This chapter starts where the last chapter finished, by dealing with the external regulations that affect accounting practice. Some of these are required by legislation and affect areas such as taxation, auditing and the regulation of limited companies. Others are ‘accounting standards’ set both in the UK and internationally by independent accounting standards bodies.

The main part of this chapter explains the internal control systems that are set up in an organisation to implement all the requirements of external regulations and other organisational requirements.

The chapter describes in detail:

- the different types of fraud that can be committed within an organisation
- the risk of fraud occurring within an organisation
- the areas vulnerable to fraud
- the need to design a system so that fraud is minimised, can be easily detected and dealt with as appropriate
EXTERNAL REGULATIONS AFFECTING ACCOUNTING PRACTICE

Legislation
The term ‘legislation’ covers a wide range of regulations based on UK Acts of Parliament and European Directives. Organisations are affected by a number of legal regulations affecting the way in which an accounting system operates. Examples include:

- **taxation regulations** – affecting areas such as:
  - PAYE for individuals on the payroll: income tax, National Insurance and other deductions
  - Value Added Tax: VAT returns, invoice format, rates applied
  - corporation tax paid by limited companies

- **company law** – set out in the Companies Acts – requires that company financial statements (of larger companies) should be audited; these statements are to be drawn up in a set format and sent to shareholders; larger companies also have to send full versions of these statements to Companies House where they can be accessed by the public

- **data protection law** – set out in the Data Protection Act 1998 – protects data (including financial data) relating to individual customers

- **late payment law** – set out in the Late Payment of Commercial Debts Regulations 2013 – allows suppliers to charge interest on late payment of invoices

UK and international accounting standards
The Financial Reporting Council (FRC) is a unified, independent regulator which:

- sets, monitors and enforces accounting and auditing standards
- oversees the regulatory activities of the professional accountancy bodies
- regulates audit
- promotes high standards of internal regulation within companies (‘corporate governance’)

The membership of the Council includes wide and balanced representation at the highest levels from the business, investor, professional and other communities interested in corporate reporting and governance.

The FRC promotes good financial reporting through its Committees and Councils, which include the Accounting Council and the Audit and Assurance Council.
The FRC takes an active role in relation to the internal regulation of companies, ensuring that they comply with company law, accounting standards, and auditing standards.

Accounting standards have been developed over many years and are now the responsibility of the Accounting Council, a part of the FRC, to provide the rules, or framework, of accounting. The intention has been to reduce the variety of alternative accounting treatments. This framework for accounting is represented in the UK by Statements of Standard Accounting Practice (SSAPs) and Financial Reporting Standards (FRSs).

As you will know from your other studies, many companies – European (including UK plcs) and worldwide – now prepare their financial statements in accordance with International Financial Reporting Standards (IFRSs). It is anticipated that international financial reporting standards will eventually replace the UK Standards.

International Standards on Auditing (ISAs) are also gradually being introduced; these will set down guidelines for the way in which UK businesses are audited.

### Report writing hint

When you write about the proposed change to the accounting system of your chosen organisation you will need to provide evidence that it takes account of any change in external factors such as changes in the law (eg company regulation, tax rates) and changes in accounting standards.

### The need for policies and procedures

External regulations – such as legislation – are only of any use if an organisation regulates its employees and keeps them up-to-date by issuing formal internal sets of rules and guidelines. These are often referred to as Policies and Procedures.

**What do Policies and Procedures cover?**

Illustrated on the opposite page is an internal document issued by a large company outlining the introduction of new Policies and Procedures for the retention and disposal of records throughout the business.

‘Records’ can be paper-based or electronic. In this case, the document produced by each function in the business – sales, administration, accounting and finance – will set out:
what records should be retained and at what level of security – ie if they should be locked up or not
- the period of time for which the records should be stored
- what records should be disposed of (ie shredded or wiped from a computer storage medium)

In the case of the **Accounting and Finance** function, this could include:

- retention of financial documents such as invoices, bank statements, payroll records – often for six years
- safe disposal of these records after this period
- immediate safe disposal of confidential details such as credit card details from customers sent in with mailed orders

In this document the need for new Policies and Procedures is made clear:

“The company is obliged under information legislation to have retention/disposal schedules for all its corporate records. Without clear retention/disposal policies the company risks falling foul of the Data Protection Act, Freedom of Information Act, and Public Record Act.”

---

**RECORD RETENTION AND DISPOSAL – NEW POLICIES AND PROCEDURES**

Our Policies and Procedures are the main reference material for people in each Department.

