Good Practice in Tackling

External Fraud

November 2005

A Paper from the FEE Public Sector Committee

CONTENTS

INTRODUCTION

1. This paper[1] concentrates on external fraud which is where third parties, such as organised crime groups, dishonest businesses or individuals, take money from public sector entities or organisations, either by obtaining payments to which they are not entitled or keeping monies they should pay over to the department. Frauds may be opportunistic attempts by individual customers or businesses to obtain a financial advantage. The sums involved in any one such case may be small, but these can mount up to significant losses of public money if there are a lot of cases involved. At the other end of the scale, public sector entities or organisations may suffer from more systematic and premeditated attacks by organised crime groups. These may be fewer in number but the losses in each case are substantial. In some cases fraudsters may work in collusion with the organisation's staff. As well as diverting money that should be spent on public services fraud can undermine the position of honest citizens and businesses and support the activities of those involved in other serious crime. All public sector entities or organisations have a responsibility to develop anti-fraud policies to show those seeking to defraud the government that such action is unacceptable and will not be tolerated.

2. Public sector entities or organisations face a wide range of different risks from external fraud which are demonstrated in Figure 1. Public sector auditors need to be aware of such risks. There are also many other types of fraud perpetrated by third parties, such as fraud by contractors. In some organisations external fraud is a sizeable and continuing problem for their main business but in others it may only occur occasionally.

Figure 1: Example of the diversity of external frauds faced by the public sector

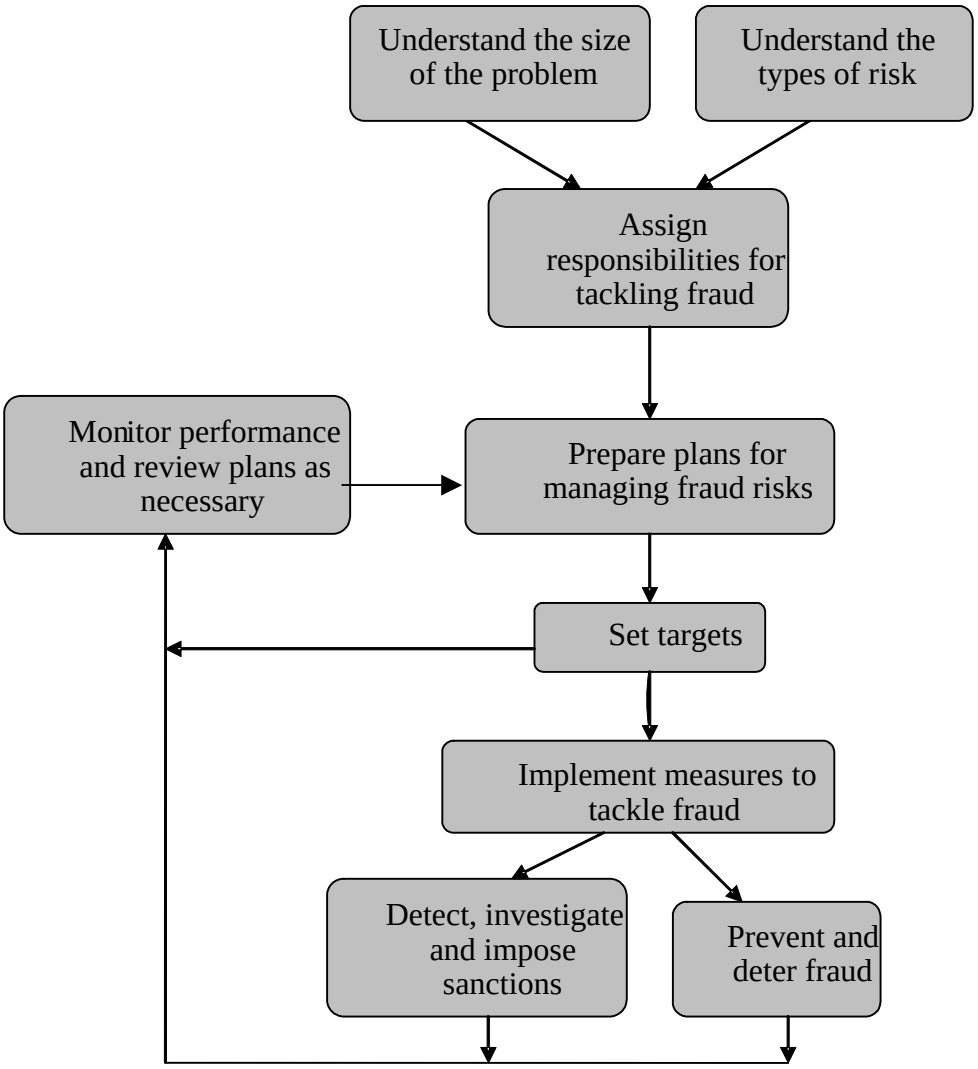
- People or businesses who claim grants to which they are not entitled;
- People who work in the shadow economy and do not pay income tax or national insurance contributions on their earnings. They may also claim means tested benefits to which they are not entitled;
- Businesses which operate in the shadow economy and do not declare their activity or pay the relevant taxes or VAT;
- Staff colluding with criminals to defraud a government organisation;
- Serious criminals obtaining large sums, for example, through evading tobacco, alcohol and hydrocarbon oil duties. They may set up what appear to be legitimate companies but intend to carry out frauds on the tax authorities, such as to steal VAT. They may also commit organised fraud against the benefit system through stolen, forged or counterfeit instruments of payment and through creating fictitious benefit claim;
- Systematic exploration of weaknesses in government social and other programmes to obtain unjustified benefits or avoid contributions, such as:

[1] This paper is based on a guide published by the UK National Audit Office and UK HM Treasury under the title "Good Practice in Tackling External Fraud".

