Counter Fraud Policy Guidance

Associated with Counter Fraud Policy to be Approved by Committee on 24 February 2021 with an implementation date of 1 April 2021

Table of Contents

1. Purpose Statement

1.1 The Counter Fraud policy defines the control environment and key principles adopted by the Council to counter all types of fraudulent activity. That includes fraud, bribery and corruption, money laundering and tax evasion. For the purposes of the policy where the term "Fraud" is used that is generically meant to include any of these activities.

1.2 This policy guidance provides additional detail and procedure guidance in relation to:

- Responsibilities
- Supporting Procedures and Documentation
- The Policy Statement and implementation of that policy
- Definitions
- Detailed appendices are provided of the Fraud Risk Matrix and checklists.

2. Responsibilities

General Responsibilities

2.1 It is the duty of all officers employed by the Council to fully comply with the Policy that forms an associated part of the Financial Regulations. Failure to comply with the requirements of this Policy and the associated guidance and procedures may result in an investigation under the Council's Conditions of Services Disciplinary and Appeals Procedure.

2.2 It is the duty of all Elected Members to fully comply with the Policy. Failure to comply with the requirements of the policy and the associated guidance and procedures may result in an investigation under the Councillors' Code of Conduct.

2.3 Any breach or non-compliance with the Policy must, on discovery, be reported immediately to the Chief Officer – Finance. The Chief Officer - Finance may consult other relevant officers, including the Chief Executive, to determine the appropriate action.

2.4 Employees who deliberately obstruct or unreasonably fail to provide information to Auditors or Investigation Officers within the specified period may be subject to disciplinary action.

2.5 Any party or person committing fraudulent activity or behaviour against the Council may be subject to relevant measures as available to the Council and other relevant agencies under the law. These may include warnings, recovery of losses through legal action, fines, interest charges and custodial sentences.

Responsibility of the Chief Officer - Finance

2.6 It shall be the responsibility of the Chief Officer - Finance, or designated officer, to ensure that the policy is kept up to date and is monitored for its effectiveness. The policy shall be reviewed every 3 years and Fraud Policy Guidance updated as required to take account of changes in statute, professional guidance or Council policy that impact upon the Regulations.

2.7 The Chief Officer - Finance, as the "Proper Officer", in terms of Section 95 of the Local

Government (Scotland) Act 1973, shall be the adviser on financial matters to the Council and all its Committees. S/he shall be responsible for the proper administration of the Council's financial affairs.

2.8 Under this legal responsibility, the Chief Officer – Finance has authority to lead and act in respect of the Council's Counter fraud response. The Chief Officer Finance has the responsibility to ensure that appropriate capability and capacity is employed on a risk managed basis to enable prevention and pursuance of fraudulent activity.

2.9 The Chief Officer Finance is responsible for co-ordinating engagement with national fraud prevention initiatives such as the National Fraud Initiative.

2.10 The Chief Officer – Finance shall deal with reported irregularities in accordance with the Council's policies and procedures through the Fraud system at www.report-fraud.co.uk/aberdeencity. S/he, may, following consultation with the Chief Executive and the Chief Officer - Governance, report matters to the Police, Crown Office and Procurator Fiscal where s/he considers it appropriate to do so.

2.11 Regulated financial services are required to appoint a Money Laundering Reporting Officer. Local authorities are not currently required to make such appointments. However, it is important that staff have a single point of contact to report any suspicion activity. The Chief Officer – Finance is responsible for receiving and actioning potential disclosures about money laundering activity which may include contacting the National Crime Agency and submitting a SAR (Suspicious Activity Report).

2.12 Records relating to Fraud, Bribery and Corruption, Money Laundering and Tax Evasion will be retained by the Chief Officer – Finance. A report on matters arising from the work of the Counter Fraud team will be presented to the Audit, Risk and Scrutiny Committee annually.

Responsibility of the Chief Officer – Governance

2.13 Records relating to Whistleblowing will be retained by the Chief Officer – Governance.

2.14 It shall be the responsibility of the Chief Officer – Governance, following consultation with the Chief Officer - Finance, to incorporate any Counter Fraud issues in the Annual Governance Statement, incorporated into the Accounts and reported to Audit, Risk and Scrutiny Committee.

2.15 The Chief Executive has ultimate responsibility for the provision of the Internal Audit service to the Council. Internal Audit has a reporting line to the Chief Officer - Governance. The Chief Officer – Governance will seek to align the work of the Internal Audit service with that of the Counter Fraud service where appropriate in consultation with the Chief Officer – Finance.

2.16 The Chief Officer-Governance is the Chair of the Risk Board, and as such will scrutinise counter fraud activity as set out below.

Risk Board

2.17 The Risk Board provides scrutiny, guidance and direction to the Counter Fraud response supplementing the role of the Chief Officer-Finance and making decisions delegated to Officers. That may include:

- Leading the Council's counter fraud culture and advocating the Council's response to the counter fraud Pillars and Themes in the policy;
- Approving the Annual Counter Fraud plan;
- Receiving recommendation summaries for review and action in cases of non compliance;
- Reviewing compliance with the FFCL checklist and SOC checklists referred to in section 4.1 and 4.49 of this Guidance;
- Making decisions on strategic activities and Counter fraud planning activities;
- Ensuring that new policies reflect appropriate Counter fraud measures;
- Providing consultation and advice and acting as the conduit to develop communication to Chief Officers and Employees.

2.18 For the purposes of Counter Fraud activity, the Risk Board represents the Senior Executive Board for decision making and approval of actions.

Audit Risk and Scrutiny Committee

2.19 The Committee responsible for oversight of the Counter fraud function is the Audit, Risk and Scrutiny Committee. The Committee will review and approve the Counter Fraud Policy every 3 years and approve any significant changes to the policy during the interim period.

2.20 ARS will receive an annual report in relation to Counter Fraud activity of all types from the Chief Officer-Finance. The Committee should seek explanations and action where the Chief Officer – Finance has indicated that any aspect of Counter Fraud Activity requires special attention. The Committee is entitled to seek explanations for any matter which it deems require special attention subject to its Terms of Reference.

Responsibility of Chief Officers

2.21 It shall be the duty of each Chief Officer to ensure that the Policy and all associated guidance is made known to appropriate staff members and shall ensure full compliance with them.

2.22 In preventing fraud and maintaining internal controls, Chief Officers will require to actively horizon scan to be aware of the wide range of Supporting Procedures and Documentation set out in Section 3 of this Guidance. For Chief Officers responsible for services highlighted as potential fraud risk in Appendix 1 that puts an additional responsibility for awareness of relevant best practice, legislation and guidance in those fields. A key responsibility in this remit is keeping appropriate records of operational, transactional and employment activity to enable effective prevention and pursuance of fraud.

2.23 Chief Officers are responsible for ensuring that risk management arrangements are in place in their Cluster to prevent, detect and prohibit fraud, bribery and corruption, money laundering and tax evasion. Risk assessments will be undertaken for each of the Council's key business activities with individuals identified who may be at most risk of being exposed to bribery. Chief Officers will engage with relevant Service Managers and employees to undertake this responsibility. Special attention should be given in this risk assessment to any areas of manager's discretion applied to associated policies in section 3.2 of the Guidance and the definitions of bribery and corruption as set out in section 5 of the Guidance.

