor in carrying out a fraud.

Bribery

A bribe is an offer or promise of a financial or other advantage, designed to induce another person to perform improperly in their position of trust and responsibility. The [UK Bribery Act 2010](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/832011/bribery-act-2010-guidance.pdf) is a UK-wide legislation that:

* makes it a criminal offence to give, promise or offer a bribe and to request, agree to receive or accept a bribe either at home or abroad.
* increases the maximum penalty for bribery from seven to 10 years imprisonment, with an unlimited fine.
* introduces a corporate offence of failure to prevent bribery by persons working
* on behalf of a business.

# 

# **Types of Fraud**

There are many different types of fraud which we could experience which can take place within and out with the workplace. In this guide we have detailed only some of the possible types of fraud, for a fuller list of possible types of fraud take a look at [Action Fraud's A-Z of Fraud](https://www.actionfraud.police.uk/a-z-of-fraud-category).

Phishing can involve sending attachments/website links which can infect computers or mobile devices. Either emails, letters, instant messages or text messages. Very often these appear to be authentic communications from legitimate organisations.

Embedded links within the message can direct you to a hoax website where your login or personal details may be requested.

Vishing is when fraudsters obtain personal details of a victim by phone.

Malware is software that’s been made by someone so that your computer, laptop, tablet or mobile phone doesn’t work as it’s supposed to. In some cases it also collects information or data saved on your device, and passes it on. It’s also known as ransomware, viruses, worms, Trojan horses, spyware, adware, scareware and crime ware.

Social engineering in the context of fraud is the psychological manipulation of people into performing actions or divulging confidential information.

One of the greatest risks of fraud within FSS is **Payment fraud**, which is any fraud that involves falsely creating or diverting payments. Payment fraud can include:

* creating bogus customer records and bank accounts so that false payments can be generated
* intercepting and altering payee details and amounts on cheques then attempting to cash them
* creating false payment and financial information to support fraudulent claims for benefits
* processing false claims by accomplices for benefits, grants or repayments
* self-authorising payments to oneself.

# **The Signs of Fraud**

Behavioural danger signs of internal fraud could include:

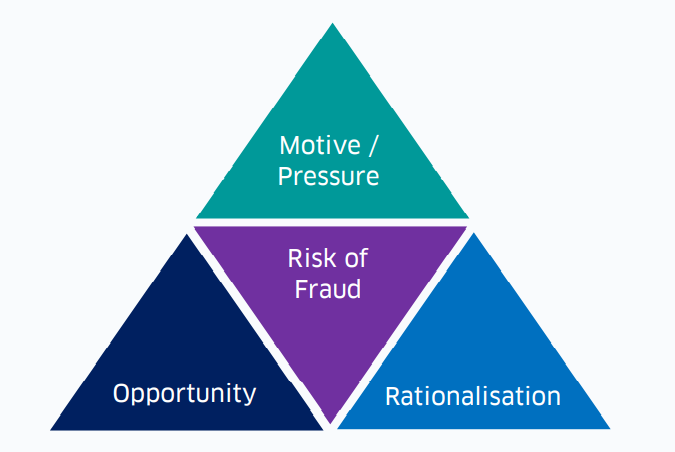
* Evidence of excessive spending by staff,
* Inappropriate relationships with suppliers
* Reluctance of staff to take leave
* Undue possessiveness of or anomalies between work records
* Pressure from colleagues to avoid normal control procedures
* Abnormal Travel and Subsistence claims, overtime or Flexible Working Hours patterns.

Managers and staff must always be alert to the risk of fraud, bribery and corruption. Danger signs of external fraud include:

* Photocopies of documents when originals would be expected
* Discrepancies in information e.g. signatures and dates
* Unexpected queries from stakeholders or suppliers e.g. bank account detail changes
* Requests for non-standard types of payment
* Unexpected trends or results e.g. from reconciliations.

