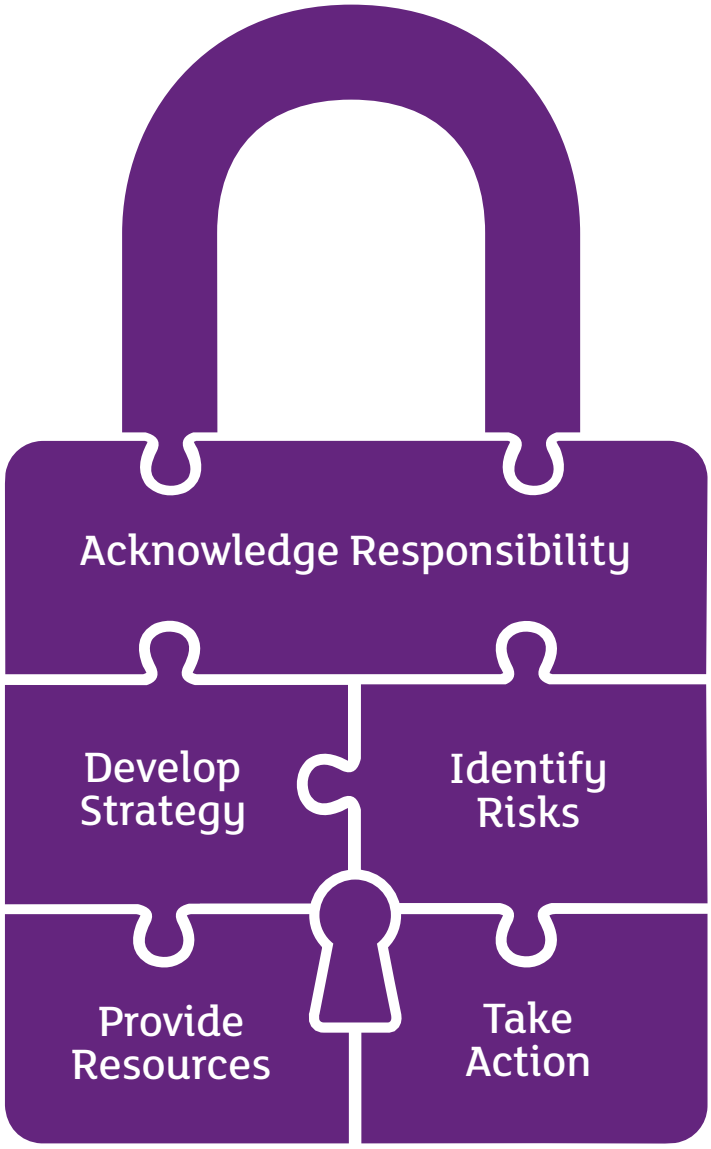
CIPFA The Chartered Institute of Public Finance & Accountancy

Code of practice on

managing the risk of fraud and corruption

Guidance notes



CIPFA COUNTER FRAUD CENTRE

CIPFA, the Chartered Institute of Public Finance and Accountancy, is the professional body for people in public finance. Our 14,000 members work throughout the public services, in national audit agencies, in major accountancy firms, and in other bodies where public money needs to be effectively and efficiently managed. As the world's only professional accountancy body to specialise in public services, CIPFA's qualifications are the foundation for a career in public finance. We also champion high performance in public services, translating our experience and insight into clear advice and practical services. Globally, CIPFA shows the way in public finance by standing up for sound public financial management and good governance.

CIPFA values all feedback it receives on any aspects of its publications and publishing programme. Please send your comments to publications@cipfa.org

Our range of high quality advisory, information and consultancy services help public bodies – from small councils to large central government departments – to deal with the issues that matter today. And our monthly magazine, *Public Finance*, is the most influential and widely read periodical in the field.

Here is just a taste of what we provide:

- TISonline – online financial management guidance
- Benchmarking
- Advisory services
- Professional networks
- Property and asset management services
- Recruitment services
- Research and statistical information
- Seminars and conferences
- Education and training
- CIPFA Regions – UK-wide events run by CIPFA members

Call or visit our website to find out more about CIPFA, our products and services – and how we can support you and your organisation in these unparalleled times.

020 7543 5600
enquiries@cipfa.org
www.cipfa.org

Environmental Information

This CIPFA publication is printed on certified FSC mixed sources coated grade stock containing 50% recovered waste and 50% virgin fibre.

Printed on stock sourced from well-managed forests, ISO 14001.

CIPFA The Chartered Institute of Public Finance & Accountancy

Code of practice on

managing the risk of fraud and corruption

Guidance notes

CIPFA COUNTER FRAUD CENTRE

Published by:

CIPFA \ THE CHARTERED INSTITUTE OF PUBLIC FINANCE AND ACCOUNTANCY

3 Robert Street, London WC2N 6RL

From 1 January 2015, CIPFA will be moving to 77 Mansell Street, London E1 8AN

020 7543 5600 \ publications@cipfa.org \ www.cipfa.org

ISBN 978 1 84508 429 5

Designed and typeset by Ministry of Design, Bath
(www.ministryofdesign.co.uk)

Printed by Trident Printing, London

Acknowledgements

CIPFA would like to thank the following for their work on this publication:

- Alan Day, commissioned author
- Kerry Ace, Finance and Policy Manager, CIPFA
- Diana Melville, Governance Advisor, CIPFA
- Rachael Tiffen, Head of CIPFA Counter Fraud Centre

Members of the Counter Fraud Advisory Panel:

- Alan Bryce, Audit Commission
- Simon Maddocks, London Borough of Croydon
- Paul Tiffen, NHS Protect

Contents

CHAPTER 1

Introduction

Fraud and corruption are ever present risks to all organisations, be they public, private or not-for-profit. Fraud and corruption can have a significant negative impact on organisations through disruption to their services or undermining the achievement of their objectives. Official estimates[1] have assessed the value of fraud loss in the public sector to be significant. Despite the risk, identifying adequate resource to manage the risk is a challenge for many across the public services.

To help organisations recognise and address their fraud risks, CIPFA has produced a Code of Practice on Managing the Risk of Fraud and Corruption ("the Code") which consists of five principles:

- Acknowledge the responsibility of the governing body for countering fraud and corruption.
- Identify the fraud and corruption risks.
- Develop an appropriate counter fraud and corruption strategy.
- Provide resources to implement the strategy.
- Take action in response to fraud and corruption.

CIPFA has built on its previous guidance, *Managing the Risk of Fraud, Actions to Counter Fraud and Corruption (Red Book)* (2008), to establish a high level set of principles that can be applied to any public service organisation. The Code together with these guidance notes replace CIPFA's previous guidance.

These guidelines are designed to assist organisations in the implementation of the Code. CIPFA considers it important that organisations tailor their approach to implementing the principles, reflecting different fraud risks and challenges and the governance requirements of their sector. Ultimately, however, all public service organisations share common goals of protecting public assets, acting in the public interest and making best use of their resources to achieve their intended outcomes. This is why CIPFA believes a common set of principles across the public services is a step forward in improving counter fraud practice.

These guidance notes provide the opportunity to consider a range of approaches to implementing the Code and to share examples of good practice. In addition, each principle has a sector interpretation to highlight where different circumstances, governance or accountabilities might need to be taken into account when planning the implementation of the Code. The guidance notes are written to support organisations putting in place counter fraud arrangements for the first time but will also be of benefit to practitioners seeking to review or refresh their existing arrangements.

1. The National Fraud Authority's Annual Fraud Indicator (2013) estimated the fraud loss in the public sector at around £20bn.

The guidance notes contain the Code, followed by five chapters, each one dealing with one of the principles from the Code. The chapters first establish the context, providing an explanation of the importance of the Code principle. Each chapter then provides sector interpretation, including pointers to relevant sector guidance or requirements. Finally there is more detailed guidance on how to apply each principle of the Code in practice. This includes examples and suggestions of good practice approaches.

There has been a period of significant change affecting the national guidance and resources to counter fraud. CIPFA will continue to provide support for counter fraud practitioners through the Counter Fraud Centre, which will include an assessment tool based on the Code.

CHAPTER 2

Code of Practice on Managing the Risk of Fraud and Corruption

CODE OF PRACTICE PRINCIPLES

Leaders of public services organisations have a responsibility to embed effective standards for countering fraud and corruption in their organisations. This supports good governance and demonstrates effective financial stewardship and strong public financial management.

The five key principles of the Code are to:

- acknowledge the responsibility of the governing body for countering fraud and corruption
- identify the fraud and corruption risks
- develop an appropriate counter fraud and corruption strategy
- provide resources to implement the strategy
- take action in response to fraud and corruption.

A Acknowledge responsibility

The governing body should acknowledge its responsibility for ensuring that the risks associated with fraud and corruption are managed effectively across all parts of the organisation.

Specific steps should include:

A1 The organisation's leadership team acknowledge the threats of fraud and corruption and the harm they can cause to the organisation, its aims and objectives and to its service users.

A2 The organisation's leadership team acknowledge the importance of a culture that is resilient to the threats of fraud and corruption and aligns to the principles of good governance.

A3 The governing body acknowledges its responsibility for ensuring the management of its fraud and corruption risks and will be accountable for the actions it takes through its governance reports.

A4 The governing body sets a specific goal of ensuring and maintaining its resilience to fraud and corruption and explores opportunities for financial savings from enhanced fraud detection and prevention.

B Identify risks

Fraud risk identification is essential to understand specific exposures to risk, changing patterns in fraud and corruption threats and the potential consequences to the organisation and its service users.

Specific steps should include:

B1 Fraud risks are routinely considered as part of the organisation's risk management arrangements.

B2 The organisation identifies the risks of corruption and the importance of behaving with integrity in its governance framework.

B3 The organisation uses published estimates of fraud loss, and where appropriate its own measurement exercises, to aid its evaluation of fraud risk exposures.

B4 The organisation evaluates the harm to its aims and objectives and service users that different fraud risks can cause.

C Develop a strategy

An organisation needs a counter fraud strategy setting out its approach to managing its risks and defining responsibilities for action.

Specific steps should include:

C1 The governing body formally adopts a counter fraud and corruption strategy to address the identified risks and align with the organisation's acknowledged responsibilities and goals.

C2 The strategy includes the organisation's use of joint working or partnership approaches to managing its risks, where appropriate.

C3 The strategy includes both proactive and responsive approaches that are best suited to the organisation's fraud and corruption risks. Proactive and responsive components of a good practice response to fraud risk management are set out below.

Proactive

- Developing a counter fraud culture to increase resilience to fraud.
- Preventing fraud through the implementation of appropriate and robust controls and security measures.
- Using techniques such as data matching to validate data.
- Deterring fraud attempts by publicising the organisation's anti-fraud and corruption stance and the actions it takes against fraudsters.

Responsive

- Detecting fraud through data and intelligence analysis.
- Implementing effective whistleblowing arrangements.
- Investigating fraud referrals.

- Applying sanctions, including internal, disciplinary, regulatory and criminal.
- Seeking redress, including the recovery of assets and money where possible.

C4 The strategy includes clear identification of responsibility and accountability for delivery of the strategy and for providing oversight.

D Provide resources

The organisation should make arrangements for appropriate resources to support the counter fraud strategy.

Specific steps should include:

D1 An annual assessment of whether the level of resource invested to counter fraud and corruption is proportionate for the level of risk.

D2 The organisation utilises an appropriate mix of experienced and skilled staff, including access to counter fraud staff with professional accreditation.

D3 The organisation grants counter fraud staff unhindered access to its employees, information and other resources as required for investigation purposes.

D4 The organisation has protocols in place to facilitate joint working and data and intelligence sharing to support counter fraud activity.

E Take action

The organisation should put in place the policies and procedures to support the counter fraud and corruption strategy and take action to prevent, detect and investigate fraud.