2.24 Chief Officers are responsible for communicating specific actions in relation to that risk assessment across the workforce and also to associated persons undertaking work on behalf of the Council. Training will be provided by the Counter Fraud service to appropriate employees who have been identified through risk assessment as being at potential risk of exposure to fraud.

2.25 Whenever any matter arises which involves, or is thought to involve, irregularities concerning funds, property or the exercise of the Council's functions, or that of any Connected Body, the relevant Chief Officer shall notify the Chief Officer - Finance in writing through the Fraud system at www.report-fraud.co.uk/aberdeencity.

2.26 Chief Officers shall engage with the Counter Fraud service and Internal Audit in receiving advice and implementing recommendations and risk assessments where required.

Responsibility of Chief Executives/Managing Directors/Trustees/Board Members of Connected Bodies.

2.27 The Head of Commercial and Procurement Services shall use reasonable endeavours to ensure that all contracts with Connected Bodies will provide that:

- In the absence of their own equivalent policies and documents, Chief Executives/Managing Directors/Trustees/Board Members of Connected Bodies shall adhere to the policy.

- Chief Executives/Managing Directors/Trustees/Board Members of Connected Bodies shall ensure that their organisation has appropriate Counter fraud arrangements in place, including internal audit arrangements.

- Chief Executives/Managing Directors/Trustees/Board Members of Connected Bodies shall respond to recommendations and advice provided by the Council's Counter-fraud service.

Responsibilities in relation to Aberdeen City Health and Social Care Partnership (ACHSCP)

2.28 The ACHSCP oversees the delivery of integrated services that the Council has been directed by the ACHSCP to deliver.

2.29 The policy as an associated document of Aberdeen City Council financial regulations is fully applicable to Council staff who are working to deliver integrated services under directions from the ACHSCP as defined in financial regulations.

Internal and External Audit

2.30 The Council's Auditors shall have the right to access all records (electronic or manual), documents and correspondence relating to any financial or other transactions of the Council. They will be able to receive such explanations as they consider necessary concerning any matter under examination.

2.31 Officers of the Council will ensure that these rights are given to the Council’s External and Internal Auditors. These rights apply to any and all examples of fraudulent activity.

Employees and Elected Members and Associated persons

2.32 Council employees, elected members, workers, agents and associated persons performing services on behalf of the Council are required to assist and to be vigilant in preventing, detecting and reporting acts of fraud, bribery and corruption. That includes responding to instructions and actions required as a result of compliance with procedures and documentation, undertaking risk assessments and taking other preventative action as identified in sections 2.21-2.26 of this Guidance.

2.33 All employees and elected members have a duty to report fraud, bribery, corruption, money laundering or tax evasion in any form. Employees will report suspicions as soon as possible to the Chief Officer – Finance through the Counter Fraud system at www.report-fraud.co.uk/aberdeencity. Employees are also expected to report any concerns of actual or suspected incidents to their line manager, and in the case of elected members, this should be the Chief Officer - Governance. If an allegation relates to a member of staff’s line manager, then the matter should be escalated to the next most senior person who is not involved.

2.34 Any person making a report of actual or suspected fraud in good faith will be given appropriate support. As described in Section 4.5 of this Guidance, reports will be in strict confidence. Reports of any form of suspicious behaviour are encouraged as they can form a robust response to fraud prevention and detection measures.

2.35 Prompt action will be taken to gather appropriate information and risk assess the suspected activity in advance of undertaking an investigation if appropriate. An alternative route for employees and workers to report an act of bribery, fraud or corruption is through the use of the Whistleblowing policy.

Individuals and Third Parties

2.36 The Council requires all individuals and organisations with whom it deals in any capacity to behave toward the Council with integrity and without intent or actions involving fraud, bribery and corruption.

2.37 All individuals and third parties are asked to assist and to be vigilant in preventing, detecting and reporting acts of fraud, bribery and corruption. Individuals and third parties may report suspicions as soon as possible to the Chief Officer – Finance through the Counter Fraud system at www.report-fraud.co.uk/aberdeencity.

3. Supporting Procedures & Documentation

3.1 Supporting procedures and documentation to the policy are wide ranging, since prevention of fraud relies on a combination of effective legislation, guidance, procedures and internal controls. Categories of supporting documents are as follows:

- Legislation relating to Financial Controls, Fraud prevention and Fraud in the context of specific activities in the Council
- Best practice guidance
- Counter fraud internal strategic and planning documents, additional procedures and guidance
- Council policies and procedures that set standards and controls that will support fraud prevention
- Statute and Common law

3.2 Key documents in the categories above are shown below:

Legislation

- S95 Local Government (Scotland) Act 1973
- Proceeds of Crime Act 2002
- Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017/692
- Sanctions and Anti Money Laundering Act 2018
- Bribery Act 2010
- General Data Protection Regulation 2016/679
- Data Protection Act 2018
- The Criminal Finances Act 2017
- Traffic Regulation Act 1984 (Blue Badge)
- Housing (Scotland) Act 1987 (False Homelessness)
- Pending Legislation - Non-Domestic Rates (Scotland) Act 2020

Best Practice Guidance

- Fighting Fraud and Corruption Locally
- Serious Organised Crime Taskforce strategy

Counter Fraud internal documents

- Counter Fraud Policy Guidance
- Counter Fraud Annual Plan
- Service Standards and Commissioning Intentions
- Training Materials
- Counter Fraud specific procedures and guidance

Council Policies and procedures

- Managing Discipline
- Corporate Information Policy
- Financial Regulations
- Following the public pound policy
- Service Income policy
- Declaration of interests
- Whistleblowing policy
- Continuous Review and Development Scheme
- Recruitment and Induction Scheme
- Risk Management Policy

Statute and Common Law

- The law associated with Fraud, Bribery & Corruption, Money Laundering and Tax Evasion is complex and thus the policy cannot provide a full and authoritative account of the relevant legislation. Any enforcement action being undertaken must take recognition of current legislation and statute and common law.

- Examples of statutes which would apply would be :
  - Criminal Justice and Licensing (Scotland) Act - references disclosure of exculpatory evidence to defence agents;
  - Criminal Procedure (Scotland) Act - necessary certification to enter documents as evidence;
  - Human RIghts Act - incorporates the principles of ECHR and an individual's right to a fair trial, private life.

- Examples of common law would be:
  - the fairness of our investigation and how we collected evidence
  - the constituent parts of a common law offence we are reported to the Fiscal
  - the quality of our evidence in tying the accused to the offence.

3.3 Changes to this guidance will be updated on the Counter Fraud section of the Council’s Intranet site without recourse to update the Policy. The Counter Fraud Policy will include references relevant at the time of approval.

3.4 Directed preventative advice by the Counter Fraud team will support services with horizon scanning and interpreting appropriate legislation, procedures and documentation.

4. Policy Statement/s

4.1 The Council will take a robust approach to countering fraudulent activity in any form using the five pillars identified under the Fighting Fraud and Corruption Locally Guidance:

Govern We will have robust arrangements and executive support to ensure anti-fraud, bribery and corruption measures are embedded throughout the organisation. Having a holistic approach to tackling fraud is part of good governance.