- Benefit claimants who fail to declare all earnings, income or capital, or who conceal family circumstances, to obtain benefits to which they are not entitled;
- People who claim exemption from paying for prescriptions to which they are not entitled;
- People who evade vehicle excise duty.

3. Organisations should consider whether they need to develop a package of measures specifically tailored to each type of fraud. There will not be a one size fits all approach. But there is much value in promoting a wider understanding of how others tackle fraud and good practices which are successful elsewhere. Smaller organisations should consider whether they can adapt and apply practices used by larger organisations in tackling external fraud. The paper describes an integrated strategic approach which is summarised in Figure 2.

Figure 2 shows the main elements of an integrated strategic approach to tackling fraud



4. The paper is structured as follows:

   - Understanding and managing the risks of external fraud (Part 1);
   - Preventing and deterring external fraud (Part 2);
   - Detecting and investigating fraud and imposing sanctions (Part 3).

   Questions at the beginning of each Part are to help assessing the organisation's practices. If particular practice is not used, one needs to consider whether that is appropriate given the circumstances[2].

5. We hope that the paper is a useful source of reference for public sector managers in demonstrating the experience and good practice of others. It does not seek to provide "everything you need to know" to tackle external fraud. To do so would require many volumes. The case examples in the paper are for illustrative purposes only. There may be many other examples in use in other public organisations.

[2] In the discussions on fraud, money laundering is increasingly becoming an issue and it can be defined as the processing of criminal proceeds to disguise their illegal origin. This paper concentrates on the prevention and detection of fraud and not on the proceeds.

PART 1: UNDERSTANDING AND MANAGING THE RISKS OF FRAUD

One needs to consider whether the organisation:

- Takes a strategic approach to tackling fraud risk;
- Assesses the size of the threat from external fraud and, where significant, undertakes a separate fraud risk assessment;
- Identifies the areas most vulnerable to the risk of fraud;
- Knows the size of the fraud threat / types of fraud committed/ who is committing them/ how often/ and how much is involved;
- Has a package of measures in place to tackle losses from fraud where these are significant;
- Has targets to stabilise (avoidance of further increase of fraud) or reduce fraud;
- Has allocated responsibilities for tackling, and ownership of, fraud risks to ensure that risks are managed, plans are implemented and progress monitored.

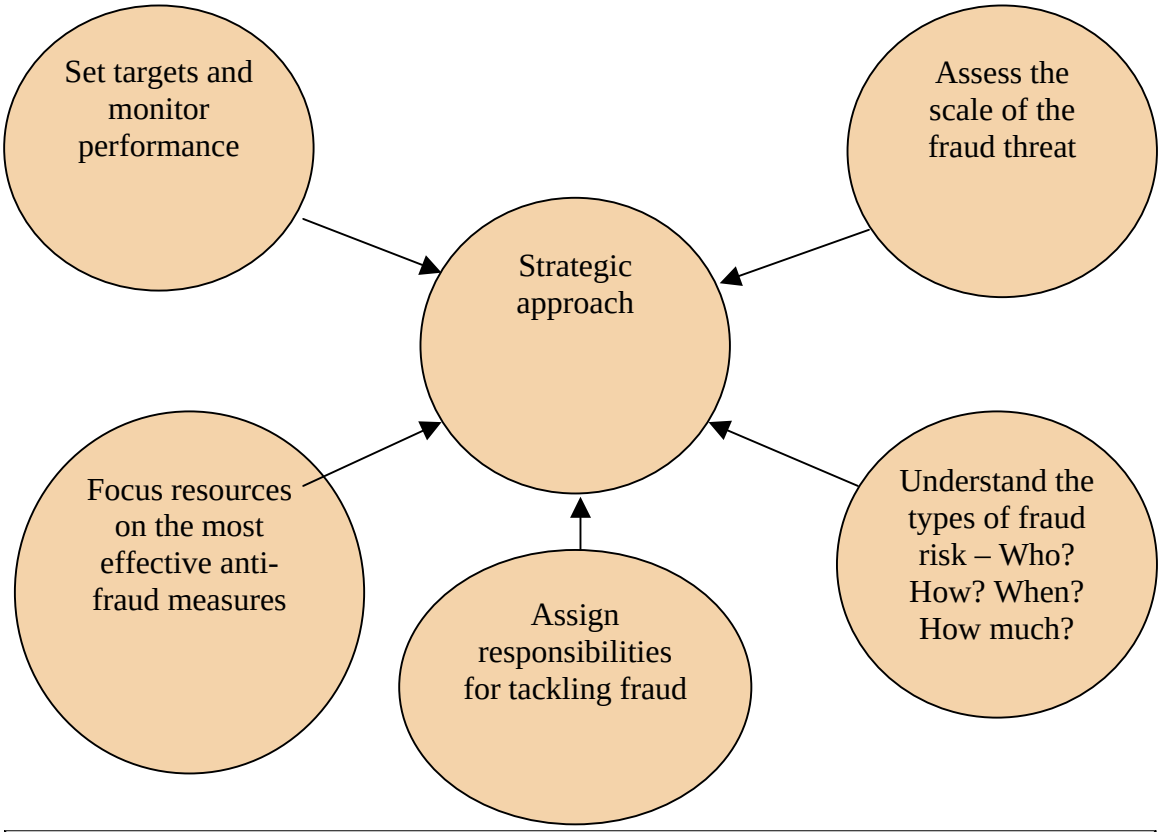
This Part of the paper looks at how one can tackle some of these issues and gives examples of how others approach these issues. The paper needs to be read considering how appropriate the practices are to the circumstances.