All formal procedures and work systems are outlined in these documents which give managers and staff the rules and guidelines.

The company is obliged under information legislation to have retention/disposal schedules for all its corporate records. Without clear retention/disposal policies the company risks falling foul of the Data Protection Act, Freedom of Information Act, and Public Record Act. Failure to dispose of records in a timely and efficient manner can lead to criticism from the Information Commissioner and Adjudicator.

Currently, information relating to how long we should be keeping records is scattered throughout operational guidance. Quite often this retention/disposal information is out-of-date and/or the reasons behind why particular time periods were chosen have been forgotten.

The people making decisions regarding retention/disposal timescales need to understand the different reasons that may effect their decision.

These new Policies and Procedures:

- lay down the company policy for documenting retention information
- explain why a retention policy is needed
- identify numerous reasons that can effect the retention period decision, and contain a good practice guide on how to construct a retention schedule
INTERNAL CONTROL IN AN ACCOUNTING SYSTEM

Any accounting system will have certain elements in common, whether it is a company Accounts Department, a Local Authority Purchasing Department or a charitable organisation’s fundraising section. It will:

- deal with money – handling cash
- need to make payments and issue cheques
- have ‘levels of authority’ within the system
- need to make decisions over ordering and purchasing
- need to set budgets for spending
- need to organise its accounting records

Unless the management is happy to let everything become totally disorganised, the accounting system will need to establish various rules and regulations which will establish an internal control system, for example:

- the establishing of money limits for certain transactions
- the definition of levels of responsibility for authorising transactions
- the need for referral of decision making to another person when required

Illustrated on the opposite page are extracts from a Policies and Procedures internal control document issued by the Accounts and Finance Department of a medium-sized business. Read through this and you will see that there are a number of examples of the three areas of internal control outlined above. These have been extracted and are shown below.

**money limits**

All orders of £1,000 or more must be authorised by the budget holder.

All cheques for £1,000 or over require two signatories.

Petty cash will be topped up on the 'imprest' system, where the amount spent is reimbursed. It is intended for small items, up to £20.

**authorisation**

All invoices must be authorised for payment by the budget holder.

Salary payments require the signature of the Accounts Manager or Financial Controller, plus one other.

**referral to another person or higher authority**

Budget holders will discuss with the Financial Controller appropriate parameters, plus maximum allowed deviations before the budget holder or senior manager is brought in; this will be documented.

Finance must be informed if there are queries delaying authorisation (of payments) or if payment is to be withheld for any reason.
POLICIES AND PROCEDURES STATEMENT– ACCOUNTING AND FINANCE (extracts)

Books of account and records
Proper accounting records will be kept. The accounts systems is based around computer facilities, using Sage and Excel, but manual/paper records will also be used if appropriate. The following records will be kept:
• Appropriate control accounts (bank control, petty cash control, VAT control, salary control)
• Monthly trial balances
• Petty cash and bank accounts will be reconciled at least monthly
• VAT Returns produced on the required quarterly cycle

Ordering supplies and services
Budget holders can place orders for goods or services within their budget areas, subject only to cash-flow restraints. All orders of £1,000 or more must be authorised by the budget holder, except for specific areas of expenditure where written procedures have been agreed. Under £1,000, the budget holder may delegate all ordering as appropriate. Budget holders will discuss with the Financial Controller appropriate parameters, plus maximum allowed deviations before the budget holder or senior manager is brought in, which will be documented.

Payment authorisation and Purchases Ledger
All invoices must be authorised for payment by the budget holder, although the actual checking of details may be delegated. The authorising department is responsible for checking invoices for accuracy in terms of figures and conformity with the order placed, that the services or goods have been received, and following up any problems. Finance must be informed if there are queries delaying authorisation or if payment is to be withheld for any reason.

A Purchases Ledger is operated by Finance. All incoming invoices are to be passed to Finance section as soon as they arrive. Invoices will be recorded in the Purchases Ledger within two days, unless there are coding problems. They are then passed on to budget holders for authorisation. Once authorised as above, suppliers will be paid within the appropriate timescale.

Cheque writing and signing
Signatories will only be drawn from senior staff and directors, and any new signatory must be approved by the directors before the bank is notified. All cheques for £1,000 or over require two signatories. Cheque signatories should check that the expenditure has been authorised by the appropriate person before signing the cheque. Salary payments require the signature of the Accounts Manager or Financial Controller, plus one other. Cheques should be filled in completely (with payee, amount in words and figures, and date) before cheques are signed.