Acknowledge We will acknowledge and understand fraud risks and commit support and resource to tackling fraud in order to maintain a robust anti-fraud response.

Prevent We will prevent and detect more fraud by making better use of information and technology, enhancing fraud controls and processes and developing a more effective anti-fraud culture.

Pursue We will recover losses through all available means, developing capability and capacity to investigate fraudsters and developing a more collaborative and supportive local enforcement response.

Protect We will protect against serious and organised crime, protecting individuals from becoming victims of crime and protecting against the harm that fraud can do to the community. We will protect public funds, protecting our organisation from fraud and cybercrime and also protecting itself from future frauds.

The FFCL guidance provides a Counter Fraud Checklist for local authorities. That is attached at Appendix 2 to this document and the Risk Board shall review that annually.

The performance in response to these pillars is measured against 6 themes of *culture, capability, competence, capacity, communication and collaboration*. Measures to support these themes are set out throughout the policy and guidance in specific statements and directions and the Counter Fraud Checklist in Appendix 2 is intended as a comprehensive list of actions for performance assessment and that is further reflected in Section 8 of the policy – Policy Performance.

The below policy statements set out directions against each pillar, references are made to where policy statements are set out elsewhere in the Policy or this Guidance.

Govern

4.2 The responsibilities set out in Section 2 of this Guidance are intended to set out a strong approach to Counter Fraud Governance. The strength of the responsibilities of the Audit and Scrutiny Committee, the Risk Board (underpinned by the role of the Chief Officer - Governance) and the Chief Officer – Finance and Internal and External Audit in that section are intended to provide a comprehensive governance approach.

4.3 The specific and practical requirements of Members, Chief Officers and all employees and parties set in place a breadth of responsibility for all across the organisation and its partners to prevent and enable pursuance of fraud.

4.4 The governance responsibilities set out in Section 2 will be supported by online training and development materials and supplemented by targeted advice where appropriate so that responsible persons comprehend fully their governance roles.

4.5 In maintaining appropriate governance of the counter fraud response, specific attention is drawn to the importance of fundamentals of governance such as confidentiality, data protection, performance management and reporting. These principles and the application of relevant appropriate Council policies with complete integrity shall be deployed in the operation of all counter fraud activity. This provides assurance to protect those reporting fraud and further assurance to the Council and its stakeholders.

4.6 The operational activities of the Counter Fraud service will be planned and managed through the Counter Fraud Annual Plan, Service Standards and Commissioning Intentions. These will be reviewed for approval by the Risk Board and Strategy Board.

Acknowledge

4.7 The responsibilities set out in Section 2 of this Guidance place a responsibility on the Chief Officer Finance to make appropriate resource available to maintain a robust anti-fraud response. The strength of responsibilities of Chief Officers (sections 2.21 to 2.23) to undertake horizon scanning and risk assessment with the support of the Counter Fraud service provides assurance in this regard.

Prevent

4.8 A critical pillar in the counter fraud response is prevention, the Council intends to put in place measures to continuously strengthen its preventative action against fraud.

4.9 All new policies will be reviewed and scrutinised by the Risk Board Policy Group. The Counter Fraud team will be represented on that group in order to ensure suitable safeguards are reflected where appropriate to minimise the risk of fraud, bribery and corruption.

4.10 The Counter Fraud annual plan will include resource allocated to specific Counter fraud prevention activities. Fraud risk will be regularly reviewed based on experience and best practice. That will result in targeted preventative reviews, advice and enabling support from the Counter Fraud service. Material fraud prevention recommendations will be recorded for implementation and reported through the Risk Board.

4.11 The Council participates in National Fraud Initiative and regularly provides information for data matching purposes with the data of other public bodies. The Counter Fraud Service will work with Council Services to undertake proactive data matching exercises. Periodically testing for anomalies can highlight irregular transactions before other methods such as a routine audit. As well as acting as a deterrent, it also allows frauds to be stopped sooner.

4.12 The Counter Fraud Service and Internal Audit Service will share knowledge and understanding of the controls environment. The Counter Fraud Annual Plan and Internal Audit plan will be considered by the Risk Board at the same meeting annually. Where appropriate, joint Counter Fraud and Internal Audit preventative reviews will be undertaken.

4.13 The Counter Fraud service will receive regular updates from Internal and External Audit work through the Chief Officer – Finance and recommendations and will build their findings into the Counter Fraud Annual Plan.

4.14 The Counter Fraud service will liaise regularly with the People and Organisation Cluster in order to provide advice for the development and implementation of any policies in relation to people or organisation. The Counter Fraud service will advise the People and Organisation Cluster on any matter or case where it is considered Counter Fraud advice would be relevant.

4.15 The Counter Fraud service may pro-actively use any data held by the Council for preventing fraud, subject to relevant data protection and confidentiality legislation. The Counter Fraud service will proactively work with Council services to improve the quality and scope of routinely captured information. Routine access is required to systems holding employee payroll and HR data, largely for the purposes of investigating matches generated through the National Fraud Initiative.

4.16 The Counter Fraud service will work with other services to have a comprehensive knowledge of data sets held across the organisation, so that they can be formally approached to disclose this for counter fraud purposes. The Counter Fraud service will work closely with Information Governance, Data and Insights and Digital and Technology services in sharing knowledge of available databases and IT systems and be given access to system owners who can be approached to access those systems.

4.17 The Counter Fraud service may pro-actively support any service or partner organisation where added value, skill or expertise may be applied. This may relate primarily to services identified in Appendix 1, and notably will relate to tenancy management, debt recovery and benefit administration. There is a considerable wealth of good practice information available from fraud prevention organisations that can support in the administration, good management practice and financial advice of many services.

4.18 The Counter Fraud service may initiate preventative reviews where indicators of possible fraud have been identified, but not to a sufficient level to lead to an investigation. The Counter Fraud service will advise services on potential issues and indicators of fraud to raise awareness.

Pursue

4.19 When fraud has been identified the Council will seek to fully recover any losses. Where appropriate the Council will seek further redress through fines or criminal procedure, where appropriate.

4.20 The Counter Fraud function shares information, as permitted by data protection legislation, with internal and external partners in order to prevent and detect fraud, and to trace offenders.

4.21 The pursuance of fraud allegations is described in the below three sections of Reporting, Evaluation and Investigation, special reference is also made for Employee Investigations and Fraudulent use of ICT.

Reporting

4.22 On receipt of a fraud allegation the details will be entered into the case management system. This is to ensure that all actions are recorded in the one location, and to enable reporting to management. Allegations may be received from two distinct groups: 1) employees, Members and those with a contractual or partnership relationship with the Council 2) individuals or third parties including members of the public.

4.23 Automated reporting tools are available to both groups. The reporting detail for Group 1 is more extensive, that group are strongly encouraged to leave their names and contact details so that investigators can obtain further pertinent information. All details are held confidentially and will not be shared without consent. Allegations from group 2 are initially recorded in a simpler form to encourage reporting without prejudice.