Taking a strategic approach to tackling external fraud

1.1 Some organisations have taken a strategic approach to understanding and managing the risks of fraud because this:

- Fits in with good corporate governance. A major element of good corporate governance is a sound assessment of the organisation's business risks. Fraud risk should be managed in the same way as managing any other business risk and should therefore be approached systematically at both the organisational and operational level;
- Helps with developing a range of measures which apply proportionate and well targeted pressure at all levels of the problem;
- Can help achieve a cost effective approach in tackling fraud by focusing on areas of greatest risk and where efforts may have the greatest impact. A strategic approach can provide, where needed, a rational and robust basis in bidding for additional resources to tackle fraud;
- Can be a helpful way of communicating to staff what the organisation is trying to do and what is expected from them. Some organisations have also published their strategies as a way of informing the public that they have a well thought out approach to tackling external fraud. This can also send a deterrent message to potential fraudsters that they are less likely to succeed in attempts to commit fraud against the organisation. Figure 3 shows the main elements of a strategic approach to tackling external fraud.

Figure 3 shows the main elements of a strategic approach to tackling external fraud



1.2 In taking a strategic approach, some organisations have taken an across the board approach to looking at external fraud, and some have looked at individual fraud risks and produced a strategy for each. Others tackle fraud within the context of an overall strategy to combat losses from all types of non-compliance. The overall compliance approach recognises that there is a 'loss continuum' ranging from inadvertent customer error at one end of the spectrum to fraud at the other with shades of grey in between. All of these approaches can be equally valid depending on an organisation's circumstances and the stage they are at in developing their approach. However, a common feature is that the organisations develop fraud risk assessment tools to identify the fraud risks, their likelihood and impacts, and how to manage them. These tools need to be reviewed to assess whether they remain appropriate or require updating to respond to the threat from new fraud risks.

Assessing the scale of the fraud threat

1.3 Assessing the scale of loss from fraud is an important first step in developing a strategy for tackling external fraud. An estimate highlights the scope for potential savings which can then help to determine the relative priority that should be given to tackling fraud in the context of all the other calls on an organisation's resources. Such estimates then establish a baseline against which performance can be judged. If repeated at intervals, estimates can help an organisation assess how well they are doing and whether the threat is changing. There may be circumstances where an

organisation decides it is not practicable to produce overall estimates. Nevertheless they may be able to use a range of techniques such as carrying out in-depth research into an area where fraud is suspected to gain a better understanding of the scale and nature of the threat.

1.4 Some may say that:

- It is too difficult to produce estimates of fraud and that it is not worth attempting to do so;
- The resources used to produce an estimate could be better used on tackling fraud, for example, by carrying out more investigations.

These issues are dealt with below.

Producing reliable estimates

1.5 Estimates of fraud or losses from fraud and error can be produced by using operational research and statistical methods to produce such estimates. Two main methods used are ***statistical modelling*** and ***sampling***.

Statistical modelling

1.6 Statistical modelling has been used to produce overall estimates of fraud or loss notably on revenue activities. This involves comparing levels of actual receipts or expenditure with the total level of receipts or expenditure that might be expected using other sources of data on the level of activity under review.

1.7 Points to consider for statistical modelling are:

- The data required may be incomplete. Therefore, the model may use a number of assumptions which mean that the results are subject to a margin of error. It is important to take this into account when making decisions on actions to reduce losses;
- Other work may be needed to give an insight into those committing the fraud or the type of action that might deter them. This may include more in depth modelling work;
- Further research may be needed into the causes of increases or decreases in the level of losses and the extent to which this is due to anti-fraud measures implemented.

Sampling

1.8 Estimates of loss can be generated by checking a representative sample of cases to see whether fraud is involved, and extrapolating the results to the whole population to estimate the total level of fraud loss in the area of expenditure or revenue. When checking individual cases it can be difficult to determine whether any discrepancy is due to fraud or error (recklessness, carelessness or ignorance) because of the judgements that need to be made.

1.9 A key consideration in producing an estimate of fraud loss on an area of expenditure/ revenue is the level of accuracy required. A greater degree of precision produces more reliable estimates (essential for assessing any real change in the level of fraud over time) but at additional cost because the size of the sample required increases. For some organisations, producing a national estimate may be sufficient. In others, it may be necessary to produce estimates which are also broken down by region.

This will have important implications for the sampling exercise and its costs, as separate samples within each region increase the total sample that must be checked.

Costs of estimating fraud

1.10 As indicated above, the costs of measurement vary according to:

- The frequency of the estimating exercise;
- The sample sizes checked;
- The work involved in checking each case sampled;
- The work involved in validating the results.

