JANUARY 2016

QUALIFIED INTERNAL AUDITOR

COURSE BOOK

IQN International Qualifications Network

www.iqnglobal.com

CONTENTS

Chapter 01: Internal Auditing, Risk and Governance

1. Internal Auditing

Internal audit is generally a feature of large companies. It is a function, provided either by employees of the entity or sourced from an external organisation to assist management in achieving corporate objectives.

Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

The codes of corporate governance that indicate good practice for companies, such as the UK Corporate Governance Code (formerly the 'Combined Code'; mandatory for UK listed companies) highlight the need for businesses to maintain good systems of internal control to manage the risks the company faces. Internal audit can play a key role in assessing and monitoring internal control policies and procedures. The internal audit function can assist the board in other ways as well:

1. Internal Audit should provide an appraisal of an organisation's internal control system and take the action needed to provide Accountable Officers with a continuing assurance that the organisation's risk management, control and governance arrangements are adequate and effective.
2. Internal audit evaluates compliance with an organisation's internal control system including relevant regulations, guidance and procedures- as part of its review process. However, the primary responsibility for monitoring compliance rests with operational areas and their line management, up to and including the relevant Accountable Officer.
3. By liaising with external auditors, particularly where external auditors can use internal audit work and reduce the time and therefore cost of the external audit. In addition, internal auditors can check that external auditors are reporting back to the board everything they are required to under auditing standards.

The activities of the internal audit function usually involve:

- Monitoring internal controls
- Examining financial and operating information (for example, reviewing the accounting system and carrying out tests of detail on transactions and balances in the same way as the external auditor does)
- Review of the economy, efficiency and effectiveness of operations (this would include looking at non-financial controls of the organisation)
- Review of compliance with laws, regulations and other external requirements
- Special investigations, for instance, into suspected fraud
- Identifying and evaluating significant exposures to risk and contributing to the improvement of risk management and control systems
- Assessing the governance process in its accomplishment of objectives on ethics and values, performance management and accountability, communicating risk and control information to appropriate areas of the organisation and effectiveness of communication among those charged with governance, external and internal auditors, and management

2. The Relationship between Internal and External Audit

External auditors seek to obtain sufficient evidence to support an opinion on overall fairness of the financial statements and accounting. Their perspective is therefore mainly backwards, what happened last year. The internal audit on the other hand is mainly interested in the situation now and in the future. External auditors also need to evaluate the system of internal control. Mainly external auditors are interested in internal controls only as far as they concern the financial statements and accounting. Also the main difference between internal and external auditors is their line of reporting and responsibility. Internal audit works for the top management of the organisation whereas external auditors work for the stakeholders and to some extent to the authorities. The main objective of internal audit is to evaluate established and implemented financial systems, i.e. procedures, which are used in preparation, accounting and presenting reliable information on financial transactions. That is why it is possible to acknowledge, that the main objective of an external auditor is to confirm that the final result (the sum) is correct, whilst the main objective of an internal auditor is to confirm that procedures, used as a basis to reach the end result, are correct. The majority of external audit objectives coincide with internal audit

objectives and goals; quite often even adequate or identical procedures and methods for identifying audit environment, selection of evidence, audit are used.

3. Code of Ethics and Principles of Professional Conduct

The Code of Ethics is a statement of principles and expectations governing the behaviour of internal auditors. It is part of the mandatory guidance for internal auditors, and non-compliance can result in the auditor being subject to disciplinary action.

The purpose of the Code of Ethics is to promote an ethical culture in the global profession of internal auditing. Internal auditing is a profession built very much on trust and so a Code of Ethics is vital to ensure that trust is not broken.

The Code of Ethics applies to both individuals and entities that provide internal auditing services. This includes:

- Institute members
- Recipients of or candidates for any internal auditing professional certifications
- Those who provide internal auditing services within the definition of internal auditing

IQN has issued its own standards for internal auditors known as *International Standards for Qualified Internal Auditor (ISQIA*). All QIA graduate must conform to ISQIA.

UK auditors are also subject to Ethical Standards the Auditing Practices Board (APB). The APB is the Auditing Practices Board in the UK, which also issues auditing standards (adopted from IFAC).

The IFAC Code contains a number of fundamental principles. The fundamental principles are:

- **Integrity.** A professional accountant should be straightforward and honest in all professional and business relationships.
- **Objectivity.** A professional accountant should not allow bias, conflict of interest or undue influence of others to override professional or business judgements.
- **Professional competence and due care.** A professional accountant has a continuing duty to maintain professional knowledge and skill at the level required to ensure that a client or employer receives competent professional service based on current developments in practice, legislation and techniques. A professional accountant should act diligently and in accordance with applicable technical and professional standards when providing professional services.

- **Confidentiality.** A professional accountant should respect the confidentiality of information acquired as a result of professional and business relationships and should not disclose any such information to third parties without proper and specific authority unless there is a legal or professional right or duty to disclose. Confidential information acquired as a result of professional and business relationships should not be used for the personal advantage of the professional accountant or third parties.
- **Professional behaviour.** A professional accountant should comply with relevant laws and regulations and should avoid any action that discredits the profession.

4. Threats to Auditor Independence and Safeguards

Occasionally, an internal auditor may find themselves in a situation which may potentially put them in a position of conflict with the Code of Ethics. This can arise when an auditor is put in a situation where they have competing professional or personal interests. The auditor's independence can be influenced by a number of threats including those set out below:

i. self-review threats that occur when an auditor provides assurance on his or her own work;

ii. self-interest threats that occur, for example, when an auditor could benefit from a financial interest in a client or when there is an undue dependence on an assurance client;

iii. advocacy threats that occur when an auditor promotes a client's position or opinion;

iv. familiarity threats which occur when an auditor becomes too sympathetic to a client's interests; and

v. intimidation threats which occur when an auditor is deterred from acting objectively by actual or perceived threats from a client.

Types of Safeguards

Safeguards that may be considered to mitigate threats to independence include:

i. safeguards created by the accounting profession, legislation or regulation, such as external practice inspection.

ii. safeguards within the Authority, such as the Audit Committee.

iii. safeguards within the auditor's own systems and procedures, such as quality control procedures or the removal of an individual from an engagement.

Non-Audit Services

Non-audit services undertaken by the auditor create actual and/or perceived self-review, self-interest or advocacy threats to the independence of the auditor. The degree of the threat depends on the nature, scale and scope of the non-audit service.

Good reasons for the auditor to be appointed to perform non-audit services include where:

i. it is economic in terms of skill and effort for the auditor to provide such services as a result of his intimate and specialised knowledge of the business.

ii. the information required is a by-product of the audit process or

iii. required by legislation or regulation.

5. International Standards for Qualified Internal Auditor (ISQIA)

Internal audit activities are performed in diverse legal and cultural environments; within organisations that vary in purpose, size, complexity, and structure; and by persons within or outside the organisation. While differences may affect the practice of internal auditing in each environment, compliance with the International Standards for Qualified Internal Auditor (ISQIA) is essential if the responsibilities of internal auditors are to be met. If internal auditors are prohibited by laws or regulations from complying with certain parts of the Standards, they should comply with all other parts of the Standards and make appropriate disclosures. The Standards are developed by the International Qualifications Network (IQN).

The purpose of the Standards (as stated in ISQIA 1100) is to:

- To outline the scope and functional requirements of internal auditing activities
- To interpret the terms and definitions used in the statement of standards

6. Other professional, legal and regulatory standards

Internal auditors must be aware of, and be able to apply, other laws and regulations in addition to those set out by the IASB.

Internal auditors come into contact with a variety of other legal and professional standards in their working lives.

Much of this legislation relates to fraud, corruption and money laundering. The specific legislation you will come into contact with will depend on where in the world you are based and the kind of organisation in which you work.

Legal and professional standards that you may come across during your career in internal auditing include:

- International Financial Reporting Standards (IFRS)
- Sarbanes-Oxley Act 2002
- Foreign Corrupt Practices Act 1977
- Racketeer Influenced and Corrupt Practices Act 1970
- 'Integrated Framework' published by COSO (Committee of Sponsoring Organisations) as well as CoCo and Cadbury (Canadian and British counterparts of COSO)
- US Government 'Yellow Book' for government audits
- UK Money laundering regulations

7. What is Corporate Governance?

Corporate governance is the system by which organisations are directed and controlled. Corporate governance is a set of relationships between a company's directors, its shareholders and other stakeholders. It also provides the structure through which the objectives of the company are set, and the means of achieving those objectives and monitoring performance, are determined. Although mostly discussed in relation to large quoted companies, governance is an issue for all corporate bodies, commercial and not for profit, including public sector and non-governmental organisations.