External and internal fraud is not always easy to identify. Often suspicion may be raised but it is not acted on and reported. Fraud is often committed where there is:

* Opportunity to commit fraud. This is where internal controls are weak and access to assets and information allows fraud to occur.
* Rationalisation that justifies fraudulent behaviour. This can be for a variety of reasons.
* Motivation or a need for committing fraud. This can be for financial reasons or other motivating factors.



# **Fraud Prevention**

Reducing the Opportunity for Fraud - Separation of Duties

The opportunity for fraud must be reduced wherever possible. Allocating responsibility for too many functions to one person can constitute a high risk of fraud and should be avoided. The risk of fraud can be reduced by ensuring proper separation of duties so that, for example, more than one person has to be involved in ordering, receiving and authorising payments for goods or services.

*The separation of key functions forms an integral part of systems control and is essential to minimise the potential scope for irregularity by staff acting on their own. The need for proper separation of duties applies as much to grant systems as it does to procurement procedures.*

Without adequate separation of duties, the effectiveness of other control measures is undermined. Where resources are limited and separation of duties is not possible, alternative management controls – such as supervisory checking - must be employed.

Robust Systems of Control

Appropriate preventive and detective controls should be put in place to counter the risk of fraud. Procedures set up to prevent and detect fraud must be proportional to the risk involved and be carefully followed and monitored. Additional information is provided in the Scottish Public Finance Manual (SPFM) sections on [Checking Financial Transactions](https://www.gov.scot/publications/scottish-public-finance-manual/checking-financial-transactions/checking-financial-transactions/) and on [Risk Management](https://www.gov.scot/publications/scottish-public-finance-manual/risk-management/risk-management/).

Preventive controls are designed to limit the possibility of a fraud occurring e.g. separation of duties. Detective controls are designed to spot errors, omissions and fraud after the event e.g. supervisory checks and reconciliations. Support for managers in establishing appropriate controls is provided by the appropriate finance business partners and internal audit.

*Managers with responsibility for awarding contracts, making payments, authorising grants and other financial transactions must ensure they have clear control procedures.* It is important that:

* There is adequate separation of duties and proper authorisation processes for payments.
* Staff dealing with these procedures are familiar with them.
* Accounting and other records, such as cash balances, bank balances, physical stock counts, are reconciled with the actual position.

The Importance of Monitoring

Managers have the prime responsibility for ensuring their systems are sound and that they are operating as intended. Both internal and external auditors have a role in carrying out independent reviews of systems and the adequacy of controls in place.

Many frauds are due to failure to comply with existing controls. It is vital that good control systems are supported by supervisory checking and alertness to the risks of fraud.

Additional guidance from the UK government and procedures on monitoring are included in [A Guide to Managing Fraud for Public Bodies](https://www.gov.uk/government/publications/a-guide-to-managing-fraud-for-public-bodies).

There is additional information available on conduct, discipline and management responsibilities in the [Civil Service Management Code](https://www.gov.uk/government/publications/civil-servants-terms-and-conditions) that sets out the regulations and instructions regarding the terms and conditions of service of civil servants.

Acceptance of Gifts or Hospitality

Under the civil service code it is made clear that you must not:

“Accept gifts or hospitality or receive other benefits from anyone which might reasonably be seen to compromise your personal judgement or integrity”

These ethical standards are described in more detail in the [conduct section of our guidance](https://scotsconnect.sharepoint.com/sites/FSS-MyLifeandCareer/SitePages/Conduct-and-discipline.aspx) and are laid down in the [Procurement Policy Manual](https://www.gov.scot/publications/procurement-policy-manual/) (for all staff involved in purchasing and contracting).

The impacts of failing to prevent fraud:

* Firstly it Impacts on bottom line diverting valuable resources away from where it is needed most
* The risks of litigation if we do not protect public resources
* Causes risks to services and delivery
* Affects our stakeholders confidence and our reputation as a competent government organisation
* Affects operational integrity
* Impacts on staff morale, not only the effect of a fraud in general terms but on those staff who are directly affected by its impacts either by failing to report or through error allowing it to take place.