Specific steps should include:

E1 The organisation has put in place a policy framework which supports the implementation of the counter fraud strategy. As a minimum the framework includes:

- Counter fraud policy
- Whistleblowing policy
- Anti-money laundering policy
- Anti-bribery policy
- Anti-corruption policy
- Gifts and hospitality policy and register
- Pecuniary interest and conflicts of interest policies and register
- Codes of conduct and ethics
- Information security policy
- Cyber security policy.

E2 Plans and operations are aligned to the strategy and contribute to the achievement of the organisation's overall goal of maintaining resilience to fraud and corruption.

E3 Making effective use of national or sectoral initiatives to detect fraud or prevent fraud, such as data matching or intelligence sharing.

E4 Providing for independent assurance over fraud risk management, strategy and activities.

E5 There is a report to the governing body at least annually on performance against the counter fraud strategy and the effectiveness of the strategy from the lead person(s) designated in the strategy. Conclusions are featured in the annual governance report.

Applying the code in practice

Where organisations are making a statement in an annual governance report about their adherence to this code, one of the following statements should be approved according to whether the organisation conforms with the code or needs to take further action. The statement should be approved by the governing body and signed by the person responsible for signing the annual governance report.

Statement 1

Having considered all the principles, I am satisfied that the organisation has adopted a response that is appropriate for its fraud and corruption risks and commits to maintain its vigilance to tackle fraud.

Or

Statement 2

Having considered all the principles, I am satisfied that, subject to the actions identified below, the organisation has adopted a response that is appropriate for its fraud and corruption risks and commits to maintain its vigilance to tackle fraud.

Actions to be taken to manage the risk of fraud:

Action:	Responsibility:	Target date:

CHAPTER 3

Acknowledge Responsibility

CIPFA CODE OF PRACTICE PRINCIPLE A

The governing body should acknowledge its responsibility for ensuring that the risks associated with fraud and corruption are managed effectively across all parts of the organisation.

CONTEXT

This section looks at the important role the governing body and senior executives have in establishing an effective response to the risks of fraud. CIPFA considers it essential for an organisation to acknowledge responsibility for protecting itself and its services from the harm caused by fraud and corruption.

The leaders of an organisation should formally accept this responsibility and publicise this to demonstrate their leadership. This helps to build confidence among staff, stakeholders and the general public that fraud risks are taken seriously and action will be taken to address them. The organisation's leaders will be members of the governing body or the organisation's executive management team, examples include cabinet members, chair of the board, accounting officer, chief executive, executive directors, vice-chancellor, principal or headteacher. Acknowledging responsibility also provides both management and counter fraud professionals with the authority to ensure that fraud and corruption risks are identified and managed correctly.

In addition to the governing body providing a high level of support to counter fraud activity, it is also recommended that there should be four levels of authority within an organisation with respect to fraud and corruption risk management:

1. **Chief executive and senior management level**

   Leadership from the very top is essential if fraud and corruption risk management is going to be taken seriously by the whole organisation. "Top level buy-in" needs to be explicit and disseminated throughout the organisation.

2. **Accountable person**

   This position should oversee the implementation of the counter fraud and corruption strategy and ensure that it is put into practice. It is essential that this position is able to have delegated authority for decisions. Appendix D includes a suggested list for most organisation types in the public services.

3. **Counter fraud team**

   This may be large or small according to the size of the organisation and may be outsourced. It may also be a stand-alone team or possibly a role combined with other advisory functions, such as internal audit, particularly for preventative actions. Increasingly the counter fraud activity is being shared between organisations.

4. **Independent review and compliance**

   This could be achieved by an internal audit review reporting to the audit committee and also by external auditors and regulators. The audit committee is likely to include responsibilities in relation to counter fraud in its terms of reference.

There is a strong relationship between good governance and counter fraud and corruption. At its most basic level most people would recognise the need for appropriate policies and procedures to prevent or investigate fraud and corruption as part of an organisation's governance arrangements. There is also a clear link to ethical standards and codes of conduct, as articulated in the Seven Principles of Public Life (the Nolan Principles). The Seven Principles were originally established by the Committee on Standards in Public Life in its first report published in 1995. The current definition of the principles can be found in Committee on Standards in Public Life – A Review of Best Practice in Promoting Good Behaviour in Public Life (2013).

A framework of good governance means more than having the right policies and procedures in place. Likewise an effective counter fraud and corruption approach requires more than policies and procedures to be successful. The Code aims to align its principles of good counter fraud and corruption practice with the principles of good governance. It should therefore be easier to communicate and embed the principles of the Code alongside other guidance.

Across the public services there are a number of codes of corporate governance. The most up-to-date thinking on good governance for the public sector is the new International Framework: Good Governance in the Public Sector (2014), developed jointly by CIPFA and the International Federation of Accountants (IFAC). This builds on The Good Governance Standard for Public Services developed in 2004 by CIPFA and the Office for Public Management (OPM), with support from the Joseph Rowntree Foundation. Sector specific codes are also important, as is the UK Corporate Governance Code, issued by the Financial Reporting Council for listed companies.

It is in the new International Framework that there are the clearest links to the principles in the Code. The International Framework states:

Governance comprises the arrangements put in place to ensure that the intended outcomes for stakeholders are defined and achieved.

The fundamental function of good governance in the public sector is to ensure that entities achieve their intended outcomes while acting in the public interest at all times.

Good governance is characterized by robust scrutiny, which places important pressures on improving public sector performance and tackling corruption.

When considering the Code against the International Framework there are two clear messages: the importance of achieving intended outcomes and acting in the public interest

and being seen to do so. It is clear from the outset that good governance cannot be achieved if the fraud and corruption risks faced by the entity are unacknowledged or inadequately addressed.

Example:

The intended outcome of providing social housing is that it provides an affordable home to a family in need. If fraud takes place, for example a unit is sub-let to someone else, then the opportunity to use that house to meet another's housing need is lost.

Appendix B contains a detailed mapping of the links between the principles in the Code and the governance principles in the International Framework.

Governance reports, such as the governance statement, are used to:

- demonstrate how the organisation has put in place robust governance arrangements and assess how well they have operated over the previous year
- set out plans for future improvement.

CIPFA's Delivering Good Governance in Local Government: Framework (Addendum) (2012), which provides guidance on annual governance statements in local government, clearly points to the review of counter fraud arrangements as part of this annual review. Going forward CIPFA would recommend that the Code is used as a basis for assessment and for reporting in the governance statement. CIPFA will take account of this in future reviews and updates to its guidance on governance statements.

SECTOR INTERPRETATION

The framework of good governance adopted by the organisation should support the Code, and it should be possible to make clear linkages between the two. Appendix C includes a map of the counter fraud code against leading governance codes currently in use in the public services. This resource should enable linkages to be made to an organisation's current code of governance. A review of Appendix C will highlight that counter fraud and corruption is not always clearly identified within existing governance codes. CIPFA recommends that the appropriate regulators should consider the alignment when updating or replacing the current governance codes.

Codes of conduct usually set out the responsibilities of the employee or member of the governing body to behave in accordance with ethical standards, such as the Standards in Public Life, and to exercise stewardship over public money, assets and data. Thus all public service employees and governors have a responsibility for the prevention, detection and reporting of fraud and corruption. Examples are given below:

- In the NHS, all managers aim to ensure all NHS officers are aware of fraud, bribery and corruption (economic crime) risks and NHS officers are required to report any suspicions of economic crime as soon as they become aware of them. For more information see NHS Protect's Standards for Providers 2014/15: Fraud, Bribery and Corruption.

- Within charities, the Charity Commission's Compliance Toolkit states that 'staff and volunteers should know how to report their concerns within the organisation, including concerns about the conduct of trustees or senior managers'.
- Other public sector organisations have similar requirements. For example, Transport for London's *Anti-Fraud and Corruption Policy* states 'every member of staff has a responsibility to report details immediately to their employing manager if they suspect that fraud or corruption has been, is being or may be committed'. Many local authorities have similar wording in their policies.

Different sectors will have differing forms of governance and governing bodies. Thus the terms governing body, board or audit committee may have different meanings to various organisations. In general, leaders of an organisation will be members of the governing body or the organisation's executive management team. Examples include cabinet members, chair of the board, accounting officer, chief executive, executive directors, vice-chancellor, principal or headteacher.

Appendix D includes a list of public service organisations and suggested governing bodies and accountable officers. In some cases responsibility is clearly identified in existing guidance. For example, Managing Public Money (HM Treasury, 2013) identifies the accounting officer as responsible for managing the organisations' risks, including fraud risks. Those organisations that need to abide by *Managing Public Money*, including central government departments, agencies and academies, will identify their accounting officer as the accountable officer. In higher education the principal or vice-chancellor is designated accountable officer, which is a mandatory requirement. The CIPFA Statement on the Role of the Chief Financial Officer in Local Government identifies the core responsibilities of the chief financial officer and this includes implementing appropriate measures to prevent and detect fraud and corruption.

Whatever the sector, the governing body and those with counter fraud responsibilities should be clearly identified and defined.

GOOD PRACTICE GUIDANCE

CIPFA CODE OF PRACTICE PRINCIPLE A1

The organisation's leadership team acknowledge the threats of fraud and corruption and the harm they can cause to the organisation, its aims and objectives and to its service users.

An organisation's leadership needs to fully understand and acknowledge the threats of fraud and corruption faced, and the harm they can cause to their organisation. For example this acknowledgement could be highlighted in public documents such as policy statements, strategies and annual reports.

An effective organisation will have a counter fraud and corruption strategy and policy which is approved and supported by the organisation's leadership team and which is communicated effectively. There are many ways to ensure wide distribution of polices such as including them in induction training, regular referrals at team meetings or including in leadership briefings.

It is good practice for the responsibilities for managing the risk of fraud and corruption to be included in the organisation's scheme of delegation or terms of reference.

Example:

A local council appointed one councillor as an "Anti-fraud Tsar". This provided senior political leadership for an authority wide, integrated and co-ordinated response across all cabinet portfolios. This provided a conduit for front line services to decision makers as part of a joined-up approach to countering fraud. The first initiative under this scheme detected over £200,000 of housing benefit fraud.

CIPFA CODE OF PRACTICE PRINCIPLE A2

The organisation's leadership team acknowledge the importance of a culture that is resilient to the threats of fraud and corruption and aligns to the principles of good governance.

There are a number of ways that the organisation's leadership team can support a counter fraud culture:

- Providing visible support for counter fraud and corruption activity.
- Recognising the risk of fraud and corruption and the harm it can cause to the organisation and to those the organisation helps and/or protects.
- Including reference to counter fraud and corruption activities in the principles of good governance and standards of conduct adopted by the organisation. In order to assist this, Appendix C provides guidance on the alignment of the Code against current governance frameworks in use in the public services.
- Ensuring the organisation is responsive to new fraud and corruption risks.
- Embedding strong counter fraud controls and systems within the organisation.
- Providing visible support and resourcing for fraud awareness activity.
- Supporting counter fraud and corruption training throughout the organisation and at all levels. The adoption of the Code could be publicised as part of this training.
- Ensuring that other governance papers, strategies and policies include fraud and corruption risks wherever relevant.

CIPFA CODE OF PRACTICE PRINCIPLE A3

The governing body acknowledges its responsibility for ensuring the management of its fraud and corruption risks and will be accountable for the actions it takes through its governance reports.

Formal adoption of this Code by the organisation will be a robust commitment by the governing body to the management of its fraud and corruption risks. The governing body should ensure that there is a clear programme of work in accordance with the Code to manage the risk of fraud and corruption.

The organisation's leadership team can also provide strong and genuine support by delegating appropriate authority to counter fraud professionals. The leadership team can also acknowledge these threats by providing their support to counter fraud and corruption

measures, by providing resources appropriate to the risks and by reporting on the management of the risks to the governing body or audit committee.