4.24 Any allegations of fraud, bribery, corruption, or other serious criminal behaviour by an employee will be notified to the Chief Officers-Finance. Under no circumstances will the employee be notified, or an investigation under the Managing Discipline procedure commence, until counter fraud officers have completed their investigation and advised the Chief Officers of the facts.

4.25 As the Officer ultimately responsible for managing member-officer relations, allegations concerning elected members will be referred to the Chief Officer, Governance as relevant to the role as Monitoring Officer and in reference to the Councillor’s Code of Conduct.

Evaluation

4.26 Every fraud referral is initially assessed by the Counter Fraud service. That criteria includes whether the allegation does indeed relate to a matter within the counter fraud remit; the quality of the information; the likely detriment to the Council; and the nature of the alleged fraud. The details of the allegation are checked against Council records, and publicly held information. Thereafter the matter will either be raised as a case for investigation by the Counter Fraud Service, referred for internal investigation through the Service or People and Organisation Cluster, referred to a more appropriate agency (for example Police, DWP, HMRC) or disposed of through closure.

4.27 After assessment the considerations and reason for evaluation are recorded based on set guidelines. Any referrals where there may be discretion regarding the evaluation outcome will be referred to relevant Chief Officers for consideration. Where relevant joint investigations may be initiated between the Counter Fraud service, agencies and services.

4.28 When an allegation has been recorded by an officer in the undertaking of their work, It is imperative that records are kept in relevant client or service systems to capture the most accurate and specific information known, in addition to records kept by the Counter Fraud service. Any actions or conversations by staff must be timeously documented on the relevant system (e.g. iWorld when a housing officer has any interaction with a client).

4.29 Counter Fraud Officers should be afforded access to whatever information or records they consider necessary to pursue their investigation.

4.30 A written or emailed request by a Counter Fraud Officer is sufficient to obtain any internally made or held note, record, recording or other data which is not legally privileged information. The Chief Officer – Finance will receive regular updates of information requests.

Investigation

4.31 Fraud investigations can result in legal action by civil or criminal procedure. The means of disposal depends on the type and quality of the evidence, as well as the specific nature of the alleged offence. As such, at all times evidence will be gathered to a criminal standard so that criminal disposal remains an option. Investigation records will be held confidentially on the case management system.

4.32 Counter Fraud Officers (CFOs), as designated by the Chief Officer – Finance, are authorised to:

- Enter freely and at all reasonable times any Council operated premises or land.
- Have access to all records (electronic or manual), documents and correspondence relating to any financial or other transaction of the Council.
- Require and receive such explanations as are necessary concerning any matter under examination.
- Require any employee to produce cash, stores, or any other Council property under his or her control.
- Examine financial records or assets of organisations in receipt of grant aid from the Council.
- In the discharging of these duties, the CFO will present, upon request, a duly authorised certificate confirming the above provisions.

4.33 To allow the timely investigation of allegations of fraud requests for information from CFOs must be managed within the timescales advised. Any failure to respond or provide information will be escalated to Head of Service, and copied to the Section 95 Officer, to identify the reasons for delay.

4.34 When obtaining witness statements, counter fraud officers are permitted to audio record that statement with the prior express permission of the witness. The witness is permitted to obtain a copy of that recording when the investigation has concluded (or been dealt with in Court, if appropriate). At the conclusion of each interview the witness will be provided with a copy of the recording.

4.35 Where permitted by law, the Counter Fraud Team will share information and intelligence with internal and external partners and agencies for the purposes of crime prevention and detection, as well as tax and rates collection.

4.36 The Counter Fraud service will report regularly to the Chief Officer Finance and the Chief Officer Governance of investigations in progress and of any significant investigations initiated immediately.

4.37 Where information is received via the whistleblowing procedure the Chief Officer -Governance will refer relevant allegations to the Counter Fraud service.

4.38 On conclusion of an investigation appropriate closure and outcome records will be recorded in the case management system. Appropriate action will be taken and in addition to civil or criminal procedure, preventative actions and recommendations will be made. Confidential summary information of an appropriate nature will be provided to relevant stakeholders and reported through the Risk Board and Audit, Risk and Scrutiny Committee. Risk registers will be updated where applicable.

Employee Investigations

4.39 For allegations relating to employees, fraud investigations may lead to internal action by Aberdeen City Council. Where that action appears to require the use of the Managing Discipline policy, counter fraud officers will notify People and Organisation immediately. If the referral to People and Organisation is of a matter of dishonesty, responsibility for investigating under the procedure will lie with an officer external to the employing service. This is to ensure that the matter is investigated impartially.

4.40 For employee allegations, it may be relevant for the Counter Fraud service to provide advice to investigating officers or to undertake an initial investigation of the fraudulent element of the allegation, dependent on the nature of the allegation. Such allegations will be considered where relevant jointly and with any decisions on approach being made by the Chief Officer – Finance and the Chief Officer – People and Organisation.

4.41 People and Organisation will advise the Counter Fraud service when a Managing Discipline case may have a fraud aspect in its nature. That case will be recorded using the Counter Fraud reporting process when required and will follow the protocol in 5.32.

4.42 If an investigation relating to an employee uncovers evidence that suggests that there has been a breach of criminal law, the Counter Fraud Officer will discuss the findings with People and Organisation and the final decision on whether the case is reported criminally will rest with the Chief Officer - Finance.

4.43 Where it has been established that an employee who, is or has been, in receipt of a state benefit or allowance or discount, and has failed to adhere to the terms of receiving the benefit, allowance or discount then consideration should be given as to whether there has been a breach in their terms and conditions of employment. People and Organisation will be notified and it will be that function’s responsibility to initiate the Managing Discipline procedure.

Fraudulent use of Information and Communications Technology

4.44 For allegations relating to employees, fraud investigations may lead to internal action by Aberdeen City Council. Where that action appears to require the use of the ICT policy, counter fraud officers will notify Digital and Technology immediately. Procedures would then follow the approach described for employee investigations.

Protect

4.45 The nature of criminal activity continues to evolve and develop. The Protect pillar of the policy relates to protecting the Council, its partners and citizens from organised crime. Protecting the victims of crime, protecting public funds and protection from future frauds. The future nature of fraudulent activity consistently evolves as new technology and global structures change and allow for new crimes to emerge.

4.46 The Counter Fraud Service will horizon scan regularly to assess the latest available knowledge on organised crime and evolving fraudulent activity.

4.47 Specific activities related to such evolving crimes are also captured within the high risk fraud areas identified in Appendix 1 and these become part of the ongoing risk assessment approach for all services. Examples that would be relevant to Council operations could be cyber crime, payment fraud, metal theft and bogus workmen.

4.48 The Council will work with relevant agencies to identify and address protection matters such as business organisations and has a responsibility to be alert to the risks of doing business with those involved in organized crime.

4.49 The Council will keep under regular review Scotland's Serious Organised Crime Strategy and the SOC checklist attached in Appendix 3.

5. Definitions

5.1 The law associated with Fraud, Bribery & Corruption, Money Laundering and Tax Evasion is complex and thus the policy cannot provide a full and authoritative account of the relevant legislation. Any enforcement action being undertaken must take recognition of current legislation and associated case law. This Guidance provides a more full description of the definitions in the policy and is expanded with examples.