1.11 For smaller organisations, a one-off estimate or one produced at intervals may be sufficient. Accepting less precision by using smaller sample sizes may be one way forward. Although the results will be less reliable, these will indicate whether further work is desirable. Others may require continuous measurement exercises to produce ongoing estimates of fraud loss. While this involves greatest cost, it does mean that a department is able to track changes over time in the estimated fraud loss, and the types of fraud committed.

1.12 Costs can be spread over several years by carrying out a rolling programme of estimates. Another alternative is to carry out a one-off measurement exercise (with possible follow up several years later) to confirm the significance of the level of fraud. This can be a useful approach where the level of fraud is thought to be less significant.

Understanding the types of fraud risks

1.13 An organisation will be unable to develop an appropriate response based only on the estimates of fraud. They also ideally need to know:

- The types of fraud perpetrated against them, for how long and the financial loss involved;
- Who the fraudsters are, their characteristics and behaviours, how often they carry out the frauds, which types of frauds they commit, how they do it, and whether they are opportunistic or organised.

1.14 Examination of detected fraud cases either from investigation or from the random samples of cases examined to produce estimates of fraud loss, can give an insight into these. Larger organisations which face serious threats also have intelligence analysts and/or commission research into the threats. At the other end of the spectrum, there are some organisations that may have few or no recent instances of external fraud. Checking a sample of cases, or carrying out research into the possible threats, will help to confirm whether the risks from fraud are low.

Focusing resources on the most effective anti-fraud measures

1.15 There is no single package of measures which can be applied universally by organisations to tackle fraud. Measures need to be tailored to the type and size of threat faced. In deciding which measures to use and the extent to which to use them some organisations have assessed the savings that could be achieved by targeting their resources in a better way. Savings could arise in three ways:

- The direct effects from recovering amounts defrauded. Where the measures involve reallocating resources into existing activities the department can look at the current costs/savings as a basis for estimating the return from increasing the levels of counter fraud activity. Where new measures are proposed, it is good practice to pilot these beforehand to test and refine their operation, assess their likely effectiveness and the type of savings that can be achieved;
- The preventive effect, through improved future compliance from those previously detected committing fraud;
- The deterrent effects on others that become more compliant as they learn of the greater efforts being taken to crack down on fraud. In practice it can be very difficult to assess these deterrent effects with any accuracy.

Setting targets and monitoring performance

1.16 Some organisations set targets to stabilise (avoidance of further increase of fraud) or reduce fraud over a period of time. Focusing targets on the overall level of fraud or loss is a good way of assessing performance, and generally a better measure than the amount of fraud or loss detected. The latter is difficult to interpret if the full scale of fraud or loss is not known. Other measures of performance are useful complements to estimates of total fraud loss, such as changes in regional levels of loss, the cost of tackling fraud compared to the return obtained and the rate of recovery of detected frauds.

1.17 Performance data on outcome targets may not be available until long after the period measured due to the amount of work involved in sampling cases, checking, calculation and validation of the results. To monitor performance in-year, managers may rely on output results to indicate whether the outcomes are likely to be achieved. For example, managers may monitor:

- The results of operational checks on transactions;
- Fraud investigation activity and outcomes;
- Number and types of sanctions imposed;
- Rate of recovery of defrauded amounts detected.

Assigning responsibilities for tackling fraud

1.18 The responsibility for tackling fraud and managing fraud risks start at the top of the organisation within the senior management board. At this level, ownership of fraud risks is assigned and responsibilities allocated for managing individual fraud risks. Although everybody in the organisation has a role to play in tackling fraud, some organisations have also set up central units or focal points with responsibility for tackling external fraud. These have coordinated work on developing the department's strategies' ensuring their implementation, monitoring results and providing advice and guidance. Fraud can be a moving target as the scale and nature of the risks change, so that regular monitoring of the situation is needed to identify and respond to new threats. Where fraud numbers and losses are significant, organisations also have teams of professionally trained investigators or enforcement officers dedicated to investigating cases of fraud.

1.19 Regardless of the arrangements in place, organisations need to ensure that someone is fully responsible for implementing the plans for tackling fraud in the way intended and that sufficient resources are in place. Someone should also be responsible for performance against targets. There is no point in having a well thought out strategy if it is not then put into effect.