This support, however, needs to be clearly laid out along with the expected outcomes in the organisation's strategies, policies and procedures. All senior managers in an organisation can be given a responsibility for fraud risk management in their particular area of the organisation and this could be included in their job description.

The governing body should also identify how accountability will be demonstrated. For example the publication of annual governance reports could include a statement about the level of adherence to the Code. The review can also report on whether this work is being effectively and efficiently implemented and how the organisation is benefiting from successful fraud and corruption risk management.

CIPFA CODE OF PRACTICE PRINCIPLE A4

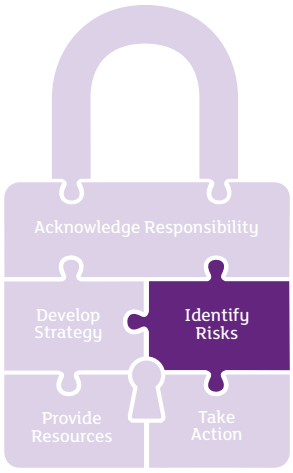
The governing body sets a specific goal of ensuring and maintaining its resilience to fraud and corruption and explores opportunities for financial savings from enhanced fraud detection and prevention.

This can be achieved by the organisation having a clear programme of work to manage fraud and corruption risks with specific goals as set out in a counter fraud and corruption strategy (see Section C of the Code and Chapter 5 of the Guidance Notes).

The programme of work will be proportionate to the size of the organisation and the risk it faces but could include:

- a formal fraud risk management process
- the production, maintenance and review of a fraud strategy
- formal fraud awareness activity and
- clear directions on actions to be taken if fraud or corruption is discovered.

The programme of work should be regularly reviewed to focus on new or increasing fraud risks identified as part of the organisation's risk management work. Where fraud prevention or detection opportunities are identified that could result in financial savings, then the benefits should be evaluated.



CHAPTER 4

Identify Risks

CIPFA CODE OF PRACTICE PRINCIPLE B

Fraud risk identification is essential to understand specific exposures to risk, changing patterns in fraud and corruption threats and the potential consequences to the organisation and its service users.

CONTEXT

Fraud and corruption risks should be considered as business risks and managed as part of the organisation's risk management process. ISO 31000:2009 – Risk Management Principles and Guidelines defines risk management as 'coordinated activities to direct and control an organisation with regard to risk'. The systematic process of understanding, evaluating and addressing risks maximises the chances of objectives being achieved and helps organisations ensure they are sustainable.

Effective risk management requires an informed understanding of relevant risks, an assessment of their relative priority and a rigorous approach to monitoring and controlling them. To be effective, risk management needs be proportionate to the size and nature of an organisation.

Fraud and corruption risk management is an important part of planning for all organisations. The process of risk management is designed to reduce or eliminate the risk of fraud and corruption happening or having a detrimental impact on the business. Successful fraud and corruption risk management will help an organisation focus on three objectives to reduce the harm and effect that fraud and corruption have on an organisation and those it is there to help. These objectives are as follows:

1. **Prevention and deterrence**
   Risk management will help you to target the organisation's resources at the right areas to prevent fraud occurring.
2. **Detection**
   Risk management will highlight those areas prone to fraud and corruption risks and again help you target your detection resources at the right areas.
3. **Response**
   Using a proactive risk management methodology means that if a fraud does occur, you can take corrective action, minimise losses and help prevent further frauds.

Unless an effective risk management methodology is used, an organisation will not be able to identify its areas of vulnerability and valuable resources and time may be used in the wrong areas.

External auditors are required to obtain an understanding of the entity they are auditing, including its internal controls. To meet international auditing standards external auditors will consider the extent of management's own assessment of the risk of fraud and the controls in place to prevent and detect it. Guidance on the responsibilities of external auditors is available in the International Standard on Auditing (UK and Ireland) 240 (Financial Reporting Council).

SECTOR INTERPRETATION

An organisation's risk management approach should take into account any recommended approaches for the sector or any regulatory requirements. Public bodies that need to adhere to Managing Public Money (HM Treasury, 2013) should take account of its Annex 4.9. This states that fraud should always be considered as a risk for the department's risk register. Further links to HM Treasury publications are included in Appendix E.

The approach to risk identification must be proportionate to its size and should also take account of the activities of the organisation. There are however many fraud risks which are generally applicable. CIPFA has produced a list of generic fraud types which can be used as a starting point for organisations that have not yet undertaken a fraud risk identification exercise. This is available to download from the CIPFA website.

To identify other fraud types that might be specific to a sector or organisation type, Appendix E includes resources that will facilitate this. For example, to some organisations procurement fraud will be a greater risk than to others and some fraud types may only be applicable to some organisation types.

An organisation needs to consider all risks and through this process can make an informed decision to accept a certain level of risk. For example, within charities fraud and financial crime can occur at any point within the charity's operations from income generation to the disbursements of funds. The types and levels of fraud will differ between charities so they need to be aware of the risks to which they individually may be vulnerable through a thorough risk assessment.

GOOD PRACTICE GUIDANCE

The starting point for risk identification is to adopt a clear definition of fraud and corruption. There are many definitions of fraud but the Serious Fraud Office states that:

Fraud is a type of criminal activity, defined as an abuse of position, or false representation, or prejudicing someone's rights for personal gain. Put simply, fraud is an act of deception intended for personal gain or to cause a loss to another party.

The many definitions of fraud all include reference to an act of "deception" and the Fraud Act 2006 (while not providing a clear definition of the term fraud) states that, for there to be fraud, the fraudster must intend to 'make a gain for himself or another, or cause loss to another or to expose another to a risk of loss'. The 2006 Act further states that this must be conducted in a dishonest way.

Corruption also has a number of definitions. Transparency International states that corruption is 'the abuse of entrusted power for private gain'. The Bribery Act 2010: Quick Start Guide (Ministry of Justice) defines bribery as 'giving someone a financial or other advantage to encourage that person to perform their functions or activities improperly or to reward that person for having already done so. So this could cover seeking to influence a decision-maker by giving some kind of extra benefit to that decision maker rather than by what can legitimately be offered as part of a tender process'. The World Bank defines corruption simply as 'the abuse of public office for private gain'. Organisations should adopt clear and concise definitions of fraud and corruption and ensure these are included in all appropriate documentation.

CIPFA CODE OF PRACTICE PRINCIPLE B1

Fraud risks are routinely considered as part of the organisation's risk management arrangements.

Fraud risks can be integrated into the organisation's risk management arrangements, allowing them to be owned in the same way as other risks. Risk owners should be supported by the nominated counter fraud person/team.

Fraud risk identification can be achieved in a number of ways, including the following:

- Compare your identified risks with other similar organisations.
- Conduct fraud risk workshops within departments. This approach can make best use of the detailed knowledge of the staff operating policies and processes.
- Use internal auditors, external auditors or a specialist consultant to conduct a fraud risk review.
- Use external reference material that identifies current risks experienced by a particular sector. For example, the Audit Commission's Protecting the Public Purse reports identify the frauds experienced by local authorities in England.

Example:

A local council's internal audit department conduct an annual fraud risk assessment which is governed by a formal risk methodology. The assessment covers all of the operations of the council to identify inherent fraud risks. An assessment is then undertaken to identify the likelihood and significance of each inherent fraud risk as well as the existing control environment to highlight any residual risks.

Audit activity is focused on those areas where residual risks have been identified and is included in the council's counter fraud work plan. Follow-up reviews are carried out to ensure that all control weaknesses have been addressed. The counter fraud work plan may be changed in year to focus on new or emerging fraud threats identified as part of information sharing and intelligence.

Fraud and corruption risk management needs to address the following:

- Identify each fraud and corruption risk. This includes defining the risk type and its source. This could include third party risks if they are significant. For example, a fraud experienced by a key supplier could impact on their ability to deliver essential services on your behalf or result in harm to your service users.

- Identify any enablers that may not be fraud and corruption risks in their own right but can assist in the perpetration of fraud. An example may be the failure to fully implement and maintain access controls in an ICT system. This could assist a fraudster in gaining unauthorised access to a system and enable them to commit fraud. Ensure that new processes and procedures cannot be used by criminals as enablers to fraud and corruption.
- Identify the risk owner:
  - It is best if this is within the department responsible for that particular process, eg HR, procurement, finance.
  - The risk owner needs to have the knowledge and the authority to manage the risk effectively.
  - Ensure that there are no gaps in the management of the risks.
- Analyse the risk:
  - Risks can then be prioritised taking into account both likelihood and potential impact.
  - It may be possible to group risks into specific categories which may make the management of these risks easier. For example, analysis may identify links between procurement and finance risks in a specific function.
- Identify mitigations and controls:
  - Analysing mitigations and controls can identify gaps in an organisation's processes.
  - This can aid proactive detection work through data analytics and continuous auditing.
  - It is possible that mitigations for a risk may not be in the same department as the risk owner and thus internal departmental co-operation is vital.
- Have an action plan and responsible person, with specific timelines and reporting processes:
  - The risk register should identify what action is to be taken, by whom and by when.
  - The risk register can be used as a reference document by the risk owner to ensure the right action is being taken.
  - The risk register can also be used by other staff to identify the risk owner if they identify fraud and corruption issues.
- Follow up with regular risk management meetings. The risk register should be regularly reviewed, risk owners called to account and any problems with implementing the action plan identified. A collaborative approach to fraud risk management should be encouraged.

Additional guidance on conducting fraud risk assessments can be found in Fighting Fraud Locally – A Good Practice Guide for Assessing Fraud Risks.

CIPFA CODE OF PRACTICE PRINCIPLE B2

The organisation identifies the risks of corruption and the importance of behaving with integrity in its governance framework.

There should be specific links between counter fraud and corruption policies and other ethical policies, such as codes of conduct and gifts and hospitality policies. These would normally be applicable to all staff as well as contractors, consultants and agency staff. Members of the governing body will also have codes covering ethical conduct and these should also include links to counter fraud and corruption policies.

It should be stressed in any policies that the management of fraud and corruption risks is the responsibility of the whole organisation and not just the counter fraud and corruption team.

CIPFA CODE OF PRACTICE PRINCIPLE B3

The organisation uses published estimates of fraud loss, and where appropriate its own measurement exercises, to aid its evaluation of fraud risk exposures.

A number of organisations publish estimates of fraud losses on a regular basis, some of which are specific to the public sector or focus on a particular fraud type. While these estimates can never be wholly accurate they do help understanding of the scale of the fraud risk and can identify trends in different types of fraud exposures. The organisation can use these estimates of fraud loss and any measurement exercises to quantify the potential losses that different fraud risks cause.

Clear identification of a fraud and corruption risk can:

- identify the financial loss should that risk not be managed correctly
- assist in the calculation of potential savings through preventative work
- provide a method of calculating the monetary equivalent of frauds identified where it is not easily apparent, for example the loss estimated for social housing fraud is based on the additional costs of using temporary accommodation.

If an organisation has clear definitions of fraud and corruption and risks have been identified, an organisation can consider adopting a method of fraud loss measurement. Loss measurement can be difficult and is not an exact science. For fraud losses, some organisations simply extrapolate known losses for a certain period and calculate what the cost would be for a particular period of time if the fraud had not been identified. For fraud prevention, it may be possible to compare your organisation's losses against other similar organisations. Whatever process or type of calculation is chosen, this needs to be approved and used consistently so that effective year on year comparisons can be made. Thus it is essential that a robust and accurate methodology is selected.

Fraud risk management can be helped and supported by use of the following:

- **Data analytics**

  Data analytics provide a capability where an organisation can extract, analyse, interpret and transform its data to not only detect potential instances of fraud but also to identify specific risks. Data analytics can then also be used to implement effective fraud risk monitoring programmes.

- **Specific fraud audits**

  Specific audits to identify fraud risks and examine the mitigations in place can help not only to prevent but also to detect fraudulent activity. Examples of such audits could be a

review of the segregation of duties when an organisation has undergone a reorganisation or reduced staffing levels.