ISQA 6000 Risk and Governance

The internal audit activity must review existing practices of governance procedures and be able to recommend ways of improvement. Organisational governance procedures aims in establishment of appropriate promulgation of organisation specific ethical stances and the extent of values placed in. Effective governance procedures should also ensure reliability in performance measurement, accountability, risks identifications and timely flows of information between senior management, boards, internal auditor and external auditor.

There are a number of elements in corporate governance:

The management, awareness, evaluation and mitigation of risk is fundamental in all definitions of good governance. This includes the operation of an adequate and appropriate system of control.

The notion that overall performance is enhanced by good supervision and management within set best practice guidelines underpins most definitions. Good governance provides a framework for an organisation to pursue its strategy in an ethical and effective way and offers safeguards against misuse of resources, human, financial, physical or intellectual.

Good governance is not just about externally established codes, it also requires a willingness to apply the spirit as well as the letter of the law.

Good corporate governance can attract new investment into companies, particularly in developing nations.

8. Agency Theory

Agency theory suggests that the firm can be viewed as a nexus of contracts between resource holders. An agency relationship arises whenever one or more individuals, called principals, hire one or more other individuals, called agents, to perform some service and then delegate decision-making authority to the agents.

The primary agency relationships in business are those (1) between stockholders and managers and (2) between debt holders and stockholders. These relationships are not necessarily harmonious; indeed, agency theory is concerned with so-called agency conflicts, or conflicts of interest between agents and principals. This has implications for, among other things, corporate governance and business ethics. When agency relation builds up it also tends to give rise to agency costs, which are expenses incurred in order to sustain an effective agency relationship (e.g., offering management performance bonuses to encourage managers to act in the shareholders' interests).

Conflicts between Managers and Shareholders

Agency theory suggests that, in imperfect labour and capital markets, managers will seek to maximise their own utility at the expense of corporate shareholders. Agents have the ability to operate in their own self-interest rather than in the best interests of the firm because of asymmetric information (e.g., managers know better than shareholders whether they are capable

of meeting the shareholders' objectives) and uncertainty (e.g., myriad factors contribute to final outcomes, and it may not be evident whether the agent directly caused a given outcome, positive or negative).

A potential agency conflict arises whenever the manager of a firm owns less than 100 percent of the firm's common stock. If a firm is a sole proprietorship managed by the owner, the owner-manager will undertake actions to maximise his or her own welfare. The owner-manager will probably measure utility by personal wealth, but may trade off other considerations, such as leisure and perquisites, against personal wealth.

If the owner-manager forgoes a portion of his or her ownership by selling some of the firm's stock to outside investors, a potential conflict of interest, called an agency conflict, arises. For example, the owner-manager may prefer a more leisurely lifestyle and not work as vigorously to maximise shareholder wealth, because less of the wealth will now accrue to the owner-manager. In addition, the owner-manager may decide to consume more perquisites, because some of the cost of the consumption of benefits will now be borne by the outside shareholders.

Stockholders versus Creditors: A Second Agency Conflict

In addition to the agency conflict between stockholders and managers, there is a second class of agency conflicts—those between creditors and stockholders. Creditors have the primary claim on part of the firm's earnings in the form of interest and principal payments on the debt as well as a claim on the firm's assets in the event of bankruptcy. The stockholders, however, maintain control of the operating decisions (through the firm's managers) that affect the firm's cash flows and their corresponding risks. Creditors lend capital to the firm at rates that are based on the riskiness of the firm's existing assets and on the firm's existing capital structure of debt and equity financing, as well as on expectations concerning changes in the riskiness of these two variables.

The shareholders, acting through management, have an incentive to induce the firm to take on new projects that have a greater risk than was anticipated by the firm's creditors. The increased risk will raise the required rate of return on the firm's debt, which in turn will cause the value of the outstanding bonds to fall. If the risky capital investment project is successful, all of the benefits will go to the firm's stockholders, because the bondholders' returns are fixed at the original low-risk rate. If the project fails, however, the bondholders are forced to share in the losses. On the other hand, shareholders may be reluctant to finance beneficial investment projects. Shareholders of firms undergoing financial distress are unwilling to raise additional funds to finance positive

net present value projects because these actions will benefit bondholders more than shareholders by providing additional security for the creditors' claims.

9. The board of directors

The nature of a board committee

A board committee is a committee set up by the board, and consisting of selected directors, which is given responsibility for monitoring a particular aspect of the company's affairs for which the board has reserved the power of decision-making.

A committee is not given decision-making powers. Its role is to monitor an aspect of the company's affairs, and: report back to the board, and make recommendations to the board.

The full board of directors should make a decision based on the committee's recommendations. When the full board rejects a recommendation from a committee, it should be a very good reason for doing so. A board committee will meet with sufficient frequency to enable it to carry out its responsibilities. It is important to remember, however, that a board committee is not a substitute for executive management and a board committee does not have executive powers. A committee might monitor activities of executive managers, but it does not take over the job of running the company from the management.

The main board committees

Within a system of corporate governance, a company might have at least three or possibly four major committees.

These are:

- a remuneration committee, whose responsibility is to consider and negotiate the remuneration of executive directors and senior managers.
- an audit committee, whose responsibility is to monitor financial reporting and auditing within the company.
- a nominations committee, whose responsibility is to identify and recommend individuals for appointment to the board of directors.
- a risk management committee, where the responsibility for the review of risk management has not been delegated to the audit committee.

The reasons for having board committees

There are two main reasons for having board committees.

The board can use a committee to delegate time-consuming and detailed work to some of the board members. Committees can help the board to use its resources and the time of its members more efficiently.

The board can delegate to a committee aspects of its work where there is an actual or a possible conflict of interests between executive directors (management) and the interests of the company and its shareholders. However, to avoid a conflict of interests, board committees should consist wholly or largely of independent directors. This means independent non-executive directors.

A remuneration committee of independent non-executive directors negotiates and recommends remuneration packages for executive directors or senior managers. The committee members do not have a personal interest in the remuneration structure for senior executives, because they are not remunerated in the same way as executives. They receive a fixed annual fee.

An audit committee of independent non-executive directors can monitor financial reporting and auditing, to satisfy themselves that these are carried out to a satisfactory standard, and that executive management are not 'hiding' information or presenting a misleading picture of the company's financial affairs. The work of the audit committee therefore provides a check on the work of executive managers, such as the finance director. The committee can also monitor the effectiveness of the auditors, to satisfy themselves that the auditors carry out their work to a suitable standard.

Similarly, the work of a risk committee of the board should be to satisfy itself that executive management have a suitable system of risk management and internal control in place, and that these systems function effectively. This is another check on executive management.

A nominations committee makes recommendations about new appointments to the board. The views of executive directors are important in this aspect of the board's work, particularly when a vacancy for a new executive director occurs. However, independent non-executives should have some influence in the nominations process, to make sure that new appointments to the board will not be selected 'yes men' and supporters of the CEO or chairman.

10. Different Approaches to Corporate Governance

Rules-based approach to corporate governance

A rules-based approach to corporate governance is based on the view that companies must be required by law (or by some other form of compulsory regulation) to comply with established principles of good corporate governance.

The rules might apply only to some types of company, such as major stock market companies. However, for the companies to which they apply, the rules must be obeyed and few (if any) exceptions to the rules are allowed.

There are some advantages with a rules-based approach:

- Companies do not have the choice of ignoring the rules.
- All companies are required to meet the same minimum standards of corporate governance.
- Investor confidence in the stock market might be improved if all the stock market companies are required to comply with recognised corporate governance rules.

There are disadvantages with a rules-based approach.

- The same rules might not be suitable for every company, because the circumstances of each company are different. A system of corporate governance is too rigid if the same rules are applied to all companies.
- There are some aspects of corporate governance that cannot be regulated easily, such as negotiating the remuneration of directors, deciding the most suitable range of skills and experience for the board of directors, and assessing the performance of the board and its directors.

Principles-based approach to corporate governance

A principles-based approach to corporate governance is an alternative to a rules based approach. It is based on the view that a single set of rules is inappropriate for every company. Circumstances and situations differ between companies. The circumstances of the same company can change over time.

This means that:

- the most suitable corporate governance practices can differ between companies, and the best corporate governance practices for a company might change over time, as its circumstances change. It is therefore argued that a corporate governance code should be applied to all major companies, but this code should consist of principles, not rules.