Handling of cash
Petty cash will be topped up on the ‘imprest’ system, where the amount spent is reimbursed. It is intended for small items, up to £20. Anything over this should be paid by cheque where possible. The imprest has a balance limit of £250. The petty cash balance will be reconciled when restoring the imprest balance, or monthly if this is more frequent. All cash collected from Finance will be signed for, and receipts will be issued for all cash returned.
reviewing the accounting system

Your review of an accounting system, whether it is in the workplace or set out in an AAT Case Study will be covered in full in Chapter 5.

You will need to appreciate that if an accounting system has weaknesses it will be because the internal control system – as seen on the previous two pages – will be deficient in one way or another. This will lead to various possible problems:

- **errors being made** because people do not know the correct way of doing things
- errors being made **and not being picked up** because the processes are not being checked properly
- and lastly . . .
- **fraud being committed** because the internal control system is deficient and the opportunity for fraud is there for the taking

TYPES OF FRAUD

Fraud is an unfortunate fact of life within organisations. It sometimes hits the headlines, as when a merchant banker’s PA diverted over £1 million of her employer’s funds into designer clothes, cars, speedboats, and general high living. This is obviously an extreme example which makes good material for the media, but the principle involved is the same as the employee who walks off with the employer’s stationery or petty cash, or who sneaks out of work an hour early to watch a football match.

Fraud within an organisation can therefore be described as an activity which presents a threat of some form of loss to the employer:

- **loss of money**, eg theft of petty cash
- **loss of inventory**, eg theft of products by supermarket staff
- **loss of time**, eg disappearing from work to do something else during contracted work hours
It is the responsibility of the management of an organisation to:

- identify areas where the **risk of fraud** exists and to grade the seriousness of the risk in each case
- set up **control systems** involving all staff to alert management to possible occurrence of fraud
- **monitor** those control systems on a regular basis to ensure that they are working
- deal with any incidence of fraud in an appropriate way, whether it be a formal warning or calling in the police

These will be dealt with in the course of this chapter. First, however, it is important to define in more detail what we mean by ‘fraud’.

**Some definitions**

Fraud covers a variety of offences, but a general definition of fraud is:

**the use of deception with the intention of obtaining an advantage, avoiding an obligation or causing loss to someone else or to an organisation**

Fraud is a criminal activity and is covered in the UK by a number of laws:

- **theft** dishonestly taking someone else’s property (Theft Act)
- **false accounting** dishonestly destroying, defacing, concealing or falsifying an accounting record for personal gain or to cause loss to someone else (Theft Act)
- **bribery and corruption** taking or giving a bribe that might influence the actions of others (Prevention of Corrupt Practices Acts)
- **deception** obtaining property, money, services or evading liability by deception (Theft Act)

**Practical examples of fraud**

In practical terms fraud is normally a combination of any of the following:

- **theft** of property or money or information (eg someone copying and selling the company’s customer database to a competitor)
- **falsification** of records so that property or money is passed to the wrong person (eg someone ‘fiddling’ the payroll)
- **collusion** – ie a ‘set-up’ between an employee and someone else outside the organisation, eg false invoices sent in by an outsider for supplies that were never made and authorised and paid by the person ‘on the inside’
public examples of fraud

There are many examples of fraud which are made public. Students involved in the public sector would find it useful to investigate the HM Treasury Fraud Reports, available as downloads from the website www.hm-treasury.gov.uk. These contain examples of fraud in local authorities and Government departments. Types of fraud in the private sector are very similar. The examples below have been adapted from cases reported by a leading insurance company.

REPORTED CASES OF FRAUD

Theft of fuel stocks – Total Loss £25,000
A local authority had their own fuel pumps for supplying their motor vehicles. The employee in charge stole fuel over a long period as the inventory checks were inadequate.

Payroll fraud: fictitious employees – Total Loss £10,000
The manager of an industrial cleaning company invented bogus employees, put them on the payroll and then cashed their pay cheques.

Bank deposits: teeming and lading – In 10 months a total of £7,000 was stolen.
A clerk in charge of a sub post office stole cash receipts due to be paid into the local bank. This was covered up by delaying paying in at the bank and altering the paying-in slips relating to subsequent deposits. Stealing money received from one source and then using money received from other sources to cover it up is known as ‘teeming and lading’.

Cheque printing machine – Total Loss £25,000
A ledger clerk responsible for making regular payment of rent for advertising was in charge of a machine that printed cheques. Numerous small cheques were made out by him for the correct amounts but payable to him. It was several months before complaints from creditors, (who had not received their cheques) were investigated and the fraud uncovered.