# **Responding to Fraud**

The signs of Fraud highlighted earlier in this guide are not exhaustive and any indication of fraudulent activity should be reported.

Staff should report any suspicions either to their line managers, to the Head of HR, Head of Audit Assurance, to their finance business partner or - either in writing to the Head of Governance and Infrastructure or using the specific Crime stoppers hot-line (08000 15 16 28) any calls to this number will be in the strictest confidence.

Under the Scottish Government (SG) [Whistle-Blowing Procedures](https://scotsconnect.sharepoint.com/:w:/r/sites/Saltire/_layouts/15/Doc.aspx?sourcedoc=%7B6170BC7E-1FE8-4B31-88FB-17B2429AB739%7D&file=Raising_a_concern_under_the_Civil_Service_Code_and_whistleblowing_policy.docx&action=default&mobileredirect=true&CID=3F9F12FF-BE36-4972-92D2-DC5580998AC2&wdLOR=cEB3243BB-33F7-4C66-AFD9-82F4A79F4A82), all matters will be dealt with in confidence and in strict accordance with the terms of [the Public Interest Disclosure Act 1998](https://www.legislation.gov.uk/ukpga/1998/23/section/1). This statute protects the legitimate personal interests of staff.

Suspicions of fraud reported to line managers, Head of HR, Head of Audit Assurance or finance business partners must also be passed on to the Head of Governance and Infrastructure for coordination purposes.

All discovered cases of actual or attempted fraud will also be notified to the FSS Audit and Risk Committee. Consideration should also be given on a case by case basis to immediately notifying external auditors when a case comes to light.

Responding to Fraud

Thorough investigations should be undertaken where there is suspected fraud and the appropriate legal and/or disciplinary action should be taken in all cases. Appropriate disciplinary action should also be taken where supervisory or management failures have occurred.

Investigating fraud is a specialised area of expertise, and those tasked with any investigation work should have received appropriate training, including the gathering of evidence. Further detail on Fraud investigation can be found later in this guide. Investigations should not be undertaken by untrained staff. Specialist advice, such as Internal Audit, HR and Legal advice should be taken where necessary and as early as possible.

All cases of actual or suspected fraud will be vigorously and promptly investigated and appropriate action will be taken. The police will be informed where considered appropriate. In addition, disciplinary action will be considered not only against those members of staff found to have perpetrated frauds but also against managers whose negligence is held to have facilitated frauds. Both categories of offence can be held to constitute gross misconduct, the penalty for which may include summary dismissal.

# **Roles and Responsibilities**

Depending on an individual’s responsibility within FSS, the Board and employees will have different roles to play in relation to identifying, reporting, investigating and dealing with fraud. Specific roles and responsibilities are outlined below.

FSS Board

Is responsible for the systems of internal control that support the achievement of the FSS’ policies, aims and objectives.

Audit & Risk Committee

Receive reports from SG Internal Audit concerning investigations and recommendations. Chair of the Audit & Risk Committee to receive disclosures under the Public Interest Disclosure Act 1998.

Accounting Officer

As Accounting Officer, the Chief Executive is responsible for managing risks, including fraud. ‘[Managing Public Money’](https://www.gov.uk/government/publications/managing-public-money)*.* sets out a range of fraud risks, both internal and external, that FSS could face. The risk of a given fraud is usually measured by the probability of it occurring and its impact in monitory and reputational terms should it occur. The Chief Executive is responsible for establishing and maintaining a sound system of internal control that supports the achievement of policies, aims and objectives. The system of internal control is designed to respond to and manage the whole range of risks that FSS face.