- The principles should be applied by all companies.
- Guidelines or provisions should be issued with the code, to suggest how the principles should be applied in practice.
- As a general rule, companies should be expected to comply with the guidelines or provisions. However, the way in which the principles are applied in practice might differ for some companies, at least for some of the time. Companies should be allowed to ignore the guidelines if this is appropriate for their situation and circumstances.
- When a company does not comply with the guidelines or provisions of a code, it should report this fact to the shareholders, and explain its reasons for noncompliance.

Which is more effective: a rules-based approach or a principles-based approach?

The advantages and disadvantages of a principles-based approach to corporate governance are the opposite of those for a rules-based approach. There is no conclusive evidence to suggest that one approach is better than the other. It has been suggested that the burden of the detailed rules in the US, especially the requirements of section 404, has made the US an unattractive country for foreign companies to trade their shares. As a result, many foreign companies have chosen to list their shares in countries outside the US, such as the UK (London Stock Exchange). However, the relative success or failure of New York and London as centres for listing shares by foreign companies is not the only relevant argument about which method of corporate governance is better.

11. Managing Risk

ISQIA 6000 Risk and governance

Internal audit activity must consider evaluating the organisational risk management policies and procedures in order to recommend suitable improvement.

Sufficient information relating to risk exposures should be obtained and analysed through number of internal audit engagements within the organisation. The analytical output should provide an overall understanding of the organisations risk management procedures.

What Is Risk?

We need go no further than the work of Peter L. Bernstein to get an insight into the quality of risk:

> The word 'risk' derives from the early Italian *risicare*, which means 'to dare'. In this sense, risk is choice rather than a fate. The actions we dare to take, which depend on how free we are to make choices, are what the story of risk is all about. And that story helps define what it means to be a human being.

This immediately introduces the concept of choice when it comes to risk – not simply being subject to risks as a part of life, but being in charge of one's destiny as there is much that we can control if we have the time and inclination to do so. The stewardship concept underpinning corporate governance forces management to seek out risks to the business and address them, where appropriate. Peter L. Bernstein goes on to suggest: 'The capacity to manage risk, and with it the appetite to take risk and make forward-looking choices, are the key elements of energy that drives the economic systems forward.

HM Treasury defines risk as 'the uncertainty of outcome within a range of exposures arising from a combination of the impact and probability of potential events'. Risk is measured in terms of consequences and likelihood.'

There are risks out there and they impact on our existence. Many of these risks arise in totally unexpected ways and can have a major effect on the key aspects of our lives. Most people have a vague awareness of the risks that exist in the wide world. Many associate risk with known benefits and perhaps view this as the price of these benefits.

The Risk Challenge

Risk represents a series of challenges that need to be met. Also, the key feature of this challenge is that it appears when a major decision has to be made. Risk has no real form unless we relate it to our own direction, which is what we are trying to achieve. It is the risks to achieving objectives that affect us, in that they detract from the focus on success and stop us getting to the intended result

Good systems of risk management keep the business objectives firmly in mind when thinking about risk. Poor systems hide the objectives outside the model or as something that is considered peripheral to the task of assessing the impact of the risks.

Most organisations create a vision but they cannot create one based on a 20/20 understanding of the future as this is impossible. Better to create the vision in steps, as the future changes one adapts and flexes and so capitalise on opportunities as they arise and respond to threats. Mission statements then communicate the vision of itself and its future. In the perfect world of plans, a blueprint can be laid out, with timetables and responsibilities. In the messy world of bets, circumstances shift unexpectedly and odds change – not an environment in which inviolable plans and rigid schedules will necessarily be helpful.

The other concept that needs to be considered is that risk, in the context of achieving objectives, has both an upside and a downside. We call these threats and opportunities. That is, it can relate to forces that have a negative impact on objectives, in that they pose a threat. Upside risk, on the other hand, represents opportunities that are attainable but may be missed or ignored, and so mean we do not exceed expectations. This is why risk management is not really about building bunkers around the team to protect them from the outside world. It is more about moving outside the familiar areas and knowing when and where to take risks. This is quite important in that if we view controls as means of reducing risk, we can now also view them as obstacles to grasping opportunities. So risk management is partly about getting in improved controls where needed and getting rid of excessive controls where they slow proceedings down too much. In other words, making sure controls are focused, worth it and make sense.

The original King report also acknowledges the two sides of risk by suggesting: 'risk should not only be viewed from a negative perspective. The review process may identify areas of opportunity, such as where effective risk management can be turned to competitive advantage.' The next point to address is the basic two dimensions of measuring risk. That is, as well as defining the impact of the risk, we also need to think about the extent to which the risk is likely to materialise.

Having established the two aspects of risk, we can start to think about which risks are not only material, in that they result not only in big hits against us, but also whether they are just around the corner or kept at bay. Since risk is based on uncertainty, it is also based on perceptions of this uncertainty and whether we have enough information on hand. Where the uncertainty is caused by a lack of information, then the question turns to whether it is worth securing more information or examining the reliability of the existing information. Uncertainty based on a lack of information that is in fact readily available points to failings in the person most responsible for dealing with the uncertainty. There is much that we can control, if we have time to think about it and the capacity to digest the consequences.

Risk Management and Residual Risk

Risk management is a dynamic process for taking all reasonable steps to find out and deal with risks that impact on our objectives. It is the response to risk and decisions made in respect of available choices (in conjunction with available resources) that is important.

Risk management is mainly dependent on establishing the risk owner, or the person most responsible for taking action in response to a defined risk, or type of risk, or risk that affects a particular process or project. The Turnbull report on corporate governance for listed companies contains the following provisions regarding risk management:

> The reports from management to the board should, in relation to the areas covered by them, provide a balanced assessment of the significant risks and the effectiveness of the system of internal control in managing those risks. Any significant control failings or weaknesses identified should be discussed in the reports, including the impact that they have had, could have had, or may have, on the company and the actions being taken to rectify them. It is essential that there be openness of communication by management with the board on matters relating to risk and control.

When reviewing reports during the year, the board should:

- consider what are the significant risks and assess how they have been identified, evaluated and managed;
- assess the effectiveness of the related system of internal control in managing the significant risks, having regard, in particular, to any significant failings or weaknesses in internal control that have been reported;
- consider whether necessary actions are being taken promptly to remedy any significant failings or weaknesses; and
- consider whether the findings indicate a need for more extensive monitoring of the system of internal control.

The stages of risk management are commonly known as:

i. ***Identification:*** The risk-management process starts with a method for identifying all risks that face an organisation. This should involve all parties who have expertise, responsibility and influence over the area affected by the risks in question. All imaginable risks should be identified and recorded. In 1999, Deloitte and Touche carried out a survey

of significant risks in the private sector with each risk scored from 1 (low level of concern) to 9 (high level of concern) with the following summary results:

	Score
Failure to manage major projects	7.05
Failure of strategy	6.67
Failure to innovate	6.32
Poor reputation/brand management	6.30
Lack of employee motivation/poor performance	6.00

Business risk is really about these types of issues, and not just the more well-known disasters, acts of God or risks to personal safety.

ii. ***Assessment:*** The next stage is to assess the significance of the risks that have been identified. This should revolve around the two-dimensional impact, likelihood considerations that we have already described. Management Armed with the knowledge of what risks are significant and which are less so, the process requires the development of strategies for managing high-impact, high-likelihood risks. This ensures that all key risks are tackled and that resources are channelled into areas of most concern, which have been identified through a structured methodology.

iii. ***Management:*** Armed with the knowledge of what risks are significant and which are less so, the process requires the development of strategies for managing high-impact, high-likelihood risks. This ensures that all key risks are tackled and that resources are channelled into areas of most concern, which have been identified through a structured methodology.

iv. ***Review:*** The entire risk-management process and outputs should be reviewed and revisited on a continual basis. This should involve updating the risk-management strategy and reviewing the validity of the process that is being applied across the organisation.

The above cycle is simple and logical and means clear decisions can be made on the types of controls that should be in place and how risk may be kept to an acceptable level, notwithstanding the uncertainty inherent in the nature of external and internal risks to the organisation. In practice, the application of this basic cycle does cause many difficulties. Most arise because we impose a

logical formula on an organisation of people, structures and systems that can be complicated, unpredictable, vaguely defined and perceived, emotive and in a state of constant change. Most risk-management systems fail because the process is implemented by going through the above stages with no regard to the reality of organisational life. Managers tick the box that states the stages have been gone through and eventually the board receives reports back that state risk management has been done in all parts of the organisation.

Mitigation through Controls

Risk management is an important part of the risk cycle, as it allows an organisation to establish and review their internal controls, and report back to the shareholders that these controls are sound. The internal control framework consists of all those arrangements, and specific control routines and processes that drive an organisation towards achieving objectives.