Fraud

5.2 The Accounts Commission for Scotland describes fraud as the use of deception with the intention of obtaining private gain, avoiding an obligation or causing loss to another party.

5.3 For the purposes of the policy, fraud is defined in its widest sense to describe any dishonest behaviour such as forgery, false representation and the concealment of material facts. The fraudulent use of Information & Communication technology (ICT) resources is included in this definition.

Examples of fraud include, but are not exclusive to:

- Distorting or concealing both financial and non-financial information;

Knowingly and intentionally obtaining or attempting to obtain benefits to which there is no entitlement through;

- Falsification or alteration of accounting records or other documents;
- Misappropriation of assets or theft;
- Suppression or omission of the effects of transactions from records or documents;

Recording transactions that have no substance e.g., time recording records that do not reflect actual hours worked.

- Willful misrepresentations of transactions or of the Council's state of affairs, which may involve the misuse of funds or other resources, or the supply of false information.

Bribery

5.4 A bribe, as defined in the Bribery Act 2010, is a financial or other type of advantage that is offered or requested with the intention of inducing or rewarding improper performance of a function or activity. Acts of bribery are designed to influence an individual in the performance of their duty and incline them to act dishonestly.

Examples of bribery include, but are not exclusive to:

- A direct or indirect promise;
- Offering or authorisation of anything of value;

The offering or receipt of a payment including a loan or fee or reward or any other advantage;

- The offer of aid or a donation.

The following would be regarded as unacceptable behaviour by employees, elected members, workers, agents and any associated persons performing services on behalf of the Council and must not occur:-

- Accepting, requesting a bribe, whether financial, or other reward, from any person or organisation in return for providing some favour.
- Offering a bribe, whether financial or other reward, to any person or organisation in return for providing some favour.
- The making or accepting of any facilitation payments, which are unofficial payments made to government officials (including Council officials) for carrying out or speeding up routine procedures.
- Dishonesty, theft, fraud or the deliberate falsification of records and / or benefit / or other claims administered by the Council.

5.5 In accordance with the Bribery Act 2010, the Council will conduct its activities honestly and will apply high ethical standards without the use of acts of bribery. The Bribery Act makes it illegal to offer or receive bribes and to fail to prevent bribery. The Act makes provision for both individual and organisational responsibility for bribery and creates offences that carry prison terms of up to 10 years and unlimited fines.

Corruption

5.6 Corruption is the unlawful offering, giving, soliciting or acceptance of an inducement or reward, which could influence the actions taken by the Council, its Elected Members or its employees. This also applies to business partners where a relationship is in place for them to undertake duties on behalf of the Council. Corruption can also include bribery which is not entirely removed from fraud either as offences may overlap between them.

5.7 Examples of Corruption include, but are not exclusive to:

- Disclosure of information;
- Using a position of authority inappropriately;
- Altering contracts or official forms;
- Misuse of IT systems;
- Falsifying records;

- Making purchases of goods or services that are unnecessary or excessive.

Money Laundering

5.8 Money laundering is the process by which criminally obtained money or other criminal property is exchanged for "clean" money or other assets with no obvious link to their criminal origins. The aim is to legitimise the possession of such monies through circulation and this effectively leads to "clean" funds being received in exchange. The term is used for several offences involving the integration of "dirty money", i.e. the proceeds of crime, into the mainstream economy. In addition to the offence of money laundering

Tax Evasion

5.9 The Criminal Finances Act 2017 ("the Act") came into force on 30th September 2017. Part 3 of the Act created two separate corporate offences:

- Failure to prevent facilitation of UK tax evasion, &
- Failure to prevent facilitation of overseas tax evasion.

5.10 The Council would be guilty of an offence if a person commits a UK tax evasion facilitation offence when acting in the capacity of a person associated with the Council.

5.11 Under s45(4) of the Act a UK tax evasion offence means:

- An offence of cheating the public revenue, or
- An offence under the law of any part of the UK consisting of being knowingly concerned in, or in taking steps with a view to, the fraudulent evasion of a tax.

5.12 Under s45(5) of the Act a UK tax evasion facilitation offence means an offence under the law of any part of the UK consisting of:

- Being knowingly concerned in, or in taking steps with a view to, the fraudulent evasion of a tax by another person, or
- Aiding, abetting, counselling or procuring the commission of a UK tax evasion offence, or
- Being involved in the commission of an offence consisting of being knowingly concerned in, or in taking steps with a view to, the fraudulent evasion of a tax.

5.13 Tax evasion is the illegal non-payment or under-payment of taxes, usually resulting from the making of a false declaration or no declaration at all of taxes due to the relevant tax authorities, resulting in legal penalties (which may be civil or criminal) if the perpetrator of tax evasion is caught.

Appendix 1

Identified sources of Fraud Risk for Councils

Fraud, Bribery and Corruption risks associated with Council Services

Tenancy	Fraudulent applications for housing or successions of tenancy, and subletting of the property
Benefits(responsibility of DWP)	False entitlement
Social care fraud	Personal budgets and direct payments Overstatement of needs through false declaration, multiple claims across authorities, third party financial abuse by carer, family or organisation, posthumous continuation of claims
Commissioning of services including joint commissioning, joint ventures, commercial services, third sector partnerships	Conflicts of interest, collusion
Procurement	Tendering issues, split contracts, double invoicing
Payroll	False employees, overtime claims, expenses
Identity fraud	False identity/fictitious persons applying for services/payments
Council tax	Discounts and exemptions, council tax support
Blue Badge	Use of counterfeit/altered badges, use when disabled person is not in the vehicle, use of a deceased person's Blue Badge, badges issued to institutions being misused by employees
Grants	Work not carried out, funds diverted, ineligibility not declared
Business rates	Fraudulent applications for exemptions and reliefs, unlisted properties
Insurance fraud	False claims including slips and trips
Disabled facility grants	Fraudulent applications for adaptions to homes aimed at the disabled
Concessionary travel schemes	Use of concession by ineligible person
No recourse to public funds	Fraudulent claims of eligibility
Right to buy	Fraudulent applications under the right to buy/acquire Money laundering exposure to suspect transactions
Schools	Issues relating to other risk areas can apply to schools
New responsibilities/ Partnership working	Can lend themselves to procurement fraud, grant fraud.
Immigration	False entitlement to services and payments, sham marriages
Cyber-dependent crime	Enables a range of fraud types resulting in diversion of funds, creation of false applications for services and payments.
Employee	Misappropriation of money, equipment, expenses; time recording irregularities

Serious Organised Crime Threats – may be associated with Council Services – please also refer to Appendix 3

- Kidnap and extortion
- Metal theft
- Bogus workmen
- Smuggling
- Payment fraud
- Cyber Attack
- Psychoactive substances
- Drug addiction
- Human trafficking

Money Laundering

Indicators of Money Laundering activity:

- Cash payments over £5,000
- Use of cash where other means of payment are normal
- Overpayments by a customer
- Unusual request for cancellation or reversal of an earlier transaction
- Requests for release of customer account details
- Customer requesting refunds to be transferred overseas, particularly to a highrisk country or tax haven
- Payments of lower amounts where cash is not the usual means of payment
- Use of new/shell companies
- A secretive customer for example one who refuses to provide requested information without a reasonable explanation
- Illogical customer transaction such as unnecessary routing or receipt of funds from third parties or through third party accounts
- Involvement of an unconnected third party without logical reason or explanation
- Absence of an obvious legitimate source of funds
- Concern about the honesty and integrity of the customer
- Unusual transaction or way of conducting business without reasonable explanation Unusual transactions or ways of conducting business
- Individuals and companies which are insolvent yet have funds
- Transaction at substantially above fair market value
- Funds received for deposits or prior to completion from unexpected sources
- Movement of funds to/from overseas particularly from a higher risk country

Tax Evasion

Value Added Tax (VAT):

- Suppliers adding VAT to invoices when not registered for VAT, or the Council paying fraudulent VAT-only invoices. The VAT would be recovered from HMRC so it would not fall as a cost to anyone’s budget. There would have to be collusion between Council officers and the supplier for there to be a criminal offence of tax evasion.