Counter Fraud Champion

Lead in promoting an anti-fraud culture; chairing the Governance and Risk Team and on their behalf develop counter fraud policy, report on fraud and lessons learned across the FSS, work with counter fraud networks in the public, private and voluntary sectors; support fraud investigation activity across FSS

* Ensure the Executive Leadership Team regular review fraud risks associated with each of the key FSS objectives.
* Establish an effective counter-fraud strategy, policy and fraud response plan.
* Report of significant incidents of fraud to the Accounting Officer
* Liaise with the Audit & Risk Committee.

The Governance and Risk Team

Receive and reviews cases of suspected external and internal fraud. Supports the Counter Fraud Champion in preparing, reviewing, updating and communicating relevant guidance on counter fraud. Coordinates assurances about the effectiveness of anti-fraud policies to support the governance statement provided as part of the accounts.

Managers

Ensure that effective internal controls are operating within their areas of responsibility. Assessing the types of risk involved in the operations for which they are responsible and responding to minimise the opportunity for fraud. Managers should also report relevant cases to the Governance and Risk Team.

* Ensure that an adequate system of internal control exists within their area of responsibility and that controls operate effectively.
* Assess the types of risks involved in the operations for which they are responsible.
* Ensure that controls are being complied with and systems continue to operate effectively.
* Provide an annual report to Financial Accounting in respect of all fraud (suspected or actual) occurring during the year within their area of responsibility.
* Ensure that all staff in their department are aware of FSS’ counter-fraud

All Staff & Board members

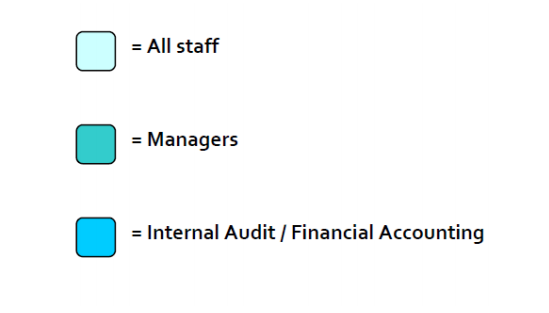
As stewards of public funds, staff and Board Members must have, and be seen to have, high standards of personal integrity. Staff and Board Members should not accept gifts, hospitality, or benefits of any kind from a third party that may be seen to compromise their integrity. For full details of accepting gifts and hospitality see the FSS’ Gifts and Hospitality Policy. All FSS staff and Board Members are:

* subject to criminal and civil law and the principles of the Civil Service Code and are responsible for complying with them
* responsible to FSS, (as employer or as members of the Board), to be aware of activities around them and to immediately report suspicions of fraud, however minor, and must be alert to the possibility that unusual events or transactions could be an indicator of fraud.
* advised to consider their personal and business activities and whether these may be considered to conflict with their duty to FSS. Any potential conflict of interest must be brought to the attention of their line manager.

Internal Audit

Are responsible for:

* assisting in the deterrence and prevention of fraud by examining and evaluating the effectiveness of control, commensurate with the extent of the potential exposure/risk in the various elements of FSS operations
* ensuring that management has reviewed its risk exposures and identified the possibility of fraud as a business risk
* assisting management in conducting potential fraud investigations where appropriate. Management and outcome of these investigations remains the responsibility of senior management.



# **Fraud Investigations - Fraud Response Plan**

FSS Fraud Response Plan aims

This plan sets out arrangements to ensure that when suspected fraud against FSS are reported, either to line managers, Head of HR, finance business partners, or others, action is taken to:

* Investigate the circumstances
* Minimise the risk of subsequent loss
* Ensure that appropriate recovery action is taken or, failing recovery, to initiate action to write off any losses
* Remedy any weaknesses in internal control procedures
* Initiate disciplinary and legal procedures, where appropriate
* Demonstrate that FSS is not a soft target for attempted fraud application

Key Roles

The Governance and Risk Team is based in the Governance and Infrastructure Division. Their role is to;

* receive and record information (anonymously or otherwise) about suspected frauds, either by telephone (using the fraud hot-line: 08000 15 16 28) or in writing, from individual members of staff or the public
* to consult and coordinate on counter fraud matters as required; agree what action, assistance and communication is required from within FSS and external sources (e.g. Police).
* to ensure that, where it is considered appropriate, senior management and/or Audit Scotland is informed about relevant cases as soon as possible after they come to light
* to report annually to the FSS Audit and Risk Committee (ARC).