Collusion: stock control system – Total Loss £1 million
A well known national company was defrauded by two gangs of employees working at the same location. The losses involved collusion between warehousemen and drivers who used the spare capacity on vehicles to remove goods from the depot. False information was entered into the computerised inventory control system and their activities were only discovered when the police reported finding large amounts of the particular product in the hands of third parties.

Collusion: fictitious sub-contractors – Total Loss exceeded £500,000
A major contractor with well established control systems to approve payments were the victims of fraud by a section supervisor in collusion with a computer operator. Cheques were made out to fictitious sub-contractors and despatched to private addresses.
risk assessment – the role of management

Assessment of fraud risk is part of the risk assessment process which is the responsibility of organisations in both the private and the public sectors.

In the case of limited companies (private sector), the Turnbull Report has stated that directors have responsibility for ensuring that risk management practices are established as part of an effective internal control system.

In the public sector the guiding document to fraud risk is HM Treasury’s ‘Managing the Risk of Fraud – a Guide for Managers’ available as a download from www.hm-treasury.gov.uk

The assessment of risk generally by management follows a number of distinct stages. This process applies equally to the assessment of fraud risk:

- setting up a risk management group and identifying objectives
- identifying the areas of risk of fraud
- grading the scale of the risk in each case
- developing a strategy to manage that risk
- setting up systems to detect and deal with fraud, allocating responsibility
- getting the systems up and running
- monitoring the running of the system

the internal control system

A robust internal control system is essential if management is going to be able to detect and deal with fraud.

There are various techniques that can be used for making an internal control system ‘fraud resistant’:

Report writing hint

When you write about your analysis of the current accounting system of your chosen organisation you will need to provide evidence that you have investigated potential areas of fraud. You will need to be aware of the various types of fraud that can be committed.
■ fraud staff

Some very large organisations may appoint employees – eg ex-bank or ex-police staff – to work full-time on fraud prevention and detection.

■ management responsibility

Managers should be given specific areas of responsibility and answerability – eg sections of the Accounts Department – to ensure that fraud is kept to a minimum.

■ management supervision

Management – particularly line management – should supervise accounting activities on a regular basis. This involves overseeing and checking activities such as data entry to computers, making payments and payroll processing.

■ segregation of duties

The system should be set up so that duties which, when combined, could lead to fraud, are given to different people – ie they are segregated. For example, the cashier taking in cash for a business should ideally not be the same person who makes out the paying-in slip for the bank. The danger is that some of the cash may disappear into the cashier’s pocket.

■ lock & key

Physical security – locking valuable items away – is a sure deterrent to theft. This does not only apply to cash: the tendency of items such as laptop computers and mobile phones to disappear has become a well-known and ever-increasing statistic.

■ authorisation

Some accounting activities may require authorisation by a nominated official. This ranges from the authorisation of petty cash, signing of cheques over a certain amount to the investing of liquid funds, eg placing £250,000 on a money market account. Clearly the larger the amount, the more senior the person giving authorisation.

detecting fraud

We have already seen the various areas in which fraud can occur. Fraud can be detected by the experienced manager by simple observation and through experience. Some of the tell-tale and danger signs include:

■ employees acting suspiciously – looking shifty and hiding paperwork

■ employees with higher levels of spending than you would expect from their income – the payroll clerk who has a new Porsche
employees working long hours and taking less than the normal holiday entitlement – it is often when employees are away that other employees notice suspicious signs and uncover criminal activity

employees who have a grudge against the organisation – they may have been passed over for promotion or they may even have a political or ethical axe to grind

employees who are known to be short of money – they may be struggling with a high mortgage or may even have a drugs problem

g *grading likelihood and impact*  

Part of the process of the management of fraud risk is the decision about whether a risk is a **likely** one or not. The likelihood of risk can be divided into three levels:

- **high** – the likelihood of fraud is at a high level (disappearing biros)
- **moderate** – the likelihood is possible (theft of cash, collusion)
- **low** – the likelihood is remote (removal of assets from a company pension fund)

The risk of fraud occurring can also be given a **numerical value**: for example a range of 1 to 5, where the higher the risk the higher the number.

Risk assessment also needs to decide whether the **impact** of the fraud is significant. Impact can relate to the **financial state** of the organisation. A major loss through fraud could seriously affect profit and liquidity. For example, the fraudulent trading by an employee of Barings Bank led to its collapse. The fraud can also seriously affect employees, as in the Robert Maxwell case in which employees’ pensions were appropriated by the Chairman and Chief Executive.