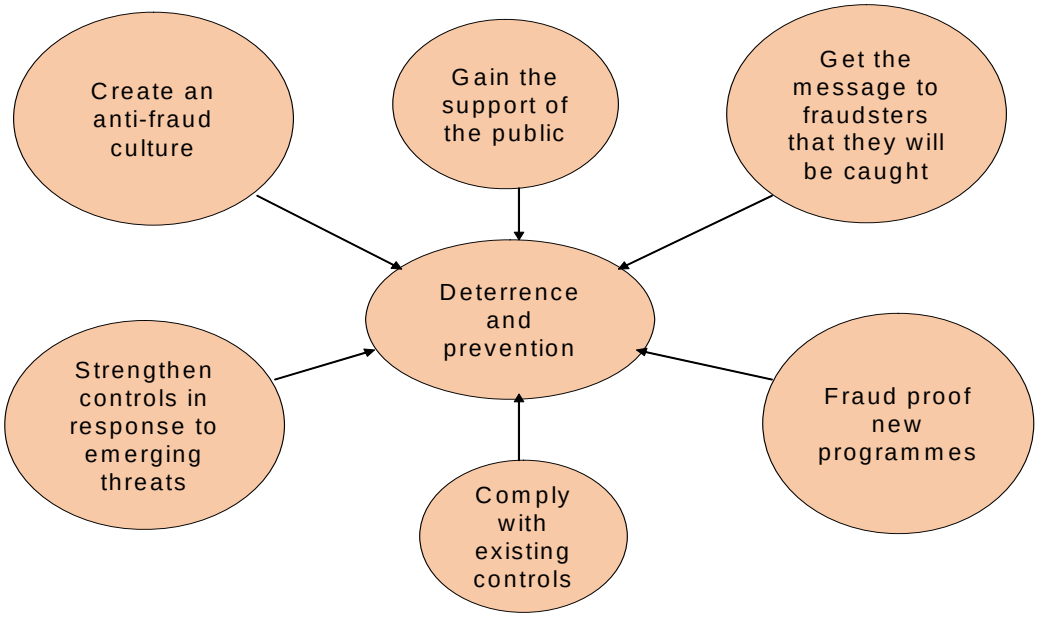
PART 2: DETERRING AND PREVENTING EXTERNAL FRAUD

2.1 **Deterrence** involves convincing potential fraudsters that frauds against a department or agency are not worthwhile. **Prevention** measures aim to stop frauds entering organisation's systems. Effective mechanisms for deterring and preventing fraud are essential elements in combating fraud. Realistically however, some fraudsters will never be deterred and not all frauds will be prevented. In these cases, prompt detection and professional investigations are needed (Part 3). Measures to deter and prevent fraud can be costly and organisations need to ensure they are well designed for greatest effectiveness. Figure 4 sets out the main elements for deterring and preventing fraud.

One needs to consider whether the organisation:

- Seeks to influence customers' and the wider general public's attitudes to fraud;
- Sends a strong message to potential fraudsters that they are likely to be caught and sanctions will be imposed. For example are there press releases on people/businesses prosecuted and are their any targeted or wider campaigns regionally or nationally;
- Considers the fraud proofing of new programmes;
- Ensures fraud controls are applied consistently and their use is monitored. What is the role of Internal Audit in this?
- Considers strengthening controls where new fraud risks appear or where fraud starts to escalate;
- Has an anti-fraud culture where staff understand the standards of conduct required and their personal responsibilities in preventing fraud; applying controls and reporting cases of suspected fraud.

Figure 4: The main elements for deterring and preventing fraud



Changing public attitudes to fraud

2.2 Organisations can seek to influence the attitude of customers and the wider general public to fraud by deterring those who might consider committing fraud and by making fraud socially unacceptable. The aim should be to get public support in the efforts to tackle fraud. Some deterrents are:

- Strong controls will stop them from succeeding; followed by
- It is likely they will be caught;
- Evidence of their fraud will then be discovered;
- They will thus face penalties; and
- Amounts defrauded will be recovered.

2.3 Organisations can use a variety of methods to publicise the success of their work, such as issuing press releases and putting information on their websites of cases prosecuted. These are cost effective actions which can be used by smaller organisations.

2.4 To maximise the deterrent effect, organisations can have:

- Researched fraudster behaviour and risk taking / aversion to determine which messages will be most effective in changing their behaviour;
- Designed media messages to achieve maximum effect;
- Used relevant media to ensure potential fraudsters are aware of these messages;
- Refreshed messages regularly to maintain a strong deterrent effect;
- Developed performance indicators to evaluate the effectiveness of the approach. It can however be difficult to make a direct link between the campaign and reductions in fraud levels, because of other anti-fraud measures also in force;

- Fed back the evaluation into renewed campaigns to deter fraudsters.

Changing staff attitudes to create an anti-fraud culture

2.5 Creating an anti-fraud culture, in which all staff understand the standards of conduct required, their personal responsibilities in preventing fraud and the importance of controls, is vital in preventing external fraud. Publicising internally the organisation's strategic approach to tackling fraud and what it is trying to achieve can be a good way of reinforcing the anti-fraud culture.

2.6 Training can help raise staff awareness of the risks of external fraud and the importance of compliance with internal control procedures and security checks to prevent such frauds. And close monitoring of staff compliance with these controls helps ensure their consistent application. Training may take several forms such as:

- Fraud awareness workshops for a wide range of staff;
- Targeted personal mentoring for staff working in areas found to be vulnerable to fraud;
- Closer managerial supervision with feedback to staff on their compliance with security procedures.

2.7 A staff survey or focus group may be used to test staff attitudes to security, and their compliance with controls to prevent fraud. The findings from such research can help identify opportunities to improve prevention and to strengthen internal controls, identify any messages that need to be reinforced, reveal any areas where compliance with prevention controls is insufficient and generate further information about the frauds identified by staff.

Controls to prevent fraud

2.8 There are a range of controls (for example, physical checks, reconciliation, supervisory checks and clear roles and responsibilities) that address risk, including fraud. Organisations need to consider which controls are most appropriate in their particular circumstances. The consistent application of internal controls can be highly effective in preventing fraud losses. Internal Audit should provide assurance on the operation of those controls and their effectiveness in preventing fraud. Internal controls can impose both internal and external costs from their operation. Controls need to be designed which are proportionate to the risk, while enabling the organisation to deliver the services to its customers to meet their needs.