- **Continuous auditing**

  Continuous auditing uses automation to perform control and risk assessments on a more frequent basis. Technology plays a key role in continuous audit activities by helping to automate the identification of exceptions or anomalies, analyse patterns within the digits of key numeric fields, review trends and test controls. Continuous auditing is a valuable tool in the management of fraud risks as it can automatically highlight exceptions which could be early indicators of fraudulent activity.

- **Compliance audits**

  These are audits to ensure that the organisation is following regulations and processes which include preventative controls, such as financial regulations. They can be used to assess whether the organisation is exposing itself to fraud and corruption risks by not following such regulations.

- **Targeted awareness campaigns**

  Through a robust risk assessment process or following an investigation, an organisation can identify areas of concern and target those specific areas for awareness campaigns; examples could be the finance department following an account mandate fraud or the procurement department if there is to be a planned increase in spend on a major project. Through such targeted campaigns, awareness of staff will be increased and greater emphasis will be placed on fraud prevention and risk identification.

- **Counter fraud tests exercises**

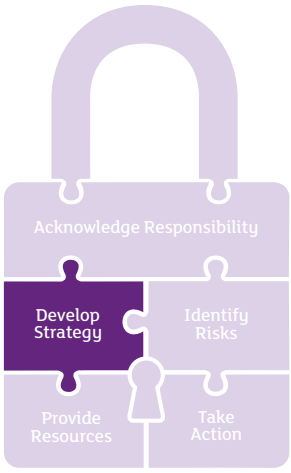
  As new technology and practices come into place, it is essential that they are "fraud tested" to ensure that they do not pose an additional threat and, if so, ensure mitigations are in place before implementation. Just as there is "security by design", think how fraud can be "designed out" of organisations' processes. This is also applicable to third party suppliers who may have access to an organisation's systems and processes, such as payroll processing or ICT system support.

CIPFA CODE OF PRACTICE PRINCIPLE B4

The organisation evaluates the harm to its aims and objectives and service users that different fraud risks can cause.

Published reports on detected fraud may provide examples of the harm that fraud could cause. Harm can be identified in a number of ways. There could be reputational damage to the organisation or individuals, potentially resulting in a loss of confidence in the organisation among the public or stakeholders. Harm can also be identified as damage to specific service objectives. For example, if disabled parking permits are perceived to be regularly abused, it could lead to further abuse of disabled parking places, thus further undermining the effectiveness of the permit policy objectives.

There is also likely to be an adverse effect on staff morale and their commitment to good counter fraud practice. If staff see that a fraud risk is not managed correctly, this will do little to cultivate a good counter fraud ethos in an organisation.



CHAPTER 5

Develop a Strategy

CIPFA CODE OF PRACTICE PRINCIPLE C

An organisation needs a counter fraud strategy setting out its approach to managing its risks and defining responsibilities for action.

INTRODUCTION

Most organisations will have strategies in place to help them achieve their business objectives. The value of a specific counter fraud strategy is that it helps the organisation to focus on the management of fraud risks and ensures the actions have the support of the leadership team.

A clearly defined strategy, approved at the highest level and focused on outcomes, is essential if the risk of fraud and corruption is to be taken seriously in an organisation. A strategic plan is a key part of establishing a counter fraud and corruption culture within an organisation. It provides the opportunity to be explicit about the organisation's approach and makes clear the support of the leadership team.

Where an organisation has set an overall goal to improve its resilience to fraud, as recommended by A4 of the Code, the strategy sets out how the organisation plans to achieve this goal. A strategy can also set specific aims and goals and these can then be measured by the organisation to see how effective its fraud and corruption risk management processes are, and whether the harm and losses caused by fraud are being reduced.

Without such a strategy, there may not be clear direction to all staff including leaders, senior management, staff and indeed the counter fraud team. Thus, a strategy can help an organisation to identify risks, prioritise resources and help to measure the effectiveness of controls.

SECTOR INTERPRETATION

The level and detail of a counter fraud and corruption strategy should be proportionate to the size and activities of an organisation and the risks it faces. There will be some generic aspects such as:

- responsibility
- aims and objectives
- action plan for awareness, prevention and investigation

- review and assessment.

Use of national or sector strategies can help the organisation to establish its own aims or prioritise its actions. For example, local government organisations in England can refer to Fighting Fraud Locally: The Local Government Fraud Strategy (National Fraud Authority, 2012), while in Scotland there is the Scottish Government Counter Fraud Strategy (2012). For charities, the Charity Commission has produced a Summary Strategy for Dealing with Fraud, Financial Crime and Financial Abuse of the Charity Sector as well as a Compliance Toolkit.

In the local government and health sectors data matching has become a key part of an organisation's counter fraud strategy. Participation in the National Fraud Initiative (NFI) has been mandatory for bodies in England under the Audit Commission Act 1998, and the Local Audit and Accountability Act 2014 has made provision for the continuation of the NFI going forward, with the Cabinet Office taking the lead. In Scotland the initiative is led by Audit Scotland under powers granted by the Criminal Justice and Licensing (Scotland) Act 2010. The Wales Audit Office has powers under the Public Audit (Wales) Act 2004 and in Northern Ireland under the Audit and Accountability (Northern Ireland) Order 2003. The NFI already includes participation from other parts of the public services, including several government departments and housing associations, but this is on a voluntary basis.

The British Universities Finance Directors Group (BUFDG) Fraud Working Group has produced a self-assessment checklist for finance managers that can be used in a number of ways to strengthen an institution's counter fraud measures. For education institutions, there is Fraud Indicators – A Generic Checklist for Learning Institutions (Education Funding Agency, 2013) and also the Schools Fraud Healthcheck (2014) developed by Mazars to support Fighting Fraud Locally. Both of these can be helpful in producing a counter fraud strategy in educational institutions.

GOOD PRACTICE GUIDANCE

CIPFA CODE OF PRACTICE PRINCIPLE C1

The governing body formally adopts a counter fraud and corruption strategy to address the identified risks and align with the organisation's acknowledged responsibilities and goals.

A strategy is a plan of action designed to achieve a long-term or overall aim. It should therefore have the following key elements:

- Aims should be clearly linked to the organisation's overall strategic objectives and show how the counter fraud strategy intends to help achieve these strategic objectives.

  Example:

  We aim to take a firm stance against fraud in social housing and where it is identified we will endeavour to recover the property. This will help us to ensure that social housing is used for those most in need and help to reduce waiting lists and use of temporary accommodation.

- The strategy needs to include all proactive counter fraud work including prevention and awareness, detection, investigation, the organisation's response to fraud and the action to be taken.

- Expected objectives, again aligned to the aims of the organisation. A specific link to the organisation's framework of good governance may be helpful here.
- Timelines which include target date for objectives, frequency of reviews and revision dates.
- How the success of the strategy is to be measured and by whom.

For the strategy to be relevant and up to date it needs to be regularly reviewed, revised and used to define success or failure. A strategy need not be lengthy and must be available to all in an organisation and not open to different interpretations.

The strategy should be linked to both fraud policies and procedures as well as other strategies, policies and procedures that may be relevant, eg pre-employment screening, procurement policies etc.

A strategy should be time limited, ie cover a period of time and:

- explain where the organisation is now
- where it is hoping to be at the end of the time agreed
- how the organisation is going to get there.

To ensure that the strategy has appropriate status and authority it should be approved by the appropriate decision making body such as the leadership team.

CIPFA CODE OF PRACTICE PRINCIPLE C2

The strategy includes the organisation's use of joint working or partnership approaches to managing its risks, where appropriate.

Working with other organisations and agencies is becoming increasingly relevant in times of budgetary and resource constraints. A governing body can therefore seek ways of improving the efficiency and effectiveness of counter fraud and corruption risk management through joint working with other organisations and agencies. Joint working is also a necessary response to the risks from organised crime which can commit fraud across a range of public service organisations.

The type of joint working may differ according to the size of the organisation and the risks it faces. However, some basic principles apply as follows:

- The aims and objectives, aligned to the organisations' overall aims and objectives are agreed and recorded.
- The governing bodies agree on the joint work to be undertaken.
- The joint work is recorded and responsibilities of each organisation are noted. This could include the identification of key staff.
- A review process is agreed. Will this be the responsibility of one organisation, both individually or a joint review team established?
- Policies, procedures and protocols are agreed in advance and any legal and employee issues considered, agreed and recorded.

CIPFA CODE OF PRACTICE PRINCIPLE C3

The strategy includes both proactive and responsive approaches that are best suited to the organisation's fraud and corruption risks.

Proactive and responsive components of a good practice response to fraud risk management include the following:

Proactive

- Developing a counter fraud culture to increase resilience to fraud:
  - A clear statement of intent, such as suggested under A1 of the Code, will send the right message to the whole organisation that fraud and corruption are being taken seriously and will help embed the counter fraud culture.
  - Other methods to support the development of a counter fraud culture include regular briefings or newsletters, recognition and praise for fraud prevention, detection, investigation and recovery activities and positive publicity of outcomes.
- Preventing fraud through the implementation of appropriate and robust internal control measures:
  - Counter fraud and corruption controls should be appropriate and robust. If they are not appropriate, time and resources will be wasted and if they are not robust, then they will be ineffective and could be by-passed. Having such controls not only deters potential fraudsters but also helps to raise the awareness of staff.
- Using techniques such as data matching to validate data:
  - Organisations should consider data matching and information/intelligence sharing, such as the National Fraud Initiative. Data matching can help to validate an organisation's risk identification process by comparing its results with similar organisations. Information/intelligence sharing can help to highlight fraud and corruption threats, including enablers to fraud that the organisation may not have considered or identified. Fraud alerts, such as those from the National Fraud Intelligence Bureau, the Metropolitan Police Service – Operation Sterling or the National Anti-Fraud Network (NAFN), are other useful sources of information.
- Deterring fraud attempts by publicising the organisation's counter fraud and corruption policy and the actions it takes against fraudsters:
  - For example, positive publicity about the successful detection or prevention of a fraud may help to deter others.

Responsive

- Detecting fraud through data and intelligence analysis:
  - If an organisation has effective prevention controls in place, it is imperative that it has an effective detection capability should these controls fail. Data analytics can help in this area and can aid in the identification of control failings.
- Implementing effective referral and confidential reporting and whistleblowing arrangements:

- Staff must feel able to report their concerns and an organisation should consider the most appropriate reporting route. There should be trusted routes open to staff to report their concerns, for example via their managers or to the counter fraud team.
- Organisations should also implement confidential reporting or whistleblowing arrangements. Effective arrangements will help there to be greater confidence in reporting concerns about fraud. Further useful advice on whistleblowing and the legal requirements of the Public Interest Disclosure Act 1998 (PIDA) can be found in the Public Concern at Work Whistleblowing Commission's Report on the Effectiveness of Existing Arrangements for Workplace Whistleblowing in the UK (2013) and their recommended Code of Practice.

- Investigating fraud referrals:
  - The strategy needs to include the general aims of any investigation, the reporting process and involvement of law enforcement. The organisation needs to have clear reporting and investigation procedures and a clear and stated policy on what investigative action will be taken.

Example:

The fraud team and internal audit will report the facts revealed during their investigations to management. Where initial investigations identify evidence of criminality, the matter will be reported to the relevant law enforcement agency.

- Applying sanctions, including internal, disciplinary, regulatory and criminal. The strategy should clearly state what the organisation will do if fraud is proven. This will provide further deterrence to potential fraudsters.

Example:

Where investigations reveal evidence of fraudulent or dishonest behaviour, corrupt practice or other culpable acts, the organisation will take appropriate steps which may include disciplinary and/or legal action whether the persons are members of staff or external to the organisation.