The members of the Governance and Risk Team are:

* Head of Governance and Infrastructure (Chair)
* Head of Finance and Procurement
* Head of HR
* A nominated Audit Assurance representative (and/or Internal Audit)
* A nominated secretariat representative

Investigations

Following the reporting of suspicions of fraud to either line managers, Head of HR, finance business partners, or others, the information must be passed on to the Governance and Risk Team for coordination purposes.

A recommendation from a specialist area will then be sought, as appropriate, to advise the Governance and Risk Team whether any allegations warrant further action or investigation.

If further action or investigation is agreed, the Governance and Risk Team should support the Business area to initiate the following action, insofar as it is appropriate to the particular case.

Key points

Fraud investigations can be undertaken by Internal Audit, HR or an Independent Investigating Officer, depending on the circumstances.

Any investigation will take account of any relevant work or recommendations by a specialist area e.g. Internal Audit and HR reports. Preliminary investigation findings must be reported to the Head of Governance and Risk Team for consultation

Decide the level at which line management should be involved and bring allegations to the notice of line management if appropriate

Secure records and assets, including restrictions on access to offices and computer terminals

Based on advice from HR involving SG legal as required, consider the prima facie case for suspension of FSS members of staff who are subject of allegations

Agree the scope and nature of any investigative work required to establish the facts of a particular case

Notify senior management as required, including the Accountable Officer

Decide whether the appropriate Police/Procurator Fiscal Service contacts should be informed

Agree a timetable for completion of any agreed actions

Terms of Reference for Investigations

The Governance and Risk Team will consider carefully the terms of reference for any investigative work. Investigations should not be restricted solely to allegations against an individual that may lead to a charge of gross misconduct. If there is a possibility that instances of serious misconduct (e.g. misconduct other than fraud) may also have occurred, these should be investigated at the same time as the fraud allegations by HR under the FSS’ Disciplinary Policy and Procedures.

Selection of Investigating Officer

It is a matter for HR to appoint, where necessary, the independent Investigating Officer although the Governance and Risk Team will be informed of the proposed appointment. The Investigating Officer should be at least B3 level with the appropriate skills to undertake an investigation and, if necessary, knowledge of the area of work under investigation. The Investigating Officer should be a person who has not had close personal or work related ties with the person under investigation.

Action on Investigation Findings

As soon as possible after investigations have been completed and the Governance and Risk Team is satisfied that no further investigations are required, it must ensure:

* That disciplinary action, if any, is being taken (in line with Disciplinary Policy and Procedures)
* That disciplinary action, if any, is being taken if the initial allegation appears to be malicious
* That the form and content of any report to senior officers is appropriate
* That the Police/Procurator Fiscal is notified if required

Case Closure, Follow Up and Review

Where evidence of fraud or serious misconduct has been identified, the Governance and Risk Team should consider whether any action needs to be taken to prevent a reoccurrence. In such cases, an action plan should be drawn up setting out recommendations. In practice, much of the required action is likely to relate directly to action plans drawn up by Internal Audit or HR and a cross reference to these plans is all that is required.

Action plans will include the required steps to take in response to an investigation’s findings. An occurrence of fraud may hold lessons to be learned for an individual business area or the whole of FSS. The Governance and Risk Team has a lead role in ensuring that all appropriate action is taken forward effectively.

The Governance and Risk Team should be informed by HR of the outcome of cases where a charge of gross misconduct has been made. In any case where such a charge has been brought but a disciplinary hearing does not uphold the charge or an appeal panel overturns the panel’s decision, the Governance and Risk Team should be informed of the reasons for the Panel's decisions. The Governance and Risk Team must consider whether, in light of this information, there are lessons to be learned in terms of the handling of cases and whether the Fraud Response Plan and related guidance, for example on disciplinary procedures, is operating effectively.