2.9 Two key aspects to prevention are:

- "Fraud-proofing" new programmes and systems;
- Consistent application of existing controls and strengthening of these where needed.

Fraud proofing new programmes and systems

2.10 Organisations need to recognise their responsibility when designing and implementing new policies, programmes and systems to build good controls in to manage fraud where there are vulnerabilities or to fraud proof them by designing them to be inherently less vulnerable to fraud. Complex rules can increase the risks of fraud. Fraudsters can exploit the situation in two ways. The rules may be difficult to police effectively, requiring officials to consult volumes of guidance in their everyday work. Where customers are often uncertain of their obligations, it is easier for fraudsters to misrepresent their circumstances and if discovered claim that it was a genuine error.

2.11 Sufficient weight should be given to expert advice on the risks of fraud in new programmes and effective counter fraud measures should be integrated into the design. Where innovative schemes are being proposed, it is good practice to pilot these to identify any further risks of external fraud. Early consultation with internal audit and counter fraud specialists can help to identify the risks, and to obtain advice on how these can be minimised, at key stages during design and implementation of new programmes. An evaluation process is helpful in determining whether early risk assessments have been effective in countering fraud risks during development, piloting and initial implementation.

Strengthening internal controls and checks

2.12 It is important that the effectiveness of controls is continually reviewed. Controls which have traditionally worked well in countering fraud may no longer be effective where fraudsters have launched determined attacks. Detected cases of fraud may show that fraudsters are using new methods to circumvent controls indicating that these need to be strengthened. Internal Audit's work may also identify system weaknesses which could lead to fraud.

2.13 Strengthening internal controls can also help prevent or reduce criminal attacks. New legislation may be required to improve controls or to deter fraudsters. Developments in technology can provide opportunities to strengthen controls in a cost effective manner to reduce the level of external fraud.

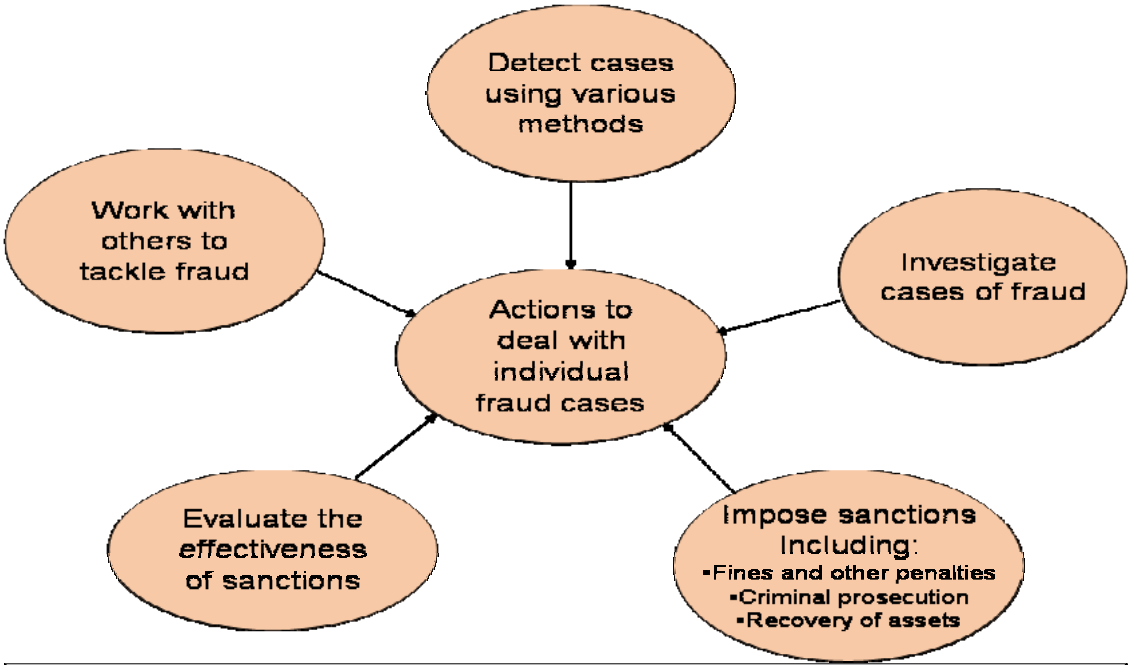
PART 3: DETECTING AND INVESTIGATING EXTERNAL FRAUD AND IMPOSING SANCTIONS

One needs to consider whether the organisation:

- Has a well publicised telephone hotline, email and freepost address to which the public can report cases of suspected fraud;
- Uses techniques proactively to detect cases of suspect fraud such as in-depth investigative work into "hotspot" areas, data matching exercises, data mining and neural networks as appropriate;
- Assesses whether suspect cases of fraud need to be investigated further such as through use of scoring systems;
- Assesses whether the number of investigations is proportionate to the potential sums lost from fraud;
- Tracks the progress of individual investigations;
- Has sufficient investigative staff with the essential technical knowledge and experience;
- Reviews independently the way fraud investigations have been conducted;
- Imposes appropriate sanctions on fraudsters such as fines or, other penalties, or criminal prosecution in appropriate cases;
- Seeks to recover the amounts lost from fraud;
- Evaluates the effectiveness of sanctions;
- Works with others to tackle fraud.