The way controls fit in with risk management is explained in the British standard on risk management:

Those managing risk should prioritise changes to controls, taking into account the impact on other activities and the availability of resources. The control changes selected should be allocated to risk response owners and a schedule for their implementation should be prepared. Progress towards implementation of control changes should be monitored. The controls implemented should be documented.

Monitoring performance of controls

After control changes have been implemented and it becomes possible to gather data on the actual residual risk, the level of residual risk should be assessed. The same decision process should be used to decide whether to retain the residual risk or whether pursuing further control changes is worthwhile. The process should be repeated until the level of residual risk is within the risk appetite and pursuing further control changes does not seem worthwhile. The organisation should monitor and test its controls to ensure:

- They have a named owner;
- They are defined, communicated and understood;
- Their implementation did not introduce any unacceptable additional risks;
- They are operating as designed, each is worthwhile, and collectively they managed the risk to an acceptable agreed level;

- They remain cost-effective; and
- That where deficiencies in the implementation or operation of controls are identified:
- The implications of control deficiencies not being remedied are established and options for resolution are identified;
- They are reported so that the consequence for the risk profile can be assessed; and
- The resolution of control deficiencies is planned and carried out.

5Ts and 5Cs model provides a wide range of techniques for developing a suitable risk-management strategy. 10 measures (5Ts and 5Cs model) for addressing risks that have been assessed for impact and likelihood are described in the following:

1. Terminate

Where the risk is great and either cannot be contained at all or the costs of such containment are prohibitive, we would have to consider whether the operation should continue. Sending sales reps to overseas countries may be common practice for enterprises that have a global growth strategy. Where certain locations are politically volatile, then we may have to take precautions in the way they conduct business in these countries and the type of security arrangements for high-risk sites. Where the costs of adequate security measures are not only sky high but also cannot give reasonable assurance that the sales people would not be attacked, kidnapped or simply caught up in dangerous situations, then we must decide whether to continue sending people to the country (or dangerous parts of the country) that is we may need to consider terminating the activity.

2. Controls

One of the principal weapons for tackling risks is better controls. Building on our example of overseas sales staff, after having assessed certain locations as high personal risk, we would go on to consider what measures we currently have in place and decide whether we are doing enough. Controls may cover local surveys, security personnel, formal guidance on socialising, say in the evenings, procedures for travelling and the use of drivers or guides, awareness seminars on ways of reducing the chances of becoming a target, good personal communications setup and so on. The degree of measures adopted may depend on the assessment of risk levels and changes in states of alert. The key question would be: Are we doing enough, bearing in mind what we know about this location?

3. Transfer

Where the risks are assessed as high impact but low likelihood, we may wish to adopt a strategy of spreading risk, wherever possible. High-likelihood risk will be hard to transfer because all parties involved will want to be fully recompensed to the value of the impact of the risk. It is only where there is some uncertainty that transfers are more appropriate. Turning again to the running example, we may spread the impact of the risk by having an insurance policy that covers overseas staff. Or we may employ an international firm or a local agency to perform the sales role in high-risk countries.

4. Contingencies

A useful response to risk that is again high impact, low likelihood is based around making contingency arrangements in the event the risk materialises. The contingencies would focus on impacts that affect the continued running of the business, so that even after having installed preventive controls, there is still the chance that the risk may materialise. The overseas sales team may be covered by an evacuation procedure in the event that the risk of civil unrest materialises. This may involve access to a special charter plane that can be made available very quickly. The contingency plan may also cover business continuity for the sales lines that may be disrupted by the unrest. Many laypeople view risk management as essentially to do with contingency planning. That is, their rather narrow view of risk does not attach to the achievement of strategic business objectives and the need for processes to handle all material risks.

5. Take more

One dimension of the risk-management strategy is derived from the upside risk viewpoint. Where the impact, likelihood rating shows operations located down at low/low for both factors, this does not necessarily mean all is well. Risk management is about knowing where to spend precious time and knowing where to spend precious resources. Low/low areas are ripe for further investment (for commercial concerns) or ripe for further innovative development (for public sector services). In the overseas sales example, we may wish to send out teams to countries that had a reputation for instability, but are slowly settling down and are open for business.

6. Communicate

One aspect of risk management that is often missed relates to high impact and either medium or high likelihood, where controls may not address the risk to an acceptable level, that is a strategy to communicate this risk to stakeholders and make them aware that this impairs the

organisation's ability to be sure of success (at all times). Communicating risk is a completely separate discipline and sensitive stock markets and high-profile public services have a difficult task in managing expectations, handling price-sensitive information and keeping politicians and the media happy. Some argue that the financial misstatement scandals in 2002 were fuelled by markets that demanded rapid and linear profit growth and resented bad news. Success in communicating risk is mainly based on a trust relationship between the giver and the receiver and the degree of consistency in the messages given. For our overseas sales people, we may simply publish the national statistic on trouble spots and rates of infectious diseases, and tell people about the known risks before they accept assignments. This is particularly helpful where there is little scope to establish robust controls in the area in question, where matters may be outside of our control.

7. Tolerate

The low/low risks that come out of our assessment will pose no threat and as such can be tolerated. This stance may also relate to high-rated risks where we really have no option but to accept what is in front of us. At times where we install more controls over an area to increase the level of comfort, people adjust other controls so they fall back to what they see a comfortable position. Extra checking installed in one part of a system can lead to a slackening of checks in another as people make this adjustment.

8. Commission research

We have argued that risk revolves around uncertainty as to the future. Gamblers are well versed in this and believe that they can beat the odds or simply enjoy placing bets because of non-financial reasons. Many risk-management systems are too rigid, in that they depend on quick assessments and a risk register that shows the agreed strategy for action. More developed systems will allow some thinking time, where one decision may be to go and find out more about the risk, its impact and whether it will probably materialise – that is to commission further research. For the overseas sales team, we may ask an international consultant to travel to a possible 'hot spot' and report back on the local conditions and risks therein. Or we may ask the experts since the Foreign and Commonwealth Office (FCO) in its published *Risk Management Framework 2002* states that the FCOs aim is to promote internationally the interests of the United Kingdom and to contribute to a strong world community, and the FCO also has a specific responsibility to help identify and manage risks to British citizens abroad.

9. Tell someone

Some high/high risks create a blockage, in that they can only really be resolved by parties outside of those participating in the risk-management exercise. Many such exercises grind to a halt as the responsibility for managing the risk in question does not reside with the people who are designing the risk strategy. A better response is to set out the unguarded risk and work out a strategy for relaying this position to the party who can tackle it and also refer the result up through the line. At times, if outside parties do not realise that their inaction has stopped progress in another area, they have no reason to address the problem. Using our sales team example, we may argue that the sales drive is affected by unreliable communications between head office and an assessment of business risk may make this a key barrier to successfully getting orders placed and turned around. The management strategy may suggest that there is nothing that can be done as communications networks are run by the country in question. A better response is to relay this information to the board and note that there is a danger of missing strategic growth objectives if it is left unattended. The board may be able to lobby the government in question or support bids to international development agencies for projects that improve global communications. While these moves may not lead to improvements straight away, it may over time facilitate progress.

10. Check compliance

The final weapon in the arsenal of risk responses is often overlooked. This is to focus on areas where controls are crucial to mitigating significant risks, and to ensure that they are actually working as intended. Controls that counter more than one material risk are particularly important. These controls may be reviewed and tested by internal auditors or a specialist compliance team at the behest of management. We can make a final visit to our sales team, for example, a key control over the team may be a regional co-ordinator who ensures smooth transport between countries and keeps everyone in touch with product developments.

12. The Internal Audit Role in Risk Management

The internal auditing standards (ISQIA6000) state that internal auditors must have regard to key risks and that:

ISQIA 6000 Risk and governance

In order to assess efficacy of the risk management process, internal audit activity should ascertain:

- Whether organisation's strategic objectives and mission are adjuvant
- Whether material risks elements are sufficiently identified and evaluated
- Whether safeguards against risks are identified that are suitable to organisation's risk appetite
- Whether relevant risk information are identified and communicated in timely manner to the personnel associated with it. This would aid in carrying out appropriate responsibilities to minimise risks.

It is clear that the rapid drive towards risk management arose partly because of prescribing codes, partly fuelled by scandals across sectors and organisations and also because successful businesses understood and addressed their key risks. This movement towards embracing risk should in no way be hindered by the internal auditor.

The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.