- Seeking redress, including the recovery of assets and money where possible. Recovery can be done using either in-house or police financial investigators who have powers under the Proceeds of Crime Act 2002 to conduct such activity as confiscation and seizure. Civil debt recovery may also be initiated for overpayments resulting from fraud.

Example:

Steps will also be taken to recover losses resulting from the fraud and a civil action against the perpetrator may be appropriate.

CIPFA CODE OF PRACTICE PRINCIPLE C4

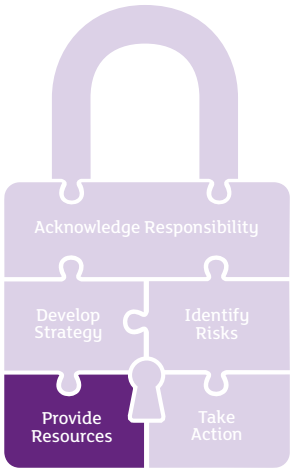
The strategy includes clear identification of responsibility and accountability for delivery of the strategy and for providing oversight.

The strategy should be the base document for the measurement of success or failure for the aims defined in C1 above. This will help all staff to understand the purpose of the counter fraud strategy and counter fraud work.

The strategy needs to identify the key fraud and corruption risks and the management and accountability for these risks. This is vital to ensure that the right resources are in place and the correct action is taken to reduce the harm caused by fraud and corruption.

The audit committee should have oversight of the organisation's strategy to assess whether it meets recommended practice and governance standards and it complies with legislation.[2] Oversight of the counter fraud strategy will support the audit committee's understanding of governance activities during the year.

2. See Chapter 4 (s4.32) of Audit Committees: Practical Guidance for Local Authorities and Police (CIPFA, 2013).



CHAPTER 6

Provide Resources

CIPFA CODE OF PRACTICE PRINCIPLE D

The organisation should make arrangements for appropriate resources to support the counter fraud strategy.

CONTEXT

A commitment to reduce the risk of fraud and corruption is clearly demonstrated by the overall investment and the application of resources within an organisation.

The resource should include the requirements to fulfil the strategy, including:

- deterrence
- awareness and prevention work
- detection
- investigation
- follow-up action
- training of counter fraud and other staff.

Not all the resources need to be dedicated counter fraud professionals and in some organisations the resource may be provided by third party suppliers or through a joint working arrangement.

Organisations should also ensure that there is co-operation between the counter fraud team and other departments. This includes internal audit, the ICT department, HR, finance and procurement. Through such co-operation, the counter fraud team can have access to vital internal information and intelligence such as details of attacks (successful and unsuccessful) against the ICT system. This may indicate fraudsters attempting to access the organisation's records. Joint internal working between HR, procurement and the counter fraud team may highlight potential conflicts of interest.

There should also be well established relationships with external partners such as law enforcement agencies (including HMRC), professional bodies (eg CIPFA), and other government departments such as the Department for Work and Pensions (DWP).

SECTOR INTERPRETATION

Larger organisations may have a dedicated fraud team, access to ICT tools and specialists such as a financial investigator. Others have established their resources through collaborative arrangements.

Smaller organisations such as schools, charities and housing trusts often have limited in-house counter fraud capability, some rely on outsource agreements while unfortunately some have no access to counter fraud and corruption capability at all. In such cases, it is even more important that the organisation's leadership team provide the right message and the staff of these organisations are used as the first line of defence in counter fraud and corruption.

GOOD PRACTICE GUIDANCE

CIPFA CODE OF PRACTICE PRINCIPLE D1

An annual assessment of whether the level of resource invested to counter fraud and corruption is proportionate for the level of risk.

An annual assessment should be conducted to review whether the level of resource invested to counter fraud and corruption is proportionate for the level of risk. This should be part of the overall counter fraud and corruption strategy and be linked to the annual review of the strategy by the nominated body.

The organisation should identify who should be responsible for this assessment in their counter fraud and corruption strategy and in most cases this is likely to be the accountable person. Approval of the strategy and the associated resources will lie with the governing body, but the adequacy of the available resource to support the strategy should also be considered by the audit committee. The assessment can also be subject to independent review and assurance from internal audit, which is again likely to be reported to the audit committee.

Section 2120 A2 of the Public Sector Internal Audit Standards (PSIAS) states that internal audit must evaluate the potential for the occurrence of fraud and how the organisation manages fraud risk. As part of this review internal audit is likely to consider the available capacity of the organisation to identify fraud risks, prevent and detect fraud and take appropriate action.

CIPFA CODE OF PRACTICE PRINCIPLE D2

The organisation utilises an appropriate mix of experienced and skilled staff, including access to counter fraud staff with professional accreditation.

Training needs to be provided to ensure that counter fraud staff have the skills, experience and accreditation to conduct their work. This is of particular importance for the conduct of fraud investigations which might lead to criminal prosecutions. In these cases the collection of evidence must meet legal standards to be admissible in a court of law. In addition, some larger organisations may decide to conduct their own financial investigations, which would require staff to be trained and accredited as a financial investigator in order to obtain direct

access to banking and other financial records without having to rely on law enforcement agencies.

Organisations should consider implementing a personal development process to help identify skills gaps and support continuous professional development.

In times of financial restraint it is often very difficult to make a case for an increase in staff but one example where this did occur is as follows:

Example:

A council needed to make the case for expanding the counter fraud team's focus from predominantly a benefits fraud team to a corporate-wide approach to tackling fraud across the council and its departments, and needed senior management buy-in. Having established a corporate team, decisions were taken to establish partnerships with various service areas, including internal audit, with the common aim of tackling fraud.

At the same time they created a technology infrastructure, including anti-fraud software which drew on data from different parts of the organisation giving the team access to real time intelligence. It allowed the team to look across investigations that ordinarily would have been missed. The team is now able to do comparisons across departments while respecting Data Protection Act protocols – they only share data that is critical to making a case.

Guidance on establishing a corporate fraud team is available in CIPFA's Developing Corporate Anti-Fraud Capability in the Public Services (2012).

The behaviours of counter fraud staff must be beyond reproach. Their activities should be governed by a code of conduct/ethical framework. Some counter fraud staff may be governed by the ethical standards of their professional bodies, such as accounting or auditing institutes, the Institute of Counter Fraud Specialists or the Association of Certified Fraud Examiners. Organisations may wish to apply their own code on investigators which should include statements on integrity, objectivity, confidentiality and competency. This code should be produced alongside the organisation's code of ethics to ensure consistency.

Where the organisation has identified "counter fraud champions" to promote awareness and act as focal point in departments, then ongoing training may be required to ensure they are aware of new risks or other developments.

Raising the awareness of all staff is also an essential part of fraud prevention. Even large organisations have a limited number of staff dedicated to counter fraud and corruption work. Thus staff can be used as the first line of defence against fraud and corruption. Staff on the "front line" are more likely to understand if something is out of the ordinary and may indicate fraudulent activity. Organisations should recruit and train and actively encourage those who can fight fraud and corruption effectively, ie their employees.

There are several methods for training staff:

- **Formal subject specific counter fraud presentations**
  While these can be customised to the audience and provide detailed input to staff, they can be time consuming for both the trainer and staff.

- **"E-learning" tools**
  Such tools can reach a far larger audience in a more cost effective manner than formal presentations but are limited in what they can deliver and limited to those who have access to the necessary technology. It can also be expensive to regularly update the presentation.
- **Regular counter fraud briefings as an input to routine generic team meetings**
  This can be a very effective way of getting short, sharp messages across the teams and can be tailored to the audience. For example, a talk on personnel type frauds can be given to the HR team. This type of training, however, is often limited in what can be included and many departments can be reluctant to allow the counter fraud team to use up valuable team talk time.

However, any investment in training will greatly improve the awareness of staff and increase and improve fraud prevention and deterrence. It is also important to evaluate the effectiveness of such training.

CIPFA CODE OF PRACTICE PRINCIPLE D3

The organisation grants counter fraud staff unhindered access to its employees, information and other resources as required for investigation purposes.

The job of the counter fraud professional is to put into practice the counter fraud and corruption strategy. Achieving this remit requires sufficient power and authority (for example, access to staff records, documents and meetings). The organisation needs to make clear this authority in documents such as standing financial instructions and partnership agreements.

Access to the organisation's records and staff personnel files and other records is an action that has to be clearly regulated with sufficient oversight to ensure that it is not abused. Whenever access to sensitive records is required, such as personnel records, this should be recorded by the investigator and approved by a superior. For example, the request could be submitted to an appropriate senior HR manager to arrange for the records to be provided. An independent audit of this access can be conducted to provide assurance to the organisation's leadership and to staff that this access is used appropriately.

If the counter fraud team is externally provided or via a joint working agreement, access to sensitive records should be agreed in advance in any agreement or contract. Consideration should be given to having a single point of contact within the organisation for any external provider who will access the records on behalf of the third party.

A counter fraud team is increasingly reliant on technical tools to assist in fraud prevention and detection. Sufficient investment may need to be made to ensure that any gaps identified in the risk management process can be monitored and identified quickly. Such tools could include continuous auditing capability to not only highlight risks but also to provide an early warning of potential fraudulent acts.

Similarly, intelligence software will be able to provide indicators of areas susceptible to fraud and corruption that may not have been highlighted during other risk assessments. This will help to target the organisation's resources at the most vulnerable areas. Additionally, a team may require specialist investigation, case management or intelligence software. A

collaborative team should use common tools and software to ensure an accurate and clear flow of information and intelligence.

CIPFA CODE OF PRACTICE PRINCIPLE D4

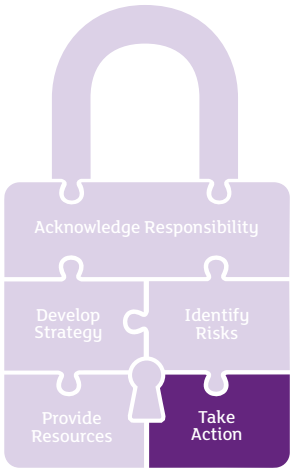
The organisation has protocols in place to facilitate joint working and data and intelligence sharing to support counter fraud activity.

Joint working with other organisations and agencies is becoming more common to reduce the need for resources in single organisations. If this is the case, frameworks can be put in place with other organisations and law enforcement agencies. Relationships need to be agreed in advance and issues clarified such as responsibilities, obligations, exchange of information, liaison, communications, meetings with key personnel and media strategies. This can be achieved through framework agreements, memorandums of understanding and service level agreements.

These agreements need to concentrate on issues that support operational co-operation, such as areas of mutual interest, joint planning and co-ordinated action. They need to be viable and have helpful arrangements in place to deliver work in line with objectives and goals.

The governance arrangements must be kept up to date and relevant. There need to be regular meetings not just between counter fraud staff but with senior management and joint reviews should be undertaken.

There are many examples of good practice in the use and sharing of resources. They include memorandums of understanding between agencies, particularly with law enforcement organisations. There are good examples of local partnerships for either general counter fraud activity or to address a specific fraud issue. For example, a council may co-operate with local housing associations to address tenancy fraud risks.



CHAPTER 7

Take Action

CIPFA CODE OF PRACTICE PRINCIPLE E

The organisation should put in place the policies and procedures to support the counter fraud and corruption strategy and take action to prevent, detect and investigate fraud.

CONTEXT

The action needed can vary from organisation to organisation and can be dependent upon size, function, activity and governance arrangements. All organisations, however, should have an action plan linked to the risk register and the overall counter fraud and corruption strategy. The action plan should be comprehensive and include:

- a fraud prevention and deterrence plan
- proactive detection (data analytics/fraud audits)
- investigation
- sanctions
- redress
- reporting.

Taking the proper and appropriate action is essential if organisations are to reduce the harm and losses caused by fraud and corruption. Such action, well publicised and adhered to, will send the right message to staff, foster a counter fraud and corruption culture and help to deter fraudsters. Furthermore, a fraud action plan can also help to reduce the impact should a fraud be discovered.