Construction Industry Scheme:

- Suppliers submitting artificially low labour breakdown on their invoices to avoid tax being deducted on the labour element or no tax being deducted at all.

PAYE – Income Tax / National Insurance:

- Failure to deduct income tax and NI at the correct rate.

Off payroll working – IR35:

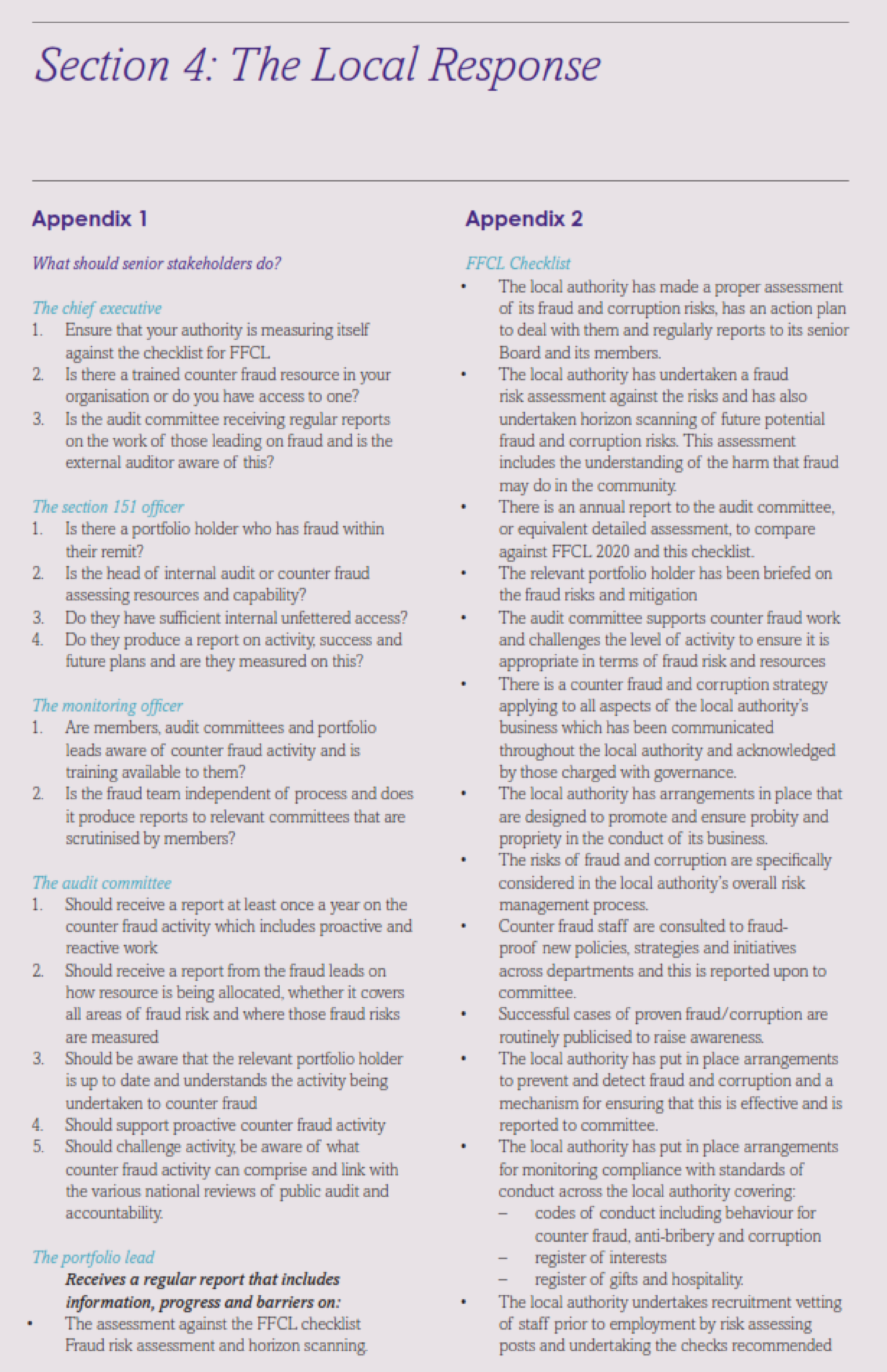
- Failure to identify workers/contractors that should be paid via the payroll.

Direct payments:

- Failure to ensure deduction of Income Tax and National Insurance from payments made to personal assistants by recipients of Direct Care Payments.

Grants:

- Failure to ensure that Grant funding is used for its intended purpose.



Section 4: The Local Response

Appendix 1

What should senior stakeholders do?

The chief executive

1. Ensure that your authority is measuring itself against the checklist for FFCL.
2. Is there a trained counter fraud resource in your organisation or do you have access to one?
3. Is the audit committee receiving regular reports on the work of those leading on fraud and is the external auditor aware of this?

The section 151 officer

1. Is there a portfolio holder who has fraud within their remit?
2. Is the head of internal audit or counter fraud assessing resources and capability?
3. Do they have sufficient internal unfettered access?
4. Do they produce a report on activity, success and future plans and are they measured on this?

The monitoring officer

1. Are members, audit committees and portfolio leads aware of counter fraud activity and is training available to them?
2. Is the fraud team independent of process and does it produce reports to relevant committees that are scrutinised by members?

The audit committee

1. Should receive a report at least once a year on the counter fraud activity which includes proactive and reactive work
2. Should receive a report from the fraud leads on how resource is being allocated, whether it covers all areas of fraud risk and where those fraud risks are measured
3. Should be aware that the relevant portfolio holder is up to date and understands the activity being undertaken to counter fraud
4. Should support proactive counter fraud activity
5. Should challenge activity, be aware of what counter fraud activity can comprise and link with the various national reviews of public audit and accountability.