Determining whether risk management processes are effective is a judgment resulting from the internal auditor's assessment that:

- organisational objectives support and align with the organisation's mission;
- Significant risks are identified and assessed;
- Appropriate risk responses are selected that align risks with the organisation's risk appetite; and
- Relevant risk information is captured and communicated in a timely manner across the organisation, enabling staff, management, and the board to carry out their responsibilities.

Risk management processes are monitored through on-going management activities, separate evaluations, or both.

The internal audit activity must evaluate risk exposures relating to the organisation's governance, operations, and information systems regarding the:

- Reliability and integrity of financial and operational information.
- Effectiveness and efficiency of operations.
- Safeguarding of assets; and
- Compliance with laws, regulations, and contracts.

Internal auditors' involvement in assessing risk or identifying controls including:

- Facilitators enabling and guiding managers and staff through the process
- Team members who are a part of broader based groups
- Risk and control analyst providing manager with expert advice
- Proving tools and techniques used by internal audit to analyse risks and controls
- Becoming a centre of expertise for managing risk

The need to balance independence and the assurance and consulting roles of internal audit is a growing feature of the new look internal auditor. The value adds equation means we cannot ignore the need to help as well as review. Some argue that internal audit needs to reposition itself at the heart of the risk dimension and drive through the required changes.

Audit should determine the effectiveness of management's self-assessment processes through observation, direct tests of control and monitoring procedures, testing the adequacy of information used in monitoring activities and other appropriate techniques. Gregg R. Maynard has provided a succinct lists of ways that internal audit can respond to the risk agenda:

1. Combining objective and subjective analysis of the audit universe to reveal audit priorities. Moving away from the audit cycle – quantitative measures then qualitative ones that change as circumstances change.
2. Analysing management's ability to achieve its stated goals and objectives in pre-audit narratives. Management's assessment of risk and tolerances.
3. Using questionnaires to examine internal controls from the top down. Explore the tone at the top – ethical standards, strategic planning, management information and risk management.
4. Analysing the processes for establishing and overseeing risk limits. Threshold and set limits and financial and operational targets.

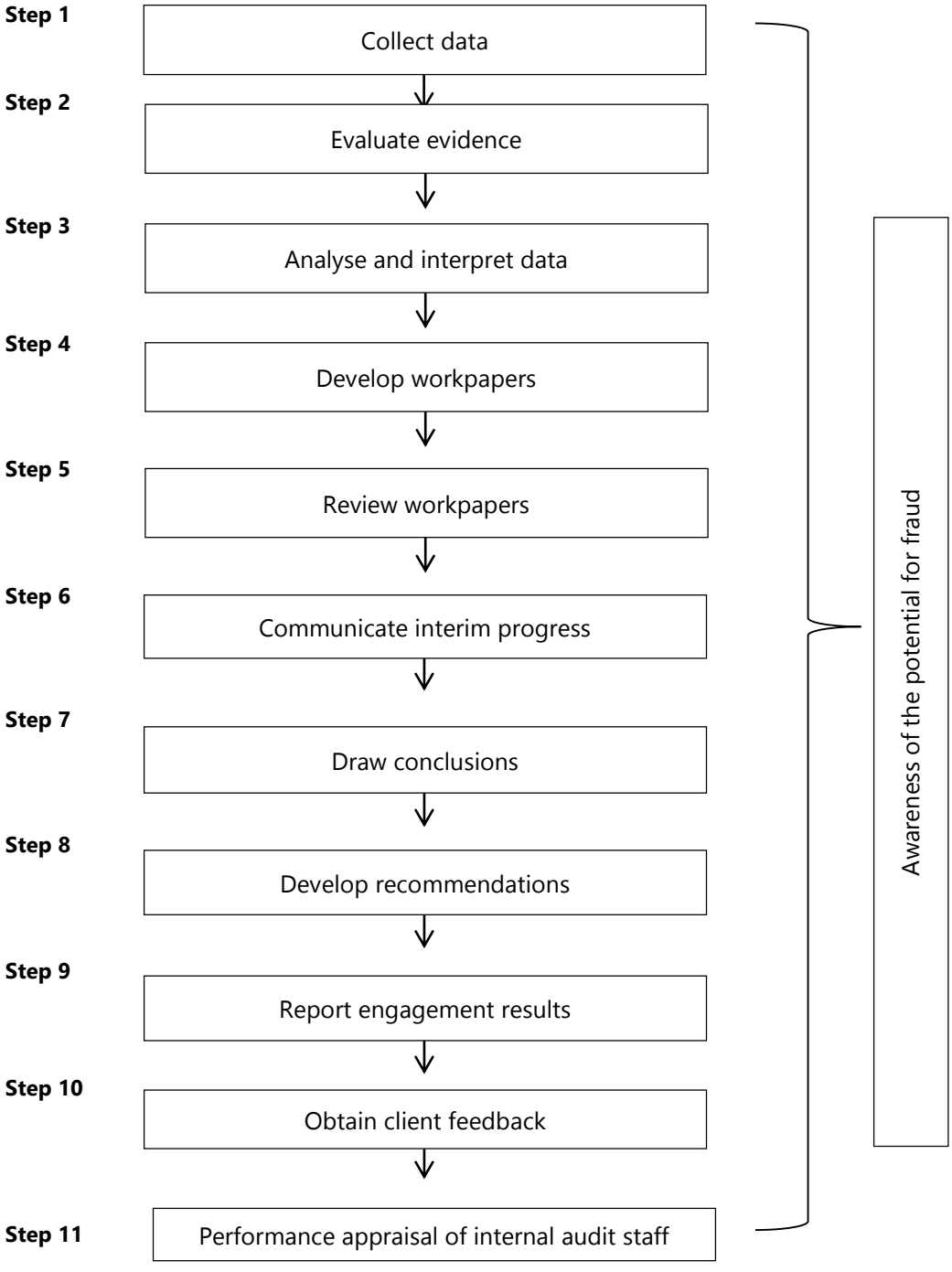
5. Reviewing other risk management functions, such as treasury, compliance, and accounting control. Base reliance on assessment and also get the big picture on risk exposures.
6. Observing the strategic planning process and its results. Look to audit the future and changing risks but not in a decision making capacity.
7. Evaluating strategic initiatives. E.g. strategic alliances and new projects.
8. Integrating audit activities. E.g. IT audit and front line audit.
9. Basing the audit process on the net effect of risk exposures and compensating controls. Audit recommendations should be based on this equation – risks less controls. Then determine the extent of substantive testing needed to confirm the position.
10. Partnering with management by providing consulting services and value added information.
11. Reviewing ethics as a basic element of internal control.
12. Conducting a comprehensive audit of the entire risk management programme.

Chapter 02: Conducting Internal Audit Engagements

1. The audit engagement process

Relevant internal auditing standards for conducting internal audit engagements has been outlined in ISQIA 3000 Planning Engagement, 4000 Performing Activities and 5000 Gathering and analysing data.

The audit engagement process is shown in the diagram below.



The rest of this chapter will take you through each of these eleven steps in greater detail. The diagram illustrates the necessity for the internal auditor to maintain awareness for the potential for fraud through the entire audit process.

2. Collecting Data

During the internal audit process, internal auditors need to collect data in order to determine facts. These facts will form the bases of the auditor's conclusions and recommendations; therefore it is important that the auditor obtains the right facts.

To determine the right facts, auditors will need to be skilled in the collection of useful data. The information you collect is vital to the success of your internal audit engagement as you will use this data and information as the basis for your observations. You will draw conclusions based on this data, and these conclusions will lead you to make recommendations for improvement.

If the recommendations are not based on sound data, you will struggle to get senior management's agreement as your findings may be meaningless.

2.1 Audit evidence

Audit evidence is the facts that the auditor uses to support the audit opinions, conclusions and recommendations.

Audit evidence can take a number of forms: physical, documentary, representational or analytical.

2.1.1 Physical evidence

Physical evidence includes the documentation of observations, pictures such as photographs or maps, and video such as CCTV footage.

This kind of evidence is generally considered to be more reliable than a person's testimony.

2.1.2 Documentary evidence

Most audit evidence will fall into this category. Examples include accounting records, letters, invoices, expense claim forms, emails, HR records, etc..

It is important to remember that documents can be forged and the auditor should remain vigilant for anything suspicious when reviewing documentation.

2.1.3 Representations

Representations are basically people's opinions, for example responses to questionnaires, interviews and inquiries would all be considered to be representational evidence.

To improve the reliability of this kind of evidence, it should be backed up with supporting documentation such as documented policies or procedures, systems notes or flowcharts.

