First Edition

Fraud Proofing Policies and Processes

Integrity Matters

Financial Crime Management Group Ltd

Forward

Fraud Proofing Policies and Procedures is just one element of an effective fraud strategy.

Visit our Fraud Management Resource Centre which brings together four key elements to help you and your company prevent, deter, and respond to fraud.

1. A comprehensive and up to date Resource Centre gives you the tools you need.
2. Our unique guide will direct you through industry best practice with clear links through to the resources and how to use them effectively.
3. Our Organisational Capability Self-Assessment Tool to help you assess your organisation's strengths and weaknesses in fraud management arrangements.
4. Our update and news all contain clear links through to relevant sections of the guide which is regularly updated to reflect that latest news and topics of interest.

Fraud Management
Resource Centre

Identify fraud risks

1

Consider what fraud risks exist

Step 1

Identify Fraud Risks

Through interviews and scrutiny of the relevant policy documents and procedures consider what fraud offences could occur as a result of system weaknesses or loopholes in those policies and procedures.

Other Information to consider:

- **Industry specific reports of frauds in the area under review**
- **General reports of frauds in the area under review**
- **Results of previous audits**
- **Lessons to be learnt from previous incidents of fraud**

Possible Fraud Offences

Fraud by false representation

Fraud by failing to disclose information

Fraud by abuse of position

Bribery

Computer misuse including data theft

Anti-competitive practices

Obtaining services dishonestly

Theft

False Accounting

Step 2

Identify Methods

Consider whether any of the following methods have been used or could be used and whether revisions/amendments could be made to the policy to prevent use in the future.

Possible methods

Fraudulent instruments: forged or counterfeited documents such as driving licenses, invoicing, receipts, tax documents, forms, certificates or qualifications, training courses undertaken, birth, death and marriage certificates, and forms of ID such as passports, National Insurance cards, NHS cards etc.

Fraudulent statements: forged or counterfeited documents (as listed above) which are linked to a statement being made by an individual.

Fraudulent disbursements: forged payee name or endorsement of payments, reissuing of old outstanding cheques, fraudulent wire or account transfers, petty cash disbursements, false vendor payments, forged payroll cheques, payroll disbursements, expense report fraud, credit card processing, credits issued to accounts or paid in cash.

Asset misappropriation: the misuse or theft of assets belonging to the organisation, such as specialist equipment, laptops, furniture, and documents.

	Common Examples
Customers	Mostly relating to fraud such as credit card, ID theft, account takeover, false refunds.
Managers and Staff	**Timesheet fraud** including false claims for overtime or claiming for additional hours. **Theft of Assets** including the use of assets for personal gain or the misappropriation of the assets for personal use. **False expense claims** including claiming excessive mileage and claiming for private journeys or expenditure **Bribery** including staff receiving gifts and hospitality from suppliers or contractors in exchange for contracts for work or orders for supply of goods. The **non-disclosure of personal interests** e.g. in regards to the firm's suppliers. **Contract fraud** includes the acceptance of late tenders or where tender records are falsified or manipulated by staff.
Suppliers	A contractor may submit **false timesheets** to claim for work not done. Supplier Fraud includes submission of **false or duplicate invoices** . Alternatively a contractor or supplier may **supply substandard products** and pass them off as products of a higher quality. **Procurement Fraud** includes contracted suppliers making false declarations or withholding relevant information as part of their application for a contract. **Collusion** between contractors in the contract tendering process in order to drive up costs.
Organised Crime	**Contract Fraud** including claims for work not done **Personal Data theft** **Money Laundering** **Bribery**

Identify Existing Prevention Controls

2

The next stage is to consider whether suitable fraud prevention controls already exist or need to be incorporated within the policy.

Step 3

Identify Existing Prevention Controls

The next stage is to consider whether suitable fraud prevention controls already exist or need to be incorporated within the policy.

The following four areas should be considered when fraud-proofing:

1. Are clear rules and procedures/processes in place?
2. Is there sufficient accountability?
3. What monitoring arrangements exist?
4. Are sanctions in place?

The following pages provide further details of each of these four areas

Are clear rules and procedures/processes in place?

Producing a set of clear rules or guidance to underpin the simplest or most complex policy reduces ambiguity which will help to minimise mistakes. It also makes it more difficult for a reasonable excuse to be provided when someone is suspected of defrauding.