The portfolio lead

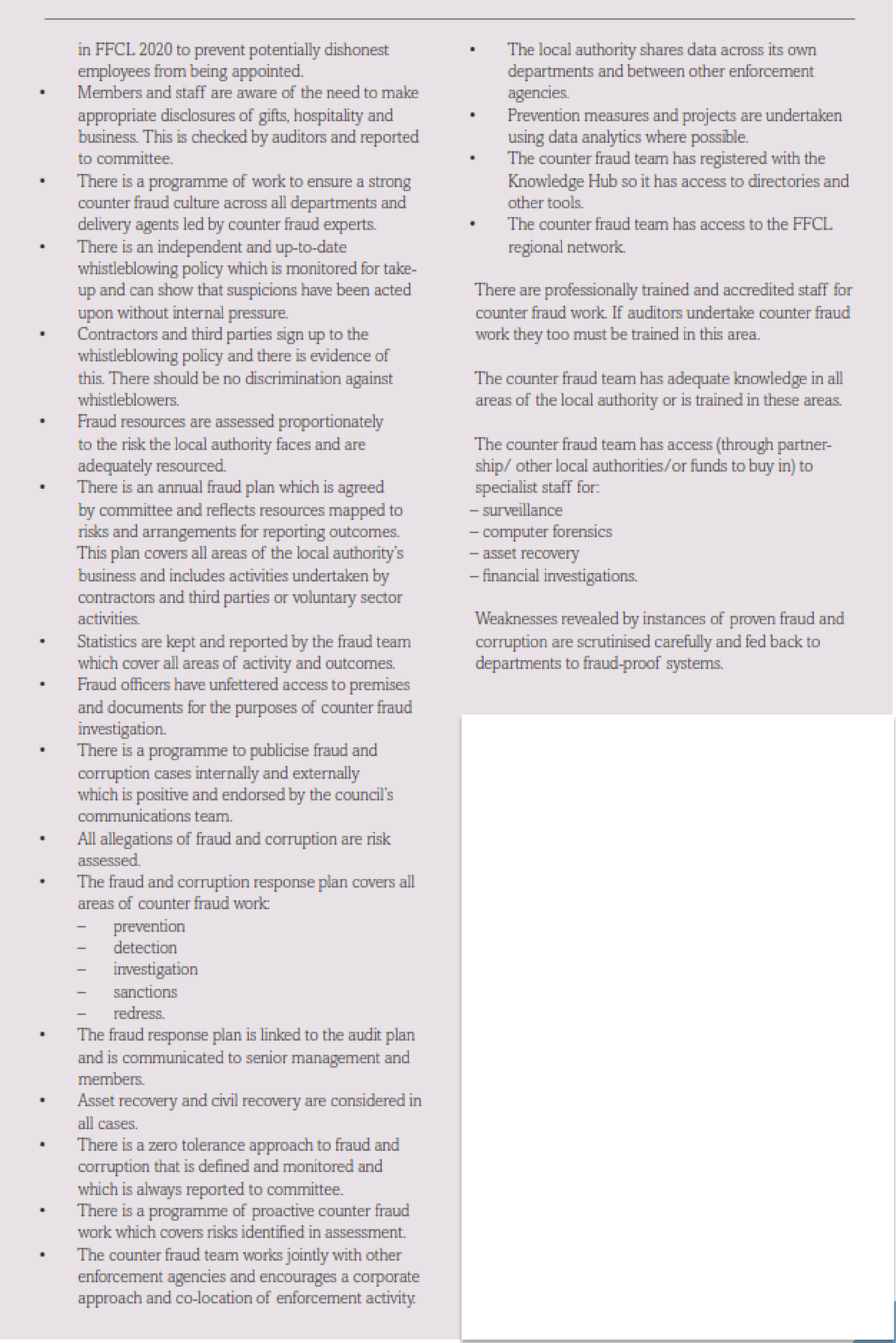
Receives a regular report that includes information, progress and barriers on:

- The assessment against the FFCL checklist Fraud risk assessment and horizon scanning.

Appendix 2

FFCL Checklist

- The local authority has made a proper assessment of its fraud and corruption risks, has an action plan to deal with them and regularly reports to its senior Board and its members.
- The local authority has undertaken a fraud risk assessment against the risks and has also undertaken horizon scanning of future potential fraud and corruption risks. This assessment includes the understanding of the harm that fraud may do in the community.
- There is an annual report to the audit committee, or equivalent detailed assessment, to compare against FFCL 2020 and this checklist.
- The relevant portfolio holder has been briefed on the fraud risks and mitigation
- The audit committee supports counter fraud work and challenges the level of activity to ensure it is appropriate in terms of fraud risk and resources
- There is a counter fraud and corruption strategy applying to all aspects of the local authority's business which has been communicated throughout the local authority and acknowledged by those charged with governance.
- The local authority has arrangements in place that are designed to promote and ensure probity and propriety in the conduct of its business.
- The risks of fraud and corruption are specifically considered in the local authority's overall risk management process.
- Counter fraud staff are consulted to fraud-proof new policies, strategies and initiatives across departments and this is reported upon to committee.
- Successful cases of proven fraud/corruption are routinely publicised to raise awareness.
- The local authority has put in place arrangements to prevent and detect fraud and corruption and a mechanism for ensuring that this is effective and is reported to committee.
- The local authority has put in place arrangements for monitoring compliance with standards of conduct across the local authority covering:
  - codes of conduct including behaviour for counter fraud, anti-bribery and corruption
  - register of interests
  - register of gifts and hospitality.
- The local authority undertakes recruitment vetting of staff prior to employment by risk assessing posts and undertaking the checks recommended



in FFCL 2020 to prevent potentially dishonest employees from being appointed.

- Members and staff are aware of the need to make appropriate disclosures of gifts, hospitality and business. This is checked by auditors and reported to committee.
- There is a programme of work to ensure a strong counter fraud culture across all departments and delivery agents led by counter fraud experts.
- There is an independent and up-to-date whistleblowing policy which is monitored for take-up and can show that suspicions have been acted upon without internal pressure.
- Contractors and third parties sign up to the whistleblowing policy and there is evidence of this. There should be no discrimination against whistleblowers.
- Fraud resources are assessed proportionately to the risk the local authority faces and are adequately resourced.
- There is an annual fraud plan which is agreed by committee and reflects resources mapped to risks and arrangements for reporting outcomes. This plan covers all areas of the local authority's business and includes activities undertaken by contractors and third parties or voluntary sector activities.
- Statistics are kept and reported by the fraud team which cover all areas of activity and outcomes.
- Fraud officers have unfettered access to premises and documents for the purposes of counter fraud investigation.
- There is a programme to publicise fraud and corruption cases internally and externally which is positive and endorsed by the council's communications team.
- All allegations of fraud and corruption are risk assessed.
- The fraud and corruption response plan covers all areas of counter fraud work:
  - prevention
  - detection
  - investigation
  - sanctions
  - redress.
- The fraud response plan is linked to the audit plan and is communicated to senior management and members.
- Asset recovery and civil recovery are considered in all cases.
- There is a zero tolerance approach to fraud and corruption that is defined and monitored and which is always reported to committee.
- There is a programme of proactive counter fraud work which covers risks identified in assessment.
- The counter fraud team works jointly with other enforcement agencies and encourages a corporate approach and co-location of enforcement activity.
- The local authority shares data across its own departments and between other enforcement agencies.
- Prevention measures and projects are undertaken using data analytics where possible.
- The counter fraud team has registered with the Knowledge Hub so it has access to directories and other tools.
- The counter fraud team has access to the FFCL regional network.