2.1.4 Analytical evidence

This includes all analysis carried out by the auditor, as well as any other computations or comparisons.

2.1.5 Source of evidence

Not all audit evidence will come from the same source; it can be either internal or external.

Internal evidence is evidence provided by the audit customer

External evidence is evidence received from a third party source

The source of the evidence will affect how much reliance can be placed on it. In general, corroborative evidence that has been provided by an independent third party (such as information provided directly by the bank that manages the organisation's account) is considered to be more reliable than audit evidence from the organisation being audited.

2.2 Legal evidence

Auditors should have an understanding of the main types of legal evidence as, although they won't have to gather evidence to use in court, they may be required to gather data for a lawyer.

2.2.1 Best (or Primary) evidence

Best evidence is usually documentary and will consist of original writing where it is available.

2.2.2 Secondary evidence

This kind of evidence is less reliable than best evidence and could be items such as a copy of a document, or oral testimonies. Document copies are considered to be more reliable than oral testimony or written summaries.

2.2.3 Direct evidence

Direct evidence supports the truth of an assertion directly, i.e., without need for any intervening inference.

2.2.4 Conclusive evidence

Conclusive evidence points to only one conclusion.

2.2.5 Circumstantial evidence

This kind of evidence proves a fact indirectly. It will prove a secondary fact from which the person using the evidence is likely to conclude that the primary fact exists.

2.2.6 Corroborative evidence

Corroborative evidence supplements and supports other evidence.

2.2.7 Opinions

Opinions are only useful evidence if they are provided by an expert. For example, in court a doctor's professional opinion may be suitable evidence, whereas the opinion of a non-expert on the same matter would not.

Auditors should only gather data that relies on an opinion when:

- They have no knowledge of the subject themselves
- The opinion provided is that of an unbiased expert

2.2.8 Hearsay

Hearsay is basically second hand testimony, for example 'Stephen said he saw her take it'. This kind of evidence is less reliable than first hand evidence, however it should not be ignored. The auditor should use the information to determine if any first hand evidence does exist.

2.3 Obtaining audit evidence

There are a number of factors the auditor should bear in mind when obtaining audit evidence.

2.3.1 Timing

When will the evidence be available for testing? This is particularly important for electronic data. This is because electronic data, for example spread sheets, are regularly updated. If the organisation doesn't back up the different versions prior to making the amendment, those old versions will be lost.

When using such data as part of your audit, it is important to liaise with the owner of the information to ensure an appropriate version 'as at the date you are interested in' is saved and backed up for you. This means the client can continue to update their version without corrupting your file to include changes outside the review period.

2.3.2 Confidentiality

Internal auditors are required by the Code of Ethics to protect the confidentiality of audited documents.

Again, this is most difficult with electronic data. When extracting data from electronic sources, such as databases, the auditor must take care to avoid accidentally corrupting or distributing the data.

2.3.3 Access to data

Auditors need to be able to gain access to the data.

The auditor may be challenged when requesting data as to why they need access to the data and may be expected to give a reason as to why this data is relevant to the engagement. Whether or not this is given will depend upon the individual circumstances of the situation concerned. The decision as to whether or not to provide a reason will be made by the head of internal auditors.

In many situations, where a cooperative engagement is being carried out, there may be no problem in giving a reason; however, internal auditors are under no obligation to do so.

Internal auditors have a right of access to all information that may be relevant to their activities.

3. Evaluating evidence

Internal auditing standard defines the qualities that audit information should possess. According to the Standard internal auditors must identify sufficient, reliable, relevant, and useful information to achieve the engagement's objectives.

These qualities of information are also important as the information will be the basis for the audit findings and the recommendations that are ultimately made.

The Standard also provides guidance as to the meaning of these terms.

Sufficient. Factual, accurate and convincing so that a prudent, informed person would reach the same conclusion as the auditor

Competent. Reliable and the best attainable through the use of appropriate engagement techniques

Relevant. Supports engagement observations and recommendations and is consistent with the objectives for the engagement

Useful. Helps the organisation meet its goals

3.1 Gathering audit evidence

Audit evidence should be collected on all matters that relate to the engagement objectives and scope of work.

Audit evidence can be gathered in many ways, including inquiry, inspection, observation, monitoring and re-performance. The most common technique used is inquiry. Auditors should choose the most appropriate method for the specific situation.

3.1.1 Analytical procedures

Analytical procedures are used by internal auditors to identify and examine information. It involves comparing information and identifying any relationships or trends it may contain. This helps the auditor to identify anomalies which can then be further looked into. Such anomalies could identify errors, unusual transactions, inefficiencies, changes, or fraud.

Auditors should not draw conclusions, however, purely based on analytical procedures. Further work should always be carried out to find out the reason for the anomaly. A large one-off transaction doesn't have to be due to fraud or error; it may simply be a legitimate large one-off transaction!

Analytical procedures can be carried out both on financial information (e.g. listing of payments to suppliers) and non-financial information (e.g. report of sick days taken by each employee in a specific area of the organisation).

4. Analysing and interpreting data

Once the data and evidence has been collected, it must then be analysed in order to transform it from a collection of notes, figures, reports and documents into meaningful information upon which to draw sensible conclusions.

A number of analytical techniques can be applied by internal auditors in order to help them make sense of the information.

Internal auditors must analyse the information they have obtained in order to make sense of it. However, simply analysing the information is not very much use on its own. In order to have any meaning they should be looked at in context by providing comparative data. This may be as simple as comparing the information obtained against what the auditor would expect to see.

There are many difference bases on which comparisons can be made, and different comparisons are better suited to different data. For example, information could be compared against:

- Prior periods
- Budgets or forecasts
- Industry averages
- Linked non-financial information (e.g. comparison of changes in payroll costs to the changes in the average number of employees)
- Different elements of the information (e.g. changes in interest costs could be compared to the changes in the related debt balances)

There may be any number of equally valid comparisons that you can think of. The important thing is to make sure you put your analysis into context by carrying out relevant comparisons.

Comparisons can also be carried out using a number of measures. For example, valid comparisons could be made using monetary amounts, physical quantities, ratios and percentages. Again, the best measure to use is the one that best fits the test you are carrying out and what you are attempting to achieve.

4.1 Analytical techniques

A very brief overview of the more common analytical techniques is provided below to indicate what tools you might be using at this stage of the audit engagement process.

Ratio analysis	Ratios provide a means of systematically analysing financial statements. They provide a common measure which can then be compared with the past, with other departments, other companies in the industry or the industry itself. They can be grouped under the headings profitability, liquidity, leverage (also known as debt, or gearing) and activity.
Trend analysis	Looks at relationships, or trends, over time.
Regression analysis	Regression analysis is a quantitative technique to check any underlying correlations between two variables (e.g. sales of ice cream and the weather).

Period to period comparisons	Looks at changes from quarter to quarter or year to year. Any big discrepancies will need to be investigated.
Comparisons with budgets, forecasts, and economic information	Budgets and forecasts are management's predictions of the future. They show what they expect to happen. Comparing actual results to these expectations show how well the company is doing at meeting its targets. Reasons for any large variances will need to be obtained.
Comparisons with independent factors	Comparing information to external benchmarks, such as best practice, industry averages or regulations.

Different techniques will be more appropriate in different situations. When deciding which is most appropriate, internal auditors may consider the following:

- The significance of the area under review, for example a high level review of expenditure relating to the construction of a new facility is likely to require a different approach to a check on petty cash usage in one or two departments.
- The sufficiency of risk assessments and risk management in the area under review.
- The availability and reliability of information (both financial and non-financial).
- How well the auditor can predict what the results of the analytical procedures will be.
- The extent to which the findings can be backed up by the results of other tests.
- The extent, reliability and comparability of industry data.

The analysing and interpreting data stage will continue until the auditor is satisfied that a sufficient explanation has been received for all discrepancies. If this is not possible, the auditor must communicate this to the appropriate levels of management and, where necessary, make appropriate recommendations for improvement.

5. Developing workpapers

Workpapers document your audit. They are where you store your evidence, meeting notes, documentation, data analyses and interpretations. They show the processes that you went through and will eventually form the basis for your conclusions, recommendations and report.

Workpapers are highly confidential.

Auditors are required by Standard to document the engagement in workpapers.

5.1 Purpose of workpapers

The purpose of workpapers is to record relevant information to support conclusions and engagement results. It is your file of evidence and you may need to draw on it to defend your decisions if your findings or recommendations are challenged.