3.1 To show that organisations are serious about tackling external fraud, they need to detect cases of fraud against them; investigate them where appropriate and impose sanctions which are proportionate to the crime. This will help to deter potential fraudsters in the future by showing that crime does not pay, especially if the outcome of cases are well publicised. Organisations also need to consider whether the frauds detected show new threats are emerging, or are on a larger scale than originally thought. From this work, organisations will need to consider whether their strategic approach needs updating. They will also need to assess whether any frauds reveal systemic weaknesses which need to be tackled (Figure 5).

Figure 5: on the actions to deal with individual cases of fraud



Detecting fraud

3.2 Frauds may be detected in a number of different ways. Referrals may come from staff who have carried out checks on transactions and suspect a fraud. Members of the public may contact the organisation about their suspicions. Organisations also use a range of techniques and technologies to identify suspicious cases for further investigation. They may also carry out special pro-active exercises to detect fraud in high risk areas. Fraud investigators may develop their own intelligence by following leads on existing cases where there may be links to other frauds. This section focuses on the use of hotlines and computer software techniques.

Hotlines

3.3 Hotlines can be a cost effective way of obtaining from staff and the public details of possible cases of external fraud which can be assessed and investigated further. Good practices include:

- Setting up a single freephone telephone number, with alternative means of contacting the department including an email and freepost addresses;
- Advertising the telephone number and contact details on the department's website, in leaflets and posters, advertisements during anti fraud campaigns;
- Giving undertakings on confidentiality; indicating the information that is useful in a referral, including the types of frauds that the department are particularly interested in hearing of and how the department will deal with the information provided.

3.4 It is also good practice to record information received onto a standard form. This can help in prompting the person making the referral into providing as much relevant information as possible. An electronic version of the form can be included on a website, which can be completed and submitted anonymously online. The person may want to know what action may be taken and feedback on what has happened. While it is possible to give general information on how referrals are handled, it may well not be possible to give specific details on individual referrals where this would breach confidentiality requirements.

3.5 Hotlines should be evaluated at regular intervals, for example, analysing the number and type of referrals received, what has happened in each case, and overall results.

The use of computer techniques to detect fraud

3.6 A range of techniques using computer software and technologies can be used to detect cases of fraud. These include techniques such as data matching, data mining and neural networks. Smaller organisations may be able to draw on the experience and lessons of others in the use of these techniques.

3.7 Data matching involves computerised scanning of data held in different data files either within the same organisation or in different organisations. It can be used by management for a range of purposes including detecting potential fraud. With increasing computer power, data matching across files is possible on a very large scale.

3.8 To help focus resources on the matches which indicate possible fraud, data matching software:

- Highlights the highest priority matches;
- Allows users to filter only those matches that meet investigators' criteria for investigation;
- Explains the importance of each match type and protocols for sharing information between matched bodies.

3.9 Data matching between different bodies is facilitated greatly by common data descriptors but is possible only if there is appropriate authority for data to be transferred or shared between these bodies. This authority may derive from a statutory basis for demanding, or disclosing, the data or both. Uncertainty regarding powers to share data may sometimes hinder the use of data matching. Data matching also raises concerns about the possible infringement of individual rights to privacy.

3.10 Data matching exercises should comply with the provisions of any data protection law. Principles of data protection include that data must be:

- Fairly and lawfully processed;
- Processed for limited purposes;
- Adequate, relevant and not excessive;
- Accurate;
- Not kept for longer than is necessary;
- Processed in line with the individual's rights;
- Secure; and
- Not transferred to countries without adequate protection.

3.11 Data mining is the process of selecting, exploring and modelling large amounts of data to reveal previously unknown patterns, behaviours, trends or relationships which may help to identify cases of fraud. Because of the large amount of data that need to be analysed, specialist computer software is used which usually contain a range of data mining tools. A number of software companies have developed such products. Data mining can be a powerful way of interrogating data and revealing anomalies that would not be revealed by other techniques. However, to enable it to function most effectively, staff need to be trained in the use of the software, and to gain experience in selecting the most appropriate tools to scrutinize the data and in following up anomalies to detect cases of fraud.

3.12 Neural networks are computer based multiprocessing systems which are designed to connect data from multiple sources to identify structures and patterns and exceptions to an identified structure or pattern. The ability of neural networks to identify patterns of activity and exceptions to a pattern that may be associated with fraud, gives organisations an ability to focus their detective efforts on these exceptions.

3.13 One of the problems of using these techniques more widely in the public sector is that the data may not be held in a way that lends itself to such analysis. The move towards providing services online may change this and allow real time analysis of transactions through the organisation's websites using some of these techniques.

Investigating cases of fraud

3.14 Where fraud has occurred, the organisation should consider:

- Stopping the fraud at the earliest opportunity and look at whether weak controls have been exploited which need to be tightened up;
- Whether to prosecute the case criminally or impose a penalty;
- Collecting any arrears and any penalties to ensure that the economics of the crime are undermined and to deter others.

3.15 Some organisations have criteria or scoring systems to determine those that should be investigated with a view to prosecution with the remainder subject to other forms of sanction. Organisations also need to look at whether the total number of investigations is commensurate with the potential sums lost from fraud. Investigating cases can be resource intensive. Assessing the financial return achieved on the overall caseload, and different categories of case will indicate the likely benefits of undertaking more investigations or a different mix.