Example:

A substantial part of our fraud took place over an eight week period between two board meetings. If it had continued at the same rate for another eight weeks before the trustees detected and dealt with the breach in financial procedures, the charity would not now be here. Still, the devastation for this small charity has been immense. There remains a profound sense of shock that over twenty years' work and a national reputation came so close to being wiped out within such a short time-scale.

Source: Charity Commission Compliance Toolkit.

SECTOR INTERPRETATION

The ability to take action will be dependent upon the size and nature of an organisation and the size of its counter fraud capacity. Irrespective of the size of activities of an organisation, however, the organisation needs to take appropriate action and report on that action to its governing body.

Accounts and Audit Regulations require the responsible financial officer in local authorities and police bodies in England, Wales and Northern Ireland to determine accounting control systems. These must include measures to enable the prevention and detection of inaccuracies and fraud.[3]

In central government, Managing Public Money (HM Treasury, 2013) states that 'the organisation's response to fraud risk should be customised to the risks it faces'. Suggested actions include:

- establishing cost-effective internal systems of control to prevent and detect fraud
- responding quickly and effectively to fraud when it arises
- establishing systems for investigations into allegations of fraud.

When frauds are identified some public service organisations are required to inform those bodies with regulatory oversight. *Managing Public Money* requires relevant organisations to retain a record of the fraud and to consider informing the National Audit Office. Academies are required to inform the Education Funding Agency of all frauds in excess of £5000 either individually or cumulatively over the year. For more information see the Academies Financial Handbook (Education Funding Agency, 2014).

The Homes and Communities Agency (HCA) requires registered providers to provide an annual report on net losses from fraudulent activity; see the Regulatory Framework for Social Housing in England (HCA, 2012).

Charities should refer to Chapter 3 of the Charity Commission's Compliance Toolkit, which states that all charities must, as a minimum:

- have some form of appropriate internal and financial controls in place to ensure that all their funds are fully accounted for and are spent in a manner that is consistent with the purpose of the charity; what those controls and measures are and what is appropriate will depend on the risks and the charity
- keep proper and adequate financial records for both the receipt and use of all funds together with audit trails of decisions made. Records of both domestic and international transactions must be sufficiently detailed to verify that funds have been spent properly as intended and in a manner consistent with the purpose and objectives of the organisation
- give careful consideration to what other practical measures they may need to consider to ensure they take reasonable steps to protect the charity's funds and the trustees meet their legal duties

3. Accounts and Audit Regulations 2011. See also the Accounts and Audit Regulations (Wales) 2005 and the Local Government (Accounts and Audit) Regulations (Northern Ireland) 2006. The latest Scottish regulations, the Local Authority Accounts (Scotland) Regulations 2014, do not include a reference to fraud.

- deal responsibly with incidents when they occur, including prompt reporting to the relevant authorities and ensuring the charity's funds are secure.

The Local Government Transparency Code 2014 requires local authorities in England to publish statistics each year, including the total number of fraud cases investigated.

Within the health sector, NHS England's Tackling Fraud, Bribery and Corruption: Policy and Corporate Procedures (2013) states that activities to tackle economic crime will be carried out within three key principles for action:

1. Inform and involve.
2. Prevent and deter.
3. Hold to account.

In addition, the NHS Protect service has produced Standards for Providers 2014/15 – Fraud, Bribery and Corruption, which gives information to providers of NHS services on the anti-fraud clauses in the NHS Standard Contract and explains what providers need to do to comply with them. There is a requirement for all providers (except "small providers") to complete an "organisation crime profile" within one month of the NHS Standard Contract coming into effect.

GOOD PRACTICE GUIDANCE

CODE OF PRACTICE PRINCIPLE E1

The organisation has put in place a policy framework which supports the implementation of the counter fraud strategy.

Having such a framework and ensuring that all policies are mutually supportive and cross referenced will encourage and raise awareness of all staff to the fraud and corruption risks. Increased awareness aids prevention and detection.

As a minimum the framework should include the following:

- **Counter fraud policy**
  This should be linked to the strategy and include prevention, detection, investigation and reporting processes and those responsible for each activity.
- **Whistleblowing policy**
  This should include the aims of the policy, what is covered, how to raise a concern, the process, safeguards and confidentiality.
- **Anti-money laundering policy**
  This may not be applicable to all organisations. The exact contents of your policy will depend on the organisation but, as advised by HMRC[4], should include:
  - details of your approach to preventing money laundering, including named individuals and their responsibilities
  - details of your procedures for identifying and verifying customers, and your customer due diligence measures and monitoring checks

4. See also Combating Financial Crime: Further Guidance on Anti-money Laundering in Public Service Organisations (CIPFA, 2015).

- a commitment to training employees so they are aware of their responsibilities
- a summary of the monitoring controls that are in place to make sure your policies and procedures are being carried out
- recognition of the importance of staff promptly reporting any suspicious activity to the nominated officer.

- **Anti-bribery and corruption policy**
  You should have an anti-bribery policy if there is a risk that someone who works for you or on your behalf might be exposed to bribery. The policy should be proportionate to the risk and include:
  - your approach to reducing and controlling the risks of bribery
  - rules about accepting gifts, hospitality or donations
  - guidance on how to conduct your business, eg negotiating contracts
  - rules on avoiding or stopping conflicts of interest.

- **Gifts and hospitality policy and register**
  This policy should include a full list of those to whom it applies, eg governing body members, full and part time staff, contractors, consultants and agency staff. It should also define what is meant by gifts and hospitality, clearly stating what is and what is not acceptable. The policy should also detail the reporting processes, the registration process and compliance checks.

- **Pecuniary and conflict of interest policies**
  It is essential that an organisation has a policy that covers any potential conflict of interest that employees may face due to their association or relationship with other organisations. The policy must clearly detail what is and what is not acceptable and the need to be fully open and transparent about one's business activities outside of the organisation. This will promote honesty and openness and also assist in any investigation into conflicts of interest and potential fraudulent behaviour.

- **Codes of conduct and ethics**
  Organisations should expect the highest standards from all staff adhering to the Seven Principles in Public Life (the "Nolan Principles") of:

  1. selflessness
  2. integrity
  3. objectivity
  4. accountability
  5. openness
  6. honesty
  7. leadership.

  Adherence to such principles will minimise the organisation's exposure to the risk of fraud committed by staff.

- **Information security policy**
  The security of information is essential to good management and public confidence. To operate effectively, organisations must maintain the confidentiality, integrity and

availability of its information; for more information see the government's Security Policy Framework (2014). This will also ensure that information is protected against unauthorised access by fraudsters.

- **Cyber security policy**
  Many frauds today are increasingly perpetrated via the internet, using digital technologies, devices and social media. Organisations should follow the government's Cyber Security Guidance (2012), which details how a clear and easily understood cyber security policy can be used by organisations to strengthen their resilience to cyber risk and tackle cyber crime. The policy, while having clearly defined reporting processes and aims, should also stress that cyber risk management is the responsibility of every employee.

These policies need to be mutually supportive and cross referenced. Specific care should be taken to ensure that they are not contradictory and are easily followed by all staff. Where possible a single department such as HR or corporate governance should be responsible for ensuring this occurs. They should be regularly reviewed to ensure they are up to date and fit for purpose. There should be regular communications to all staff especially whenever a policy is amended or replaced. All policies should be signed off and supported at the highest level within an organisation.

CIPFA CODE OF PRACTICE PRINCIPLE E2

Plans and operations are aligned to the strategy and contribute to the achievement of the organisation's overall goal of maintaining resilience to fraud and corruption.

PROACTIVE DETECTION

A proactive plan can be developed to achieve early detection of fraud and corruption. The plan needs to include any audits that may assist in this detection or specify any activity by the dedicated counter fraud team. The counter fraud team or person responsible for fraud risk management can liaise with the internal auditors at the audit planning stage to give ideas and direction concerning the fraud risk.

Specific fraud detection audits can be conducted.

Example:

An organisation conducted a real time audit of financial authority approvals during a specific period when large numbers of staff were engaged on non-routine duties and when the normal segregation of duties system may not have been fully in place.

Data analytics can also be used to detect fraud in a proactive manner.

Example:
An organisation had in place a level of self-authorisation for spends. Data analytics were used to review whether this level was being abused by looking at:

- multiple spends with particular suppliers at just below the authorised spend limit
- separate purchases being made with one supplier to bypass OJEU regulations
- excessive use of the self-authorisation by any particular members of staff.

INVESTIGATION

If a fraud or corruption case is identified, all organisations need a clear fraud response plan. Those involved need to be aware of the immediate actions to be taken, the aims of any investigation and to whom they should go to for help and advice. This will ensure that investigations are correctly managed, evidence is secured, the investigation remains confidential and losses are minimised. The initial detection of fraud and corruption is often the most critical time in an investigation and decisions must be made quickly to secure evidence, mitigate losses and ensure a legal and effective investigation.

The aims of any investigation should be clearly defined in the counter fraud and corruption strategy and these aims adhered to during the investigation. If a third party investigative organisation is being used, it should adhere to these aims and follow the organisation's laid down procedures.

Investigations should ensure that they comply with current legislation (criminal and employment) and procedures. As such, legal advice should be sought in the early stages of an investigation.

An organisation needs to be aware of any regulatory reporting requirements for its sector or the need to inform other external parties of fraud and fraud losses, for example external auditors or the organisation's insurer.

If an organisation has a policy of reporting frauds to law enforcement agencies, there needs to be clear criteria and reporting methodology in place. For example, when does this happen, who is responsible and what method of reporting will be used?

Following the conclusion of the investigation the report should not only detail the investigation and conclusion but should also cover:

- identification of any weaknesses in any defences used by the organisation
- improvement opportunities both in risk management, fraud prevention, detection and investigation
- identification of strengths and best practice procedures
- a review of responsibilities and risk ownership
- a review of the resource plan including technical resources and training requirements.

Investigation reports have the most impact if they are circulated to the organisation's leadership team as well as the risk owners.

CIPFA CODE OF PRACTICE PRINCIPLE E3

Making effective use of national or sectoral initiatives to detect fraud or prevent fraud, such as data matching or intelligence sharing.

The prime example of this is the National Fraud Initiative. This exercise has shown that data matching and the sharing of information and intelligence can help to identify fraud. Regional or joint initiatives may also be possible.

CIPFA CODE OF PRACTICE PRINCIPLE E4

Providing for independent assurance over fraud risk management, strategy and activities.

As stated in Section A4 of the Code, the organisation needs to have a clear programme of work to manage fraud and corruption risks with specific goals as set out in a counter fraud and corruption strategy. The governing body can assess whether this plan of work is achieving its aims by implementing an independent review of compliance, goals and resources.

This independent review can be conducted by internal auditors and will support internal audit conformance with Section 2120 A2 of the Public Sector Internal Audit Standards. Additionally as stated in Section C4 above, the audit committee should have an independent oversight of the organisation's strategy to assess whether it meets recommended practice and governance standards and it complies with legislation.

REPORTING

CIPFA CODE OF PRACTICE PRINCIPLE E5

There is a report to the governing body at least annually on performance against the counter fraud strategy and the effectiveness of the strategy from the lead person(s) designated in the strategy. Conclusions are featured in the annual governance report.

There also needs to be a robust reporting, compliance and governance process, including the following:

- The independent view of compliance, goals and resources (see E4 of the Code).
- A report to the governing body at least annually on:
  - performance against the counter fraud strategy from the lead person(s) designated in the strategy
  - the impact and cost effectiveness of its counter fraud activities; loss measurement should not solely be in terms of monetary loss but also reputation, effects on staff and morale and costs of investigations
- Conclusions should feature in the annual governance report.

ANNUAL STATEMENTS

The Code states that where organisations are making a statement in an annual governance report about their adherence to this Code, they should assess their level of conformance with the Code. Following this the most appropriate statement should be approved by the governing body and signed by the person responsible for signing the annual governance report.