However, working papers have a number of purposes. Generally, audit working papers

- Aid in the planning, performance, and review of engagements
- Document whether the engagement objectives were achieved
- Support the accuracy and completeness of the work performed
- Provide a basis for evaluating the internal audit activity's quality assurance and improvement programme
- Facilitate third party reviews.

The applications of workpapers include:

Report writing	Writing the report is much easier if workpapers are carefully written and organised. If each workpaper contains a valid conclusion and has determined the root cause and effect of the problem, the information can be almost transferred directly into the report.
Communication tool	The workpapers can provide evidence for external auditors, and can also provide the basis and background information for future internal audits. Future reviews are much easier when there is a strong set of existing workpapers documenting the area.
Quality self-assessment	The workpapers are a good basis for quality self-assessments and performance reviews of the internal auditor that carried out the work. This can illustrate compliance with the Standards.
Defence	When delivering the final report, the auditor can rely on the workpapers to defend the conclusions and recommendations. Annotating the auditor's copy of the report with the working paper references will make this easier.
Compliance	The workpapers can assist in documenting the organisation's compliance with laws and regulations.

Workpapers should be compiled carefully with each of these purposes in mind so that where necessary the relevant roles can be provided.

5.2 Documenting the engagement

Internal audits have to be documented. The documentation makes up the audit file (which may be either physical or electronic) that contains your evidence and documents exactly what you have done. This will prove that you have done everything you should have and back up your findings and recommendations by identifying the processes that led to these conclusions being drawn.

The following aspects of the engagement should be documented.

- Planning
- Risk assessment
- Examination and evaluation of the adequacy and effectiveness of the system of internal control
- The engagement procedures performed, the information obtained, and the conclusions reached
- Reviews
- Communication
- Follow-up

Consulting engagements also have to be documented in working papers. All work carried out in order to achieve the objectives, and support the results of, a formal consulting engagement should be documented.

5.3 Content of workpapers

Workpapers contain everything you did during the audit. They include all your meeting notes, results of audit tests, process notes, organisation charts, and other audit evidence. It is a record of how you reached the conclusions that led you to the recommendations and opinions expressed in the report.

A good set of workpapers could be picked up by another auditor who had no involvement in the work and by reading through could follow the processes the auditor went through and arrive at the same conclusions.

Among other things, engagement working papers may include:

- Planning documents and engagement programmes
- Control questionnaires, flowcharts, checklists, and narratives
- Notes and memoranda resulting from interviews
- Organisational data, such as organisational charts and job descriptions
- Copies of important contracts and agreements
- Information about operating and financial policies
- Results of control evaluations
- Letters of confirmation and representation
- Analysis and tests of transactions, processes and account balances
- Results of analytical auditing procedures
- The engagement's final communications and management's responses
- Engagement correspondence if it documents engagement conclusions reached

5.4 Policies

The head of internal auditors is responsible for developing policies for the working papers for the different types of engagements performed. This might include setting standard formats for specific working papers and standardized audit programme formats, or the categorising of certain working papers as 'permanent' i.e. can be carried forward for use in future audits.

5.5 Style and order

Good working papers will be well structured and easy to follow. Here are some characteristics they should possess

Complete	The workpapers should leave no question unanswered. This will include following up previous findings and answering review points
Understandable	Everything should be clearly explained, including pictures and documents etc. and should be easy to follow
Tidy	The files should be neat, clearly written and well organised
Relevant	If it is not specifically relevant to the audit engagement, it should be omitted from the file. A clear purpose statement or objective helps auditors to decide what is and is not relevant.

Uniform	Papers should be the same size (attach smaller papers to regular sized papers)
Logical	The workpapers should be in sensible order and arranged in segments that match up with the segments of the audit
Economical	Duplication should be avoided. Use working papers from previous audits where possible (if they are relevant and the findings are unchanged). Don't do more work than is necessary in order to establish a fact. Once you are certain of it, move on.
Simple language	Avoid jargon and technical language and explain things clearly and simply. You should write for someone who knows nothing of the subject being audited so that any auditor could pick up your file and understand your workpapers.

5.6 Format of workpapers

The specific way your working papers will be formatted will depend upon your personal preferences and any standard formatting in place at the organisation for which you work.

However, there are a few requirements for working paper format that should always be adhered to.

Every engagement working paper should:

- Identify the engagement
- Describe the purpose or content of the paper
- Be signed/initialled and dated by the auditor performing the work
- Be given a specific reference number
- Contain an explanation of any verification symbols (tick marks) used. These should be kept uniform throughout the audit
- Clearly identify the sources of any data used

It can be helpful to include working paper summaries in your workpapers. This will help you to focus on the reason for including data in the workpapers, and will provide you with a conclusion to each audit segment by making you consider the findings in relation to the scope and objective of the audit.

Working papers are not necessarily paper documents; they could easily be a series of electronic files. If electronic working papers are used they should be access controlled using passwords and should be set to 'read only' for all except the authoring auditor.

5.7 Control of workpapers

Audit workpapers should be carefully controlled; responsibility for their control lies with the head of internal auditors.

There are two reasons why this is such an important issue

1) The workpapers are likely to contain confidential or personal information.
2) Workpapers are crucial to the success of the engagement. They hold the evidence that supports the recommendations and conclusions and if lost can delay or and cause duplication of work. In severe cases it can halt the engagement entirely and the lost evidence may be irreplaceable.

Work papers should be held securely and kept confidential at all times. Access to these documents should be carefully controlled.

Head of Internal Auditor (HIA) must approve any requests for access to workpapers made by any members of the organisation (outside the internal audit activity) or by the external auditors.

Any requests for access to the workpapers by personnel external to the organisation is also subject to approval from senior management, the legal counsel or both. The HIA is responsible for obtaining this approval.

At the end of the audit engagement, the HIA should develop policies for the retention of workpapers and all other engagement records.

The HIA should also develop policies for the control and retention of records from consulting engagements. For example, ownership of consulting engagement records must be established to prevent misunderstandings and protect the organisation.

6. Reviewing workpapers

The HIA should ensure audit engagements are properly supervised. This includes reviewing and approving workpapers both to ensure the work is of a sufficient high quality standard, and to evaluate the current skills and training needs of the internal auditor.

Supervision should take place at all stages of an audit, from the initial planning stages right through to follow-up. It will involve many different aspects, including ensuring the auditors are competent, that the working papers support the findings, and that the overall objectives of the engagement are met.

6.1 Evidencing the review

Supervising an audit includes reviewing the workpapers. This review should be evidenced to prove when, and by whom, the review was carried out. The reviewer of the workpapers should initial and date each workpaper after reviewing it to provide evidence of their review. The review could also be evidenced in a number of other ways, including:

- Completing a workpaper review checklist, which would then remain on file with the rest of the workpapers
- Preparing a memorandum detailing the review carried out, how it was done, what was covered, and the results of that review. Again this would remain on file.
- Evaluation and acceptance using electronic working paper software.

The reviewer may prepare a list of review notes for the auditor to consider. The auditor should then evidence that these points have been resolved, perhaps by writing their response and signing off each review point as it is actioned. Care must be taken to ensure adequate evidence to demonstrate that the points have been resolved is provided.

7. Communicating interim progress

Problems identified shouldn't wait until the end of the audit. They should be discussed with management in interim progress reports to make sure the client is fully aware of any potential problems, can begin to think about (or even implement) measures to remedy the problems and can clear up any misunderstandings with the auditor.

Interim progress reports should occur during the process of the audit engagement to inform the client of the progress and findings so far.

There is no set format for an interim report, and it doesn't even have to be in writing. The approach taken will depend on the specific situation, the relationship with the client and what is to be communicated. It could be an informal chat or a detailed, written formal report or anything in between.

If management are aware of the issues so far, then they can begin to think about possible solutions that could be put in place. In some cases this may mean that by the time the engagement ends they have already corrected the problem and established the necessary controls or procedures. In such cases, these findings may not even need to be raised in the final report.

This is in the interest of both the auditor and the client. It reduces the auditor's work as there will be fewer issues to agree with management and less recommendations to follow up. It also beneficial to management as they will create a better impression with senior management as less negative points will be raised in the final report. Their cooperation may also be noted by senior management.

As well as being helpful for keeping management up to date, interim reports can also be used to inform clients of any changes to the scope of the audit, or to highlight any findings that require immediate action or attention.

Regardless of whether or not interim reports are used, a final report will still have to be issued at the end of the process. A series of interim reports cannot be used to avoid this obligation.

7.1 Fraud

Fraud should be immediately communicated to senior management and the board as soon as its existence becomes apparent to the internal audit activity. The head of internal auditors is responsible for doing this.

Immediately means as soon as an investigation has established with reasonable certainty that the fraud has occurred.