Wherever a claim or application is made, systems should be designed to require original evidence to support the claim. For example, this could be receipts for expenses claims or a counter signature on a timesheet for agency staff. Providing evidence to back up a claim or exemption will help validate any payment and also make monitoring more effective.

Systems should be as simple and clear to use as possible and actions to defraud made as difficult as possible. This all helps to make it clear what a person should and shouldn't do.

Is there sufficient accountability?

This could be signing a proper declaration to confirm that the details someone has provided in an application or claim are correct; that they are aware of the consequences if they have provided false information; and that they permit the sharing of relevant details in the claim or application to enable effective monitoring to take place.

A good declaration will help to deter some who may be tempted to defraud; it will assist with an investigation in ensuring that the person is accountable for their actions; and it will ensure any legal issues regarding the monitoring arrangements are dealt with properly.

Of course some systems and processes will not easily lend themselves to declarations on forms for each transaction, so consideration needs to be given to contractual terms for individuals or companies and to retaining a proper audit trail of instructions and acknowledgements of those instructions.

What monitoring arrangements exist?

Any system involving payment of money, claims or granting application is at risk from fraud, so effective monitoring needs to take place to identify any such potential fraud or error. Checks should validate the claim or payment against original documents and evidence to support the transaction. A good monitoring system will ensure an appropriate percentage of checks are undertaken which may be from a random sample or targeted at the highest risks.

The monitoring system should have a process to refer any suspicions of fraud to the designated person. The outcome of any anomalies found from the monitoring should inform revisions to the policy or procedure and guidance discussed above.

Are sanctions in place?

Even with clear rules, accountability and monitoring in place, instances of fraud can still occur. Where fraud is not prevented or deterred and the monitoring identifies a case of fraud, appropriate sanctions will need to be considered. This may include criminal, disciplinary, regulatory or civil proceedings to recover any losses following an investigation. However, when developing a policy or system, consideration may also be given to including a sanction specifically for that process, for example removal from a particular scheme.

Sanctions have the added effect of acting as a deterrent to would-be fraudsters because they represent real repercussions should the fraud be proven. In order to achieve this, the system of sanctions available must be well publicised.

Identify Further Controls

3

Identify and put in place further counter fraud solutions

Step 4

Identify Further Counter Fraud Controls

If any of the controls described above are missing or need to be more robust, consideration should be given as to whether any of the following controls or counter fraud processes can be put in place.

Once the appropriate controls have been identified, the existing policy should be revised. Furthermore, there is a need to ensure that these controls are put into practice, by enlisting the support of managers and training staff.

Controls

Safeguarding assets

Separation of duties

Reconciliation of records

Pre- and post-payment verification

Monitoring by managers

Spot checking of output

Scheme of delegation

Allocated roles

Reporting

Liaison

Supervision

Authorising

IT access controls

Budgetary controls

Stocktaking

Audit trails

Recruitment

Procurement

Examination of documentation

Examination of cancelled cheques

Independent verification

Job and vendor rotation

Review Effectiveness

4

Review and evaluate the effectiveness of fraud-proofing measures

Step 5

Review And Evaluate The Effectiveness Of Fraud-proofing Measures

Counter-fraud controls that are successfully implemented in policies are not necessarily the best ones possible.

Finally review the effectiveness of fraud-proofing efforts through consideration of the following points.

1. Do the new controls meet the counter-fraud needs of the organisation with respect to a specific policy or policies, i.e. reducing fraud to a minimum?
2. Do they inhibit the smooth operation of procedures?
3. Are there sufficient levels of compliance by managers and staff?
4. Do managers and staff understand and agree with the purpose of the counter-fraud controls?

Step 6

Periodic Reviews

The organisation should conduct periodic reviews aimed at assessing the usefulness of the newly implemented counter-fraud measures (in addition to examining new policies and procedures for potential weaknesses). Any problem areas should inform the fraud-proofing process on a continual basis and determine whether additional risks call for further counter-fraud controls or policy revision.

Anti-competitive practices

Enterprise Act 2002

The above legislation covers ‘cartel’ offences.