STATEMENT 1

Having considered all the principles, I am satisfied that the organisation has adopted a response that is appropriate for its fraud and corruption risks and commits to maintain its vigilance to tackle fraud.

Or

STATEMENT 2

Having considered all the principles, I am satisfied that, subject to the actions identified below, the organisation has adopted a response that is appropriate for its fraud and corruption risks and commits to maintain its vigilance to tackle fraud.

Actions to be taken to manage the risk of fraud:

Action:	Responsibility:	Target date:

APPENDIX A

Glossary

Annual Fraud Indicator (AFI)	A compendium of fraud loss indicators which strives to provide a best estimate of the scale of the problem and raise awareness.
Annual governance report	The mechanism by which an organisation publicly reports on its governance arrangements each year.
Audit committee	The governance group charged with independent assurance of the adequacy of the risk management framework, the internal control environment and the integrity of financial reporting.
Bribery Act 2010	Provides for a consolidated scheme of bribery offences to cover bribery both in the UK and abroad.
Charity Commission	The independent government department which registers and regulates charities in England and Wales.
Chief financial officer (CFO)	The organisation's most senior executive role charged with leading and directing financial strategy and operations.
Cyber security	The protection of systems, networks and data in cyber space. This is a critical issue for all businesses.
Economic Crime Command	Part of the National Crime Agency (NCA) whose role is to fight economic crime by undermining criminals and educating those most at risk of attack by sharing intelligence and knowledge with partners, disrupting criminal activity and seizing assets.
Fighting Fraud Locally (FFL)	A strategic approach developed by local government for local government, addressing the need for greater prevention and smarter enforcement.
Fraud Act 2006	An Act of Parliament creating a general offence of fraud with a maximum custodial sentence of ten years; replacing all previous deception offences as detailed under the Theft Acts 1968-1996.
Governance	Governance comprises the arrangements put in place to ensure that the intended outcomes for stakeholders are defined and achieved, includes political, economic, social, environmental, administrative, legal, and other arrangements.

Governing body	The person(s) or group with primary responsibility for overseeing an entity's strategic direction, operations, and accountability.
Information security	The practice of defending information from unauthorised access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.
Intelligence	Information that has been collected, analysed and evaluated.
Internal audit	An assurance function that provides an independent and objective opinion to the organisation on the control environment by evaluating its effectiveness in achieving the organisation's objectives.
International Federation of Accountants (IFAC)	The global organisation for the accountancy profession.
Leadership team	Comprises the governing body and management team.
Management team	The group of executive staff comprising the senior management charged with the execution of strategy.
Managers	The staff responsible for the achievement of the organisation's purpose through services/ businesses and delivery to its clients/customers.
National Crime Agency (NCA)	A UK law enforcement agency with national and international reach and the mandate and powers to work in partnership with other law enforcement organisations to address serious and organised crime.
National Fraud Initiative (NFI)	An exercise that matches electronic data within and between public and private sector bodies to prevent and detect fraud.
Protecting the Public Purse (PPP)	Annual reports which give details on amounts of detected fraud, warn of fraud risks and promote best practice in local government.
Public Interest Disclosure Act 1998	An Act of Parliament that protects whistleblowers from detrimental treatment by their employer.
Public service organisation	One or more legal bodies managed as a coherent operational entity with the primary objective of providing goods or services that deliver social benefits for civic society, are not privately owned, and receive public and/or charitable funding.
Risk management	The systematic process of understanding, evaluating and addressing risks to maximise the chances of objectives being achieved and ensuring organisations are sustainable.

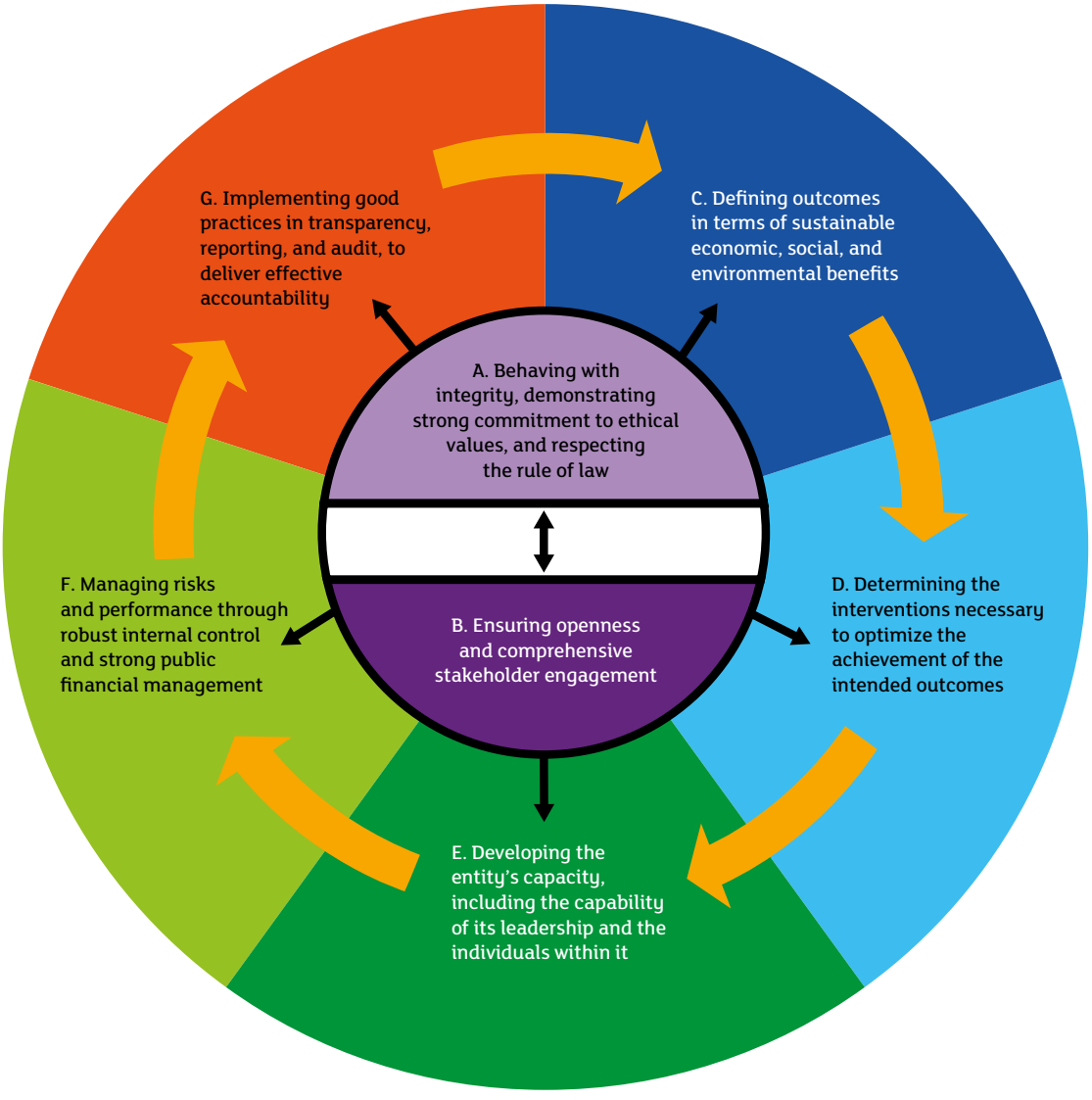
Seven Principles of Public Life	Seven principles established by the Committee on Standards in public Life, which are: selflessness, integrity, objectivity, accountability, openness, honesty and leadership. Used as the basis for many ethical governance frameworks.
Single Fraud Investigation Service (SFIS)	An organisation operating under a single policy and one set of operational procedures for investigating all welfare, benefit and tax credit fraud.
The Code	CIPFA Code of Practice on Managing the Risk of Fraud and Corruption.
Whistleblowing	When a worker reports suspected wrongdoing at work. Officially this is called “making a disclosure in the public interest”.

APPENDIX B

The Relationship of the Code of Practice to the International Framework

Seven principles underpin good governance in the International Framework. These are outlined in the following diagram:

Achieving the Intended Outcomes While Acting in the Public Interest at all Times



While there are linkages that can be made between the Code and each of the principles, two in particular stand out:

Acting in the public interest requires:

A. Behaving with integrity, demonstrating strong commitment to ethical values, and respecting the rule of law.

F. Managing risks and performance through robust internal control and strong public financial management.

Comparison of the Code against the International Framework: Good Governance in the Public Sector

Code Principle	International Framework (IFAC/CIPFA)
Acknowledge responsibility The governing body should acknowledge its responsibility for ensuring that the risks associated with fraud and corruption are managed effectively across all parts of the organisation.	Acting in the public interest requires: A. Behaving with integrity, demonstrating strong commitment to ethical values, and respecting the rule of law.
Identify risks Fraud risk identification is essential to understand specific exposures to risk, changing patterns in fraud and corruption threats and the potential consequences to the organisation and its service users.	F. Managing risks and performance through robust internal control and strong public financial management: – regularly reviewing key strategic, operational, financial, reputational, and fraud risks and then devising responses consistent with achieving the entity's objectives and intended outcomes. (p.27)
Develop a strategy An organisation needs a counter fraud strategy setting out its approach to managing its risks and defining responsibilities for action.	D. Determining the interventions necessary to optimize the achievement of the intended outcomes. F. Managing risks and performance through robust internal control and strong public financial management. – regularly reviewing key strategic, operational, financial, reputational, and fraud risks and then devising responses consistent with achieving the entity's objectives and intended outcomes. (p.27) – role of the audit committee – helping the entity to embed the values of ethical governance, including effective arrangements for countering fraud and corruption. (p.30)
Provide resources The organisation should make arrangements for appropriate resources to support the counter fraud strategy.	E. Developing the entity's capacity, including the capability of its leadership and the individuals within it.

Code Principle	International Framework (IFAC/CIPFA)
Take action The organisation should put in place the policies and procedures to support the counter fraud and corruption strategy and take action to prevent, detect and investigate fraud.	F. Managing risks and performance through robust internal control and strong public financial management: – safeguarding the entity's resources against loss, fraud, misuse, and damage. (p.29) – internal audit reviews can cover a wide range of topics, including those relating to the achievement of value for money and the prevention and detection of fraud and corruption. (p.29) G. Implementing good practices in transparency, reporting, and audit, to deliver effective accountability.

APPENDIX C

Mapping of the Code to Governance Frameworks in use in the Public Services

A number of governance frameworks operate across the public services. There is a greater synergy of the Code with some more than others. The following table shows the mapping of the principles in the Code to the most relevant parts of each sectoral code. Understanding the linkage to the governance framework will help those implementing the Code to link it to the organisation's objectives.

Code Principle	Delivering Good Governance in Local Government CIPFA/SOLACE 2007[5]	Corporate Governance in Central Government Departments: Code of Good Practice 2011	Excellence in Governance National Housing Federation 2010
Acknowledge responsibility The governing body should acknowledge its responsibility for ensuring that the risks associated with fraud and corruption are managed effectively across all parts of the organisation.	Promoting values for the authority and demonstrating the values of good governance through upholding high standards of conduct and behaviour: ■ ensuring authority members and officers exercise leadership by behaving in ways that exemplify high standards of conduct and effective governance ■ ensuring that organisational values are put into practice and are effective.	3.8 The Accounting Officer should establish and document a clear allocation of responsibilities amongst officials in the department, but he or she retains overall personal responsibility and accountability to parliament for propriety and regularity. 4.10 Board members should act in the public interest in keeping with the Nolan Principles of Public Life.	A. The board must be effective in leading and controlling the organisation and acting in its best interest. Board members must ensure that the interests of the organisation are placed before any personal interests. L. Organisations must maintain the highest standards of probity and conduct.
Identify risks Fraud risk identification is essential to understand specific exposures to risk, changing patterns in fraud and corruption threats and the potential consequences to the organisation and its service users.	Taking informed and transparent decisions which are subject to effective scrutiny and managing risk: ■ ensuring that an effective risk management system is in place.	6.1 The board should ensure that there are effective arrangements for governance, risk management and internal control for the whole departmental family.	B2. The core responsibilities of the board include: ■ establishing and overseeing a risk management framework in order to safeguard the assets of the organisation.
Develop a strategy An organisation needs a counter fraud strategy setting out its approach to managing its risks and defining responsibilities for action.			