Generally speaking, frauds that are likely (the disappearing biro) have a lower impact than the remote risk (removal of assets from a company pension fund). The **impact** of a fraud can therefore be similarly graded:

- **high** – the effects of fraud are very serious for the organisation, affecting its profit and/or liquidity
- **moderate** – the effects of the fraud are significant but can be dealt with internally, or in some cases by the police (theft, collusion)
- **low** – the impact of the fraud is insignificant (petty pilfering)

**using a matrix to grade fraud risk**

Organisations sometimes use a matrix to assess the extent of fraud risk in an accounting system. The areas of the system in which the fraud might occur must first be identified, for example:
- cash payments
- cash receipts
- sales ledger
- purchases ledger
- expenses
- inventory control
- payroll
- fixed asset purchase

A matrix (or a section of a matrix) will then be drawn up for each of the areas identified. An example of entries in a typical matrix is illustrated below. The matrix might display:

- the identified risk area of the organisation
- the details of the type of fraud
- the role of the employee who may become involved in it
- any third party who may become involved through collusion
- the likelihood of the fraud (high, moderate, low)
- the impact of the fraud (high, moderate, low)

This matrix will then become a valuable tool which will enable management to assess the risks and establish an appropriate strategy for minimising them. Note that the format of the matrices you will encounter in your studies may vary. The example below is fairly typical and could be used in your Report.

### Accounting System Fraud Matrix – Some Sample Entries

<table>
<thead>
<tr>
<th>Details of Risk</th>
<th>Employees</th>
<th>Collusion</th>
<th>Likelihood</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Payroll section:</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stationery pilferage</td>
<td>payroll staff</td>
<td>none</td>
<td>high</td>
<td>low</td>
</tr>
<tr>
<td>Theft of cash</td>
<td>payroll staff</td>
<td>none</td>
<td>moderate</td>
<td>moderate</td>
</tr>
<tr>
<td>Payments to fictitious employees</td>
<td>payroll staff</td>
<td>third party recipients</td>
<td>moderate</td>
<td>moderate</td>
</tr>
<tr>
<td><strong>Purchase ledger:</strong></td>
<td>buyer</td>
<td>third party recipients</td>
<td>moderate</td>
<td>moderate</td>
</tr>
<tr>
<td>Paying fictitious suppliers</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>etc... etc...</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Fraud detection is an important function in any internal control system. We have already seen earlier in this chapter some of the warning signs of fraud which managers should look out for as a matter of course. It is useful, however, for an organisation to set up a Fraud Policy which might include:

- a clear indication of which managers are responsible for which potential areas of fraud and at what levels
- setting up of control systems to help avoid fraud, eg strict checking, segregation of tasks and division of responsibilities, eg in the purchasing process the person who sets up a purchase order should not be the same as the person who approves it or the person who writes out cheques should not be the same person who signs it (unless maybe it is for a very small amount)
- the regular monitoring of the control systems to ensure that they are working satisfactorily and are amended from time-to-time as circumstances require
- decisions about which type of frauds are significant (eg moderate and high risk) and should be acted upon and those which should be generally guarded against but which are low risk and do not require strict disciplinary action (eg the ‘borrowed’ biro)
- the need for an anti-fraud ‘culture’, ie instilling in employees the notion that any form of fraud (including the ‘borrowed’ biro) is inherently wrong and alerting them to the risks that exist
- following on from the last point, the mechanism should exist for ‘whistle-blowing’, ie for employees to alert the management if they become aware of any fraudulent goings-on at any level of the organisation; the employee in this case is given protection by the Public Interest Disclosure Act 1998

**FRAUD POLICY**

It is recommended that you should not only research into potential areas of fraud, but you should also identify each type of fraud and grade its risk (using a high/medium/low or a numerical system) and its impact, using some form of matrix — such as the one on the previous page.

Remember, however, that you will need to be diplomatic with the organisation that you are dealing with, as fraud is a very sensitive issue.
**action taken to deal with fraud**

As part of its Fraud Policy, an organisation should set up a system which ensures that the correct action is taken when:

- fraud is discovered by someone within the organisation
- fraud is reported by someone outside the organisation – the police, for example

Areas which should be dealt with are:

- provision of clear directions to managers about whom to contact when a fraud is discovered
- in a large organisation the appointment of a senior manager with special responsibility for fraud who can take responsibility for any major occurrences
- directions for disciplinary procedures for occurrences of fraud which will not have to involve the police and possible prosecution
- directions for how to deal with a case of fraud which will involve the notification of the police and may result in a criminal prosecution
- directions for how to deal with a case of fraud which is reported to the organisation by the police (eg the discovery of stolen inventory or a bank reporting suspicious money transactions) – and which may result in a criminal prosecution

As you will have gathered from this chapter, fraud is inevitable. The lesson for the organisation is – be prepared.