Involves two or more people dishonestly agreeing to engage in:

- Price Fixing – agreeing prices with competitors
- Market sharing – contractors agreeing to divide contracts between themselves
- Limitation of production or supply - agreeing to limit availability of contractors to drive up price
- Bid rigging – paying money to rivals to stay out of tenders

These are all potential frauds related to any form of tendering for contracts

---

Related Glossary Terms

Drag related terms here

Index Find Term

Bribery

Bribery Act 2010 Offences

Section 1 Offences of bribing another person

This offence relates to a person offers, promises or gives a financial or other advantage to another person, and intends the advantage to either:

a) induce a person to perform improperly a relevant function or activity, or

b) to reward a person for the improper performance of such a function or activity.

Section 2 Offences relating to being bribed

This offence relates to a person who requests, or agrees to receive or accepts a financial or other advantage intending that, in consequence, a relevant function or activity should be performed improperly.

Section 6 Bribery of Foreign Public Officials

A person who bribes a foreign public official is guilty of an offence if they directly or through a third party, offers, promises or gives any financial or other advantage with the intention of influencing a foreign public official in order to obtain or retain business, or an advantage in the conduct of business.

Section 7 Failure of commercial organisations to prevent bribery

A relevant commercial organisation is guilty of an offence under this section if a person associated with the organisation bribes another person intending to obtain or retain business for the organisation, or to obtain or retain an advantage in the conduct of business for the organisation. But it is a defence for the organisation to prove that it had in place adequate procedures designed to prevent persons associated with it from undertaking such conduct.

Related Glossary Terms

Drag related terms here

Index Find Term

Chapter 1 - Step 1

Computer misuse including data theft

Computer Misuse Act 1990 Section 1

It is an offence for a person to cause a computer to perform any function with the intention of securing access to programs or data where access is unauthorised and they know at the time that this is the case. This can include access to use information and includes copying, moving or printing information.

Computer Misuse Act 1990 Section 2

Section 2 relates to a person who has committed an offence under Section 1 of the Act as set out above, with the intention of committing a further offence or to facilitate such a further offence.

Related Glossary Terms

Drag related terms here

Index Find Term

False Accounting

Theft Act 1968 Section 17 False Accounting

An offence is committed if a person dishonestly, with a view to making a gain for themselves or another, or intent to cause a loss to another: destroys, defaces, conceals, falsifies, produces or makes use of any account which they know or suspect is false.

Related Glossary Terms

Drag related terms here

Index Find Term

Chapter 1 - Step 1

Fraud by abuse of position

Fraud Act 2006 Section 4 Abuse of Position

The offence of Fraud by abuse of position requires the person to be in a position in which he is expected to safeguard, or not act against, the financial interests of another person; and he must abuse that position. Such positions include: employee and employer, trustee and beneficiary, director and company, professional and client. Internal corruption by an employee will usually fall within this category.

Related Glossary Terms

Drag related terms here

Index Find Term

Chapter 1 - Step 1

Fraud by failing to disclose information

Fraud Act 2006 Section 3 Failure to Disclose

The offence of Fraud by failure to disclose information involves a legal duty to disclose that information. This duty is not specifically defined but may derive from statute, an utmost good faith transaction, custom, or the terms of a contract.

Related Glossary Terms

Drag related terms here

Index Find Term

Chapter 1 - Step 1

Fraud by false representation

Fraud Act 2006 Section 2 False Representation

In relation to the offence of fraud by false representation, a person commits fraud if he dishonestly makes a false or misleading representation as to fact or law, intending to make a gain for himself or another, or to cause loss to another, or to expose another to a risk of loss. The representation may be express or implied and may include a representation made to a machine, covering cash point transactions and trading over the internet.

Related Glossary Terms

Drag related terms here

Index Find Term

Chapter 1 - Step 1

Obtaining services dishonestly

Fraud Act Section 11 obtaining services dishonestly.

Obtains services for themselves by a dishonest act, knowing that the services are made available on the basis of payment and avoids or intends to avoid payment in full or in part.

Related Glossary Terms

Drag related terms here

Index Find Term

Chapter 1 - Step 1

Theft

Theft Act 1968 Section 1 Basic Theft

An offence is committed if a person dishonestly appropriates property belonging to another with the intention of permanently depriving the other of it.

Related Glossary Terms

Drag related terms here

Index Find Term

Chapter 1 - Step 1