5. The Framework is to be revised in 2015.

Provide resources The organisation should make arrangements for appropriate resources to support the counter fraud strategy.	Developing the capacity and capability of members and officers to be effective: ■ making sure that members and officers have the skills, knowledge, experience and resources they need to perform well in their roles.		
Take action The organisation should put in place the policies and procedures to support the counter fraud and corruption strategy and take action to prevent, detect and investigate fraud.		6.1 The board should ensure that there are effective arrangements for governance, risk management and internal control for the whole departmental family.	K. The board must establish a formal and transparent arrangement for considering how the organisation ensures financial viability, maintains a sound system of internal controls, manages risk and maintains an appropriate relationship with external auditors. K1. Every organisation must have effective internal controls.
Requirements to consider adequacy of counter fraud and anti-corruption arrangements as part of annual governance reports Code E5	Addendum 2012: Key elements of an authority's governance should include arrangements for: ensuring effective counter fraud and anti-corruption arrangements are developed and maintained.		

Code Principle	The NHS Foundation Trust Code of Governance Monitor 2014	Clinical Commissioning Groups, NHS England recommend following the principles of the Good Governance Standard for the Public Services	Governance Code of Practice and General Principles, Committee of University Chairs 2009 (CUC)[6] Memorandum of assurance and accountability Higher Education Funding Council 2014 (HEFCE)
Acknowledge responsibility The governing body should acknowledge its responsibility for ensuring that the risks associated with fraud and corruption are managed effectively across all parts of the organisation.	A.1.8 The board of directors should establish the constitution and standards of conduct for the NHS foundation trust and its staff in accordance with NHS values and accepted standards of behaviour in public life, which includes the principles of selflessness, integrity, objectivity, accountability, openness, honesty and leadership (The Nolan Principles). A5b The council of governors is responsible for representing the interests of NHS foundation trust members and the public and staff in the governance of the NHS foundation trust. Governors must act in the best interests of the NHS foundation trust and should adhere to its values and code of conduct.	3. Good governance means promoting values for the whole organisation and demonstrating the values of good governance through behaviour. The governing body should take the lead in establishing and promoting values for the organisation and its staff. These values should be over and above legal requirements (for example, anti-discrimination, equal opportunities and freedom of information legislation) and should build on the Nolan principles. They should reflect public expectations about the conduct and behaviour of individuals and groups who control public services.	Role of the Governing Body 1.2 Individual members and governing bodies themselves should at all times conduct themselves in accordance with accepted standards of behaviour in public life which embrace selflessness, integrity, objectivity, accountability, openness, honesty and leadership. (CUC)

6. Currently under review.

Identify risks Fraud risk identification is essential to understand specific exposures to risk, changing patterns in fraud and corruption threats and the potential consequences to the organisation and its service users.	C.2.a The board of directors is responsible for determining the nature and extent of the significant risks it is willing to take in achieving its strategic objectives. The board should maintain sound risk management systems.	4. Good governance means taking informed, transparent decisions and managing risk. A risk management system should consider the full range of the organisation's activities and responsibilities, and continuously check that various good management disciplines are in place, including: ■ laws and regulations are complied with ■ financial resources are managed efficiently and effectively and are safeguarded.	2.35 Higher Education Institutions are expected to identify and actively manage risks, having particular regard at governing body level to risks which could threaten the existence of the institution. (CUC)
Develop a strategy An organisation needs a counter fraud strategy setting out its approach to managing its risks and defining responsibilities for action.			
Provide resources The organisation should make arrangements for appropriate resources to support the counter fraud strategy.			

Take action The organisation should put in place the policies and procedures to support the counter fraud and corruption strategy and take action to prevent, detect and investigate fraud.	C.2.b The board of directors should maintain a sound system of internal control to safeguard patient safety, public and private investment, the NHS foundation trust's assets, and service quality.	Principle 6: Governing bodies have robust and effective processes for decision-making, as outlined in their constitution, that support and maintain transparency and accountability at every level. Complying with laws against bribery, including implementing clear guidance on gifts and hospitality.	29 In accordance with the HEI's own statutes and constitution, there should be effective arrangements for providing assurance to the governing body that the HEI: a. Has a robust and comprehensive system of risk management, control and corporate governance. This should include the prevention and detection of corruption, fraud, bribery and irregularities. (HEFCE)
Requirements to consider adequacy of counter fraud and anti-corruption arrangements as part of annual governance reports Code E5	C.2.b The board should report on internal control through the Annual Governance Statement (formerly the Statement on Internal Control) in the annual report.		Corporate Governance Statement Appendix A2 Consider responsibilities in respect of: maintaining proper accounting records, compliance with institution's charter or statutes, compliance with the SORP (Statement of Recommended Practice) and Funding Council Financial Memorandum, safeguarding assets and prevention and detection of fraud. (CUC)

APPENDIX D

Public Service Organisations – Governing Bodies and Accountable Officer

Organisation Type	Governing Body	Mandated or Suggested Accountable Officer
Central Government[7]		
Devolved Administrations:		
■ Scottish Government	Strategic board	Principal accounting officer
■ Welsh Government	Board	Accounting officer
■ Northern Ireland Assembly	Department board	Accounting officer
Government Departments:		
■ Ministerial Government Departments	Department board	Accounting officer
■ Non Ministerial Government Departments		
Government Agencies and Public Bodies (including Non Departmental Public Bodies[8]:	Agency board[9]	Chief executive officer
High Profile Groups	Strategic board	Accounting officer
Public Corporations	Board	
	Departmental board	

7. www.gov.uk/government/organisations

8. NDPBs are further analysed into Advisory, Executive, Tribunal and Other and are subject to review and rationalisation under the Cabinet Office Public Bodies Act review. www.gov.uk/government/publications/public-bodies-2014 Categories of Public Bodies: A Guide for Departments https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/80075/Categories_of_public_bodies_Dec12.pdf

9. www.gov.uk/government/uploads/system/uploads/attachment_data/file/80076/exec_agencies_guidance_oct06_0.pdf para 14

Local Government		
Local authorities	Council	Chief finance officer
Police	Police and crime commissioner	Chief finance officer
	Chief constable	Chief finance officer
Fire	Fire authority	Chief finance officer
Health		
NHS England	Board	Chief finance officer
NHS foundation trusts	Board	Chief finance officer
NHS trusts	Board	Chief finance officer
Ambulance trusts	Board	Chief finance officer
Clinical commissioning groups	CCG governing body	Chief finance officer
Special health authorities	Board	Chief finance officer
Community interest companies	Board	Chief finance officer
Education		
Higher education	University council or board of governors	Vice-chancellor or principal
Further education colleges	Board or corporation	Principal
Schools, including academies	Governing body	Headteacher
Not for Profit and Charitable Bodies		
Charities	Board council	Chief finance officer, chief operating officer
Housing associations	Board	Chief finance officer

APPENDIX E

Further Guidance and Useful Resources

RESOURCES FROM CIPFA

CIPFA Counter Fraud Centre

The CIPFA Counter Fraud Centre (CCFC) brings together collaboration, strong leadership and 125 years of expertise in public finance and governance to support organisations. The CCFC provides a "one stop shop" for fighting fraud, including tools, training and the ideas to shape the future of counter fraud.

CIPFA is working with the Home Office and the National Crime Agency on the government's response to anti-corruption, procurement fraud and threats, and will be providing tools and resources in this area.

CIPFA Better Governance Forum

The CIPFA Better Governance Forum is a network for governance practitioners covering governance, internal audit, risk management, counter fraud and audit committees.

International Framework: Good Governance in the Public Sector (CIPFA/IFAC)

The aim of the International Framework is to encourage better service delivery and improved accountability by establishing a benchmark for aspects of good governance in the public sector.

CIPFA's TISonline Risk Management and Counter Fraud Information Stream

The TISonline Risk Management and Counter Fraud information stream outlines the major issues to consider when developing an integrated risk management framework. It also identifies the main areas where local authorities face significant losses due to fraudulent activity and provides guidance to help create an effective counter fraud culture.

OTHER RESOURCES

Fighting Fraud Locally

Fighting Fraud Locally: The Local Government Strategy (NFA, 2012) is a strategic approach developed by local government for local government and addresses the need for greater

prevention and smarter enforcement. Further Fighting Fraud Locally resources can be found on the CIPFA Counter Fraud Centre.

Audit Commission

Protecting the Public Purse

The Protecting the Public Purse reports describe what has happened in the field of fraud detection and prevention and identify fraud risks. They also describe the action taken by some councils to tackle fraud and provide links to tools to help councils improve their counter fraud defences.

National Fraud Initiative

Since 1996 the Audit Commission has run the National Fraud Initiative (NFI), an exercise that matches electronic data within and between public and private sector bodies to prevent and detect fraud. This includes police authorities, local probation boards, fire and rescue authorities as well as local councils and a number of private sector bodies.

Cabinet Office

Tackling Fraud and Error in Government: A Report of the Fraud, Error and Debt Taskforce (2012) sets out an ambitious but focused delivery programme that seeks to reduce levels of fraud and error across government.

Department for Communities and Local Government

Government Response to Social Housing Fraud – Presentation.

Financial Reporting Council

International Standard on Auditing (UK and Ireland) 240 establishes standards and provides guidance on the auditor's responsibility to consider fraud in an audit of financial statements.

HM Treasury

Managing Public Money (2013) offers guidance on how to handle public funds.

London Public Sector Counter Fraud Partnership

The London Public Sector Counter Fraud Partnership (LPSCFP) has been in existence since 2000. It was formed in response to the Crime and Disorder Act 1998 and is a partnership between the Metropolitan Police and the other counter fraud public sector agencies and teams in London. Its aim is to combat fraud by working in partnership across London.

British Universities Finance Directors Group

Managing Fraud and Risks in Construction Projects is available to members of the British Universities Finance Directors Group (BUFDG). See their website for more information.

NHS England

Tackling Fraud, Bribery and Corruption: Policy and Corporate Procedures (2013) aims to explain how NHS England intends to tackle economic crime, provides guidance to officers and ensures officers are able recognise economic crime and understand the correct reporting requirements.

NHS Protect

Standards for Providers 2014/15 – Fraud, Bribery and Corruption aims to provide information on the anti-fraud and security management clauses in the 2014/15 NHS Standard Contract, and explain what providers need to do to comply with them.

National Audit Office

The National Audit Office's fraud website contains a number of reports covering areas such as whistleblowing, tax credits error and fraud and good practice in tackling external fraud.

National Crime Agency

The National Strategic Assessment of Serious and Organised Crime 2014 provides a single, comprehensive picture of serious and organised crime affecting the UK and is a key document in the reporting and priority setting cycle.

Metropolitan Police Service

The Little Book of Big Scams is a general guide to many of the scams currently operating in the UK.

CIPFA The Chartered Institute of Public Finance & Accountancy

Registered office:
3 Robert Street, London WC2N 6RL
T: +44 (0)20 7543 5600 F: +44 (0)20 7543 5700
www.cipfa.org

From 1 January 2015:
77 Mansell Street, London E1 8AN
T: +44 (0)20 7543 5600 F: +44 (0)20 7543 5700
www.cipfa.org

CODE OF PRACTICE ON MANAGING THE RISK OF FRAUD AND CORRUPTION \ GUIDANCE NOTES

CIPFA\