The Governance and Risk Team should make recommendations for any changes to procedures that it considers necessary in light of the outcome of individual cases and should consult relevant interests, including the Civil Service Government Union, on any recommended changes. If appropriate, where individuals have been dismissed or subject to other disciplinary action for matters other than fraud (e.g. abuse of IT systems), HR will inform Internal Audit of the circumstances of the case and consideration given to whether a further review (by Internal Audit) should be undertaken to establish whether or not there has been possible misuse of other systems by the same individual(s).

Confidentiality

Members of the Governance and Risk Team will receive the appropriate information relating to individual cases. They must treat all information relating to individual members of staff on a Restricted - Staff basis and should ensure that it is only passed on to colleagues on a strictly need to know basis. HR will place a record on the career folder of a FSS member of staff only where there has been disciplinary action taken. Further information is provided under the FSS Whistle-blowing procedures.

Reporting Cases of Fraud

Details of fraud should be reported at least annually to the Scottish Government’s (SG) Governance and Risk Team. This should include details of fraud where actual losses have been incurred. Details must also be reported to the Head of Financial Accounting in FSS to arrange for notation for the accounts.

The Governance and Risk Team will provide an annual report to ARC covering the arrangements for dealing with fraud within FSS and providing summary details of cases coming to light during the preceding financial year.

The Head of Governance and Infrastructure will report cases of fraud that may have wider implications to the SG Audit and Assurance Committee via the SG Governance and Risk Team.

External Fraud

External fraud are fraud perpetrated by third parties against the FSS (e.g. contract fraud or fraudulent applications for grants or subsidies or expenses). The SG Governance and Risk Team is available to advise on arrangements for dealing with external fraud.

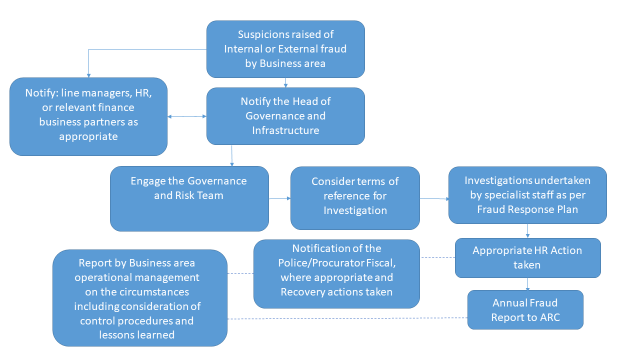
Procedures for responding to suspected external fraud, insofar as they are appropriate to the particular case, may include the following:

* A report by operational management on the circumstances surrounding the case, including the results of any investigations
* A formal assessment of whether the evidence tends to substantiate fraud. Any invalid claims or invoices that could reasonably be argued were submitted in good faith should not normally be regarded as fraud
* Notification of the Police/Procurator Fiscal, where appropriate
* Recovery action
* Consideration of control procedures and lessons learned

It will normally be sufficient to alert the IT Department about any cases of internet scams. If fraud by a supplier is suspected, the Head of Finance and Procurement should be kept informed of developments. Cases of straightforward theft (which does not qualify as fraud) should be notified to the Head of Finance and Procurement.

If there is any suspicion of collusion on the part of FSS members of staff in a suspected or discovered external fraud, the procedures relating to internal fraud should apply as appropriate, given any requirements arising from ongoing Police/Procurator Fiscal investigations.

# 



# **Conclusion**

FSS takes fraud and potential fraud very seriously. The circumstances of individual frauds will vary, however it is important that all are thoroughly and promptly investigated and that appropriate action is taken.

Successful fraud prevention involves creating an environment which inhibits fraud. It is the responsibility of all staff to ensure that such an environment is created. Staff who are alert to the possibility of fraud and who act accordingly are a powerful deterrent against fraud.