There are professionally trained and accredited staff for counter fraud work. If auditors undertake counter fraud work they too must be trained in this area.

The counter fraud team has adequate knowledge in all areas of the local authority or is trained in these areas.

The counter fraud team has access (through partnership/ other local authorities/or funds to buy in) to specialist staff for:

– surveillance
– computer forensics
– asset recovery
– financial investigations.

Weaknesses revealed by instances of proven fraud and corruption are scrutinised carefully and fed back to departments to fraud-proof systems.

Appendix 3

Awareness, Strategy, Guidance and Training,	Have you made your senior management team and Elected Members aware of Scotland's Serious Organised Crime Strategy? If so, how did you do this?
	Do you think that the messages in the Strategy are well embedded across the leadership of your Council?
	What role has your SOC Single Point of Contact had in raising awareness across your Council?
	Do you have an Anti-Fraud and Corruption Strategy and associated Anti-Fraud / Crime procedures? If so, are these up to date, well embedded, and followed in practice?
	How have you disseminated your Council's understanding of the risks of SOC to other stakeholders? For example, across your Community Planning Partners, and to local businesses via your Business Gateway / Economic Development arrangements?
	What training is available to your Council's Officers and Members on the risks associated with SOC?
Risk Management	Have the risks posed by SOC and Corruption been reflected within your Community, Corporate, Service and, where appropriate, Project Risk Registers?
	Has the inclusion of SOC risks within relevant Risk Registers led to any behavioural or process changes within your Council?
	Have you considered the risks posed SOC from a Business Continuity perspective? How would your Council deal with / recover from a scenario involving loss / harm as a result of SOC?
	Does your Council have anti-crime guidance that incorporates arrangements for SOC / corruption related Business Continuity Planning?
Communication and Information / Intelligence Sharing	Do you make any use of technology (e.g., your Council's website, Twitter feed, or Facebook page) to disseminate information on the risks posed by SOC?
	What arrangements do you have in place for both internal and external data sharing? Do you have arrangements in place to share information / intelligence with Police Scotland?
	Do you and / or your SOC Single Point of Contact have regular meetings with Police Scotland to discuss the sharing of information / intelligence?
	What steps has your Council taken to develop minimum standards in relation to data security and online processes to mitigate the threat of cyber-crime?
	Have you made your staff aware of the risks of cyber-crime? If so, how?
	Does your Council's Business Gateway / Economic Development Department provide guidance and information to local businesses on how to protect themselves from the risks of SOC?
	Does your Council's Trading Standards service take an active role in promoting consumer awareness, particularly in relation to the sale of illicit and counterfeit goods (e.g. via website / Twitter, door stop selling initiatives, Trusted Trader Scheme, Scottish Scambusters, etc.)?

Whistle-blowing and Staff Support	Do you have whistle-blowing / confidential reporting arrangements in place? Are these available to staff and other stakeholders (such as suppliers and members of the public)?
	Are your whistle-blowing / confidential reporting arrangements effective (e.g., how many positive outcomes as a result of information received via this channel in the last 12 months)?
	What arrangements do you have in place to protect and support staff who may be working under duress?
Assurance	How do you provide assurance to your Elected Members that you and your management team are aware of, and are managing, the risks posed by SOC?
	What role does your Internal and External Audit teams, and your Monitoring Officer, play in this assurance process?
	Do you capture your arrangements for managing and monitoring the risk of SOC within your Annual Governance Statement?
Licensing (Liquor and Civic)	How confident are you that your Authority has not granted a licence (liquor or civic) to an individual or organisation linked to SOC in the last 12 months? On what basis have you reached this conclusion? Could you please highlight any particularly innovative practice?
External Funding (to 3rd party organisations)	How confident are you that your Authority has not provided funding (cash or 'in kind') to a 3rd party organisation with links to SOC in the last 12 months? On what basis have you reached this conclusion? Could you please highlight any particularly innovative practice?
Development Management (Planning)	How confident are you that no Planning or Development Management decision made by your Council over the last 12 months has been exploited by any individual or organisation with links to SOC? On what basis have you reached this conclusion?
Commercial Property	How confident are you that no property within your Council's Commercial Property Portfolio is being used by, or sub-let to, an individual or organisation with links to SOC On what basis have you reached this conclusion?
Council Housing	How do you obtain assurance that no properties within your Council's Housing stock are being used for the purpose of furthering SOC (e.g., cannabis cultivation, prostitution, sub-letting, people trafficking, counterfeiting)? If your Council's Housing stock has been transferred to another Registered Social Landlord, how do you obtain this assurance?
	Who maintains and repairs your Housing stock?
	If this is done in-house, how do you know that work is not being sub-contracted to organisations with links to SOC?
	If outsourced (or a mix of in-house / out-sourced), how do you know that the organisations you are paying to do that work have no links to SOC?
	How do you make your tenants aware of the risks posed by SOC in the community? How would tenants report their concerns to you?
	How do your Housing Allocations and Homelessness Policies assist with deterring inappropriate use of your Housing stock?
Procurement	Is your Council at risk of purchasing goods or services from organisations with links to SOC? Please explain your response to the question above.

	What steps have you taken to minimise the risk of your Council buying goods and services from organisations with links to SOC?
	What policies or protocols does your Council have in place to ensure that supplier checks aimed at minimising the risk of contracting with an organisation linked to SOC are completed as part of the procurement process?
	To identify (and seek appropriate scrutiny of) high risk contracts, does your Council participate in the National Procurement Portal Notification System and associated Information Sharing Protocol with Police Scotland?
	What have you done to ensure that those members of your staff with purchasing responsibilities are aware of the risks of transacting with an organisation linked to SOC?
	How would staff with purchasing responsibilities raise any potential concerns about organisations with which your Council transacts?
	The Scottish Government launched Scotland's Serious Organised Crime 'Strategy in 2015. Have you made any changes to your Council's procurement arrangements as a result of that?
Insider Threat	Is your Council at risk from employees who have links to SOC? Please explain your response to the question above.
	Listed below are various control mechanisms aimed at minimising the 'Insider Threat' risk. Could you please summarise your Council's arrangements for each (capturing Policies Procedures, and practices)? Officer / Member Vetting (on recruitment and thereafter) Officer / Member External Interests (Extra Mural Employment / Interest) Declarations of Officer / Member Gifts and Hospitality (offered and received) Officer / Member Notifiable Associations (e.g. associations with persons linked to SOC
	How do you know that the arrangements you have set out above are working effectively (e.g., by linking Extra Mural data to absence data) and that records are up to date? Who is responsible and accountable for the effective operation of these processes?
	How would a member of your staff, or another Council stakeholder (e.g., member of the public, supplier, etc.) report suspected or alleged malpractice to you?
	Does your Council have a group tasked with developing, maintaining, and monitoring the corporate Integrity Framework, including the identification of emerging threats, vulnerabilities, risk, opportunities, and relevant mitigation measures to reduce the threat posed by SOC Groups
	How do you challenge and deal with any emerging integrity issues, and how are the outcomes of these fed back into your continuous improvement process?