---

**Report writing hint**

Your Report should include a note of any formal Fraud Policy, and if this does not exist, details of managerial control systems and any arrangements made for these systems to be monitored. Evidence of the introduction of any anti-fraud culture could also be included.

---

**some useful websites**


In order to access information about fraud you are likely to have to carry out a website search on ‘fraud’.

This chapter concludes with two Case Studies on fraud and analysis of fraud published by HM Treasury. They should provide you with an understanding of how a weakness in the accounting system can make fraud possible.
Travel and subsistence fraud

Case description

This fraud involved an employee who travelled regularly on official business. He set his own programme of visits which was not checked by his line manager. He then regularly submitted fraudulent travel and subsistence claims which included examples of:

- Claiming subsistence allowances in excess of entitlement;
- Claiming for overnight stays in hotels when in fact he had stayed with friends or family;
- Claiming for visits not made;
- Forging authorising signatures;
- Inflating claims by altering details on claim forms after authorisation by countersigning officer.

These claims were paid by the finance team despite the lack of receipts, invoices or other supporting documents to verify his expenditure. Travel and subsistence guidance was also out of date and consequently had fallen into disuse.

The fraud came to light when his office tried to contact him at a hotel where he claimed to be staying. An investigation uncovered a large number of fraudulent claims spanning several years and the officer was eventually prosecuted.

Control weaknesses

- Inadequate guidance on submitting, authorising and paying claims;
- Inadequate supervision by line management;
- Failure of countersigning officer to verify that journeys had been made;
- Inadequate control exercised by countersigning officer in returning signed claim forms to the claimant rather than passing them directly to the finance team;
- Inadequate checks by finance teams to query amendments to claims, verify countersignatures and ensure that receipts and invoices were included to substantiate claims;
- Absence of spot checks on claims by the finance team management.
Cash handling fraud

Case description

Transactions involving receipts of cash or cheques are high risk. Of the cases of staff fraud reported to the Treasury each year, a significant proportion involves misappropriation of cash. In this sample case, a member of staff committed a number of frauds over a period of five years, resulting in a loss of over £10,000.

The organisation’s business included the receipt of cheques through the post and cash and cheques over the counter. It was the responsibility of the member of staff to receive, record and prepare the receipts for banking. She had been in the job several years and her line managers, who trusted her implicitly, had given her sole responsibility for these duties. They were no longer carrying out checks or monitoring the process.

She would arrive early each morning, usually before her colleagues, and open the post on her own. Money handed in over the counters was also passed to her for banking. However, she did not record or account for the cheques or money prior to banking. She would, however, complete a daily cash balance record as part of the banking reconciliation procedures, but by this time she had already removed some of the cash and a number of cheques. There were no independent cross-checks between the documentation which came with the receipts and the amounts sent for banking. To make matters worse written procedures were out of date and had fallen into disuse.

The fraud came to light during the officer’s infrequent absences on leave. A minor query by a member of the public regarding a previous payment led to an unexplained difference between the amount quoted in the documentation accompanying the payment and the amount recorded by the officer and banked.

Internal audit were brought in to carry out an initial investigation. They identified major discrepancies between records of receipts kept by counter staff, documentation accompanying payments from members of the public and the amounts being banked. The police were called in and under questioning the officer admitted the offences. She had opened a bank account with the initials of the organisation and had been paying in cash and cheques over a five year period. The case was taken to court and on conviction she was given a custodial sentence and had to repay the amounts stolen.
Control weaknesses

- Lack of separation of duties between post opening, preparation of cash and cheques for banking and reconciliation of amounts banked
- Inadequate supervision and monitoring by line management
- Absence of management checks of accounting records, cash balances or bank reconciliations
- Over-reliance on the honesty and integrity of one individual
- Lack of adequate written instructions
- Unawareness of implications of reluctance to use leave entitlement

The internal audit report also identified organisational factors which had contributed to the fraud. The main ones were:

- The organisation had not assessed the risk of fraud;
- There was no policy statement on fraud;
- Line managers were not clear about their responsibilities;
- Manuals and procedures were poorly structured and out of date.