3.16 Tracking the progress of fraud investigations allows managers to assess the overall workload (such as whether investigations are concentrated on the main types of fraud set out in the organisation's strategy); identify problem areas such as where progress is slower than would be expected; understand the cost implications of investigations and the effects on planning future resource usage or the consequences of increasing or decreasing resource levels. Where organisations investigate frauds they will need to consider whether there are sufficient staff with the right technical and investigative knowledge and experience and whether they need to provide a range of training for fraud investigators.

3.17 Investigations into fraud should be consistent with the aims of the criminal justice system to reduce crime and the fear of crime and to dispense justice fairly and efficiently, promoting confidence in the rule of law. Fraud investigations need to be of high quality. Independently reviewing the way in which fraud investigations have been carried out can help to ensure that appropriate standards and legal requirements have been followed. The findings can highlight areas where improvement is needed. The reviews can be undertaken by:

- Independent internal teams, with expertise in fraud investigation, to review the conduct and quality of fraud investigations;
- The appointment of an external assessor.

Imposing sanctions

3.18 Where investigations find evidence of fraud, organisations will usually seek to impose some form of sanction. The purpose is to deter others from carrying out similar types of fraud against the organisation; recover the money defrauded and punish the fraudster by imposing a penalty, such as a fine, or confiscating an asset, or by prosecuting them criminally in the courts. Some organisations have published their approach to deter potential fraudsters and ensure that a consistent approach is taken:

Fines and other penalties

3.19 Fines and other penalties imposed on those committing fraud need to be recovered to ensure that they act as a deterrent. It is important to monitor progress in recovering the fines and penalties involved, including the enforcement of fines imposed by the courts for convicted fraudsters. Organisations need to be aware of any human rights law.

Criminal prosecution

3.20 Preparing cases to the state of proof required for a criminal prosecution can take a long time and involve significant resources. Decisions on whether to prosecute may depend on whether:

- There is sufficient evidence to obtain a conviction;
- The case involves a systematic attack on the department's systems and has led to substantial amounts of money being lost;
- There is a history of re-offending;
- Professionals such as lawyers and accountants are involved in the fraud;
- Prosecution will increase the deterrent effect.

3.21 These factors need to be balanced against the time and cost of bringing a case to court, and the availability of other forms of sanction which may be more appropriate. Some organisations have laid down the circumstances in which they will prosecute to ensure that they take a consistent approach in each case. Organisations will need to consider whether the number of prosecutions is commensurate with the potential sums at stake in lost revenue and provide a sufficient deterrent.

The recovery of money defrauded

3.22 The means of recovering assets may be achieved through the criminal process or through the civil courts. In some circumstances it may be appropriate for an organisation to proceed with a civil action while a criminal prosecution is underway. As part of an investigation, organisations may look into the financial affairs of the suspected fraudster to see whether evidence can be provided to the court on the extent of the benefit obtained by the defendant, and to make a confiscation order. Before the suspected person or persons become aware that an investigation is taking place, action may be needed to secure misappropriated funds by seeking a civil injunction or a criminal restraint order.

3.23 Where an organisation seeks to recover stolen monies through the civil courts it may have to prove on a balance of probabilities, that it has cause of action against the defendant. Further the plaintiff may have to prove the amount taken. If successful the court may then make an order against the defendant requiring him or her to compensate the plaintiff together with an award of costs in most cases. Legal costs can be high. Organisations may need to consider:

- The amounts stolen and therefore could be recoverable;
- The prospects of winning the case;
- The value of assets held by the suspected fraudster;
- The likely legal costs;
- Whether it will be possible to pursue a civil action whilst a criminal investigation is underway.

3.24 Organisations may be able to recover stolen monies as part of criminal proceedings. This normally can be through restraint, confiscation, forfeiture or compensation orders.

Evaluating the effectiveness of sanctions

3.25 Evaluating the effectiveness of sanctions is not straightforward, mainly because of the difficulties in assessing the deterrent effect. In broad terms, the deterrent effect of sanctions will be reflected in whether the amount of fraud has reduced, although it is hard to disentangle the effects of sanctions from other action to reduce fraud as well as wider economic effects. Trends in the indicators can help to determine whether the level of activity may be having a desirable effect.

Working with others in tackling fraud

3.26 Individuals and businesses may be committing frauds against more than one government department or agency. Joint working enables organisations to identify common threats and pool their knowledge and expertise to investigate fraudsters. Other benefits of working together to tackle fraud are:

- Good practice can be shared across organisations;
- Information can be exchanged more efficiently;
- Skills, informal systems and culture are developed across participating organisations;
- A more consistent approach from the different organisations can be developed;
- The consistency of information provided by customers to different organisations can be tested;
- Trust and understanding can be built across organisations.

3.27 Joint working arrangements can be set up by having a Memorandum of Understanding with other organisations to enable sharing of data and carrying out matching and profiling with their data. This may be facilitated through data warehouses accessible to the organisations involved. The data warehouse can include data from each organisation and from external sources, such as the population register which includes data such as national insurance numbers, driving licences, passport holders and electoral rolls. Joint working may also include co-operation on fraud investigations. This enables organisations to identify and investigate cases of common interest, avoiding duplication of effort.