The HIA's report should state whether or not a full fraud investigation is recommended, along with a summary of the observations and recommendations that have led to this decision.

8. Drawing conclusions

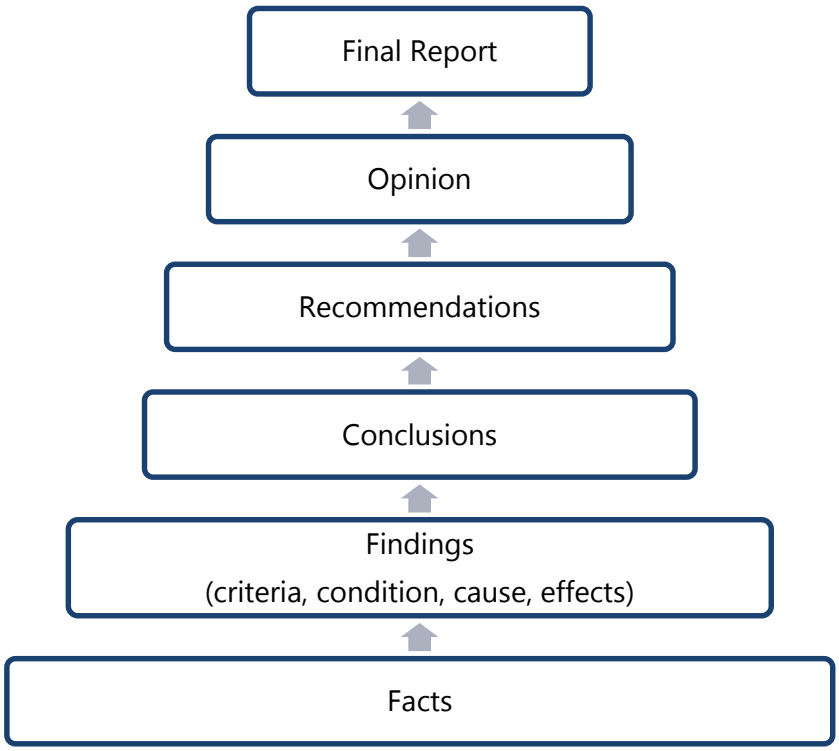
After the auditor has finished collecting data and evidence and recording the findings in the workpapers, the auditor will need to review the evidence and the workpapers in order to draw conclusions.

The conclusions will form the basis of the report, which is the method by which the internal auditors communicate the results of the audit.

8.1 Organise the facts

The first step towards drawing conclusions is to review and organise the facts that you have established during the audit process.

The purpose of this is to find out what these facts mean for the organisation and the client. These facts are the foundation of your report.



Once you have established what the facts are, you will need to organise them into findings.

A finding is made up of four elements:

Criteria	What the auditor would expect to see. For example this could be based on legislation or regulation, or on best practice or industry norms.
Condition	This is what is actually happening in practice (as opposed to what should happen, as per the criteria).
Cause	Why are the criteria not being met? The auditor must establish the root cause of the problem. This can be very difficult as it is easy to

	mistake a symptom for a cause. It is also possible that the root cause of the problem is much deeper than initially expected.
Effect	Finding the effect means asking yourself 'So what?' The effect can be any number of things. Wasted time and money are regular effects. Where the condition is non-compliance with legal requirements, fines and possibly jail could be potential effects.

8.2 Develop conclusions and opinions

The conclusions are based on the findings; they are the auditor's professional opinion of the activity based on the facts gathered during the audit process.

Conclusions should be clearly identified in the engagement report. They can relate to either the entire engagement, or just one part of it. Examples of what conclusions may cover include:

- Whether operating or programme objectives and goals conform with those of the organisation
- Whether the organisations' objectives and goals are being met
- Whether the activity under review is functioning as intended.

This list is not exhaustive and conclusions could cover other aspects of the review depending on what was found.

As well as conclusions, internal audit reports also include an opinion. An opinion could be an overall assessment of the controls of the area that has been reviewed, or again, it could relate specifically to certain controls or aspects of the engagement.

8.2.1 Types of conclusion

Audit findings and opinions can be positive as well as negative, presuming that there is sufficient reason to compliment the client.

Conclusions can be positive, negative or mixed. Look at the following examples for a review of the Payroll system.

Positive conclusion

"Based on the results of our audit, we believe that an adequate system of control has been established over the Payroll system and the objectives of the system are met effectively and efficiently."

Mixed conclusion

"In our opinion, the Payroll system is adequately controlled and, with the exception of the timely payment of casual workers, the system is operating efficiently and effectively."

Negative conclusion

"In our opinion, the Payroll system is inadequately controlled due to the lack of segregation of duties and responsibilities within the system."

9. Developing recommendations

Recommendations suggest ways that operations can be improved, or existing conditions can be corrected. They are based upon the internal auditor's observations and conclusions. It should be remembered that recommendations are only suggestions, not obligations.

Once the auditor has formed opinions and conclusions, they will use them as the basis for developing recommendations.

Recommendations are the auditor's suggestions for how the identified problems can be remedied.

However, just because you have developed a recommendation it doesn't mean that management will agree with it or see the point in acting on it. Disagreements can arise when the auditor is perceived by the manager as 'thinking they know better'. They may feel that the auditor is trying to do their job for them.

It is important that auditors do not take on the responsibilities of management as doing this may threaten their objectivity, particularly in consulting engagements where the auditor may be required to give specific advice on a problem, such as whether or not a new Computerised system should be installed.

If the auditor is responsible for actions based on recommendations, then their future objectivity is in doubt. This is because they could essentially end up auditing their own work.

Any impairment to objectivity should be disclosed to management immediately. Also, when making recommendations, the auditor should ensure any other conflicts of interest are disclosed.

Another way of preventing disagreements arising is through keeping the manager regularly informed of progress, alerting him to any developments or potential findings early on and

keeping the channels of communication open throughout the audit to ensure any misunderstandings or disagreements are resolved early on.

Any disagreements should be fully documented along with the reasons for those disagreements and the views of both the client and the auditor. If appropriate, the comments of the client can be included in the final report either as an appendix or in the covering letter.

9.1 Recommendations not obligations

It is important to remember that recommendations are just that: recommendations! They are not obligatory requirements that management must follow, rather they are a suggested course of action for remedying a problem. It is one option only, and auditors should remember that management may choose to follow a different course of action other than the one given in the report. This is because:

- Managers have a wider understanding of the likely outcomes of acting upon a recommendation
- Recommendations should be discussed with the manager before the end of the audit to ensure the best course of action is identified
- Working with the manager to jointly identify a solution will improve their working relationship
- The manager's involvement in developing the recommendations will improve the perception of the manager by his superiors.

Both the cost and benefit to the organisation of following a recommendation should be considered to ensure a balance between cost and risk. Sometimes however cost will be irrelevant, for example laws and regulation must be complied with regardless of the cost.

10. Reporting engagement results

ISQIA 8000 Reporting and communication

The followings aspects must be taken into account during the issuance of overall opinion and should include:

- Expectations of senior management
- The management board
- Key stakeholders and users of the information
- The possible prospects of senior management, the governing board and relevant stakeholders should be considered by the internal auditors when providing opinions and conclusions.

At the end of the audit engagement, the results have to be communicated to relevant staff. The results will be made up of a number of findings and recommendations and their aim is to get management to implement measures to solve the problems identified.

Internal audit reports are most likely to be received favourably if there are 'no surprises' i.e. the findings should already have been discussed with key personnel and their views incorporated to ensure the recommendations in the report are suitable, feasible, likely to work and likely to be accepted by management.

The head of internal auditors has the overall responsibility for ensuring the final report is prepared skilfully, well presented, provided to the relevant people, and kept confidential from all others.

10.1 Exit meetings

An exit meeting is held at the end of the audit engagement after a draft report has been produced. The people at this meeting are likely to be the same as those who attended the opening meeting (or entrance conference) and will include both operational staff who understands the workings of the operation that has been reviewed, and staff with suitable levels of authorisation to authorise the implementation of the corrective actions identified.

The objectives of this meeting are to:

- Discuss the findings and associated recommendations
- Provide the client with the opportunity to give their views on, and ask for clarification of, the observations and recommendations allowing any misunderstandings to be resolved
- Agree on possible solutions to the problems the audit has identified
- Acknowledge the help and participation of the client and thank them for their cooperation

10.2 Final report

You are now ready to put together your final report for the client. Depending on the organisation in question, this may take the form of a written report or take a different format, such as a PowerPoint presentation.

When putting the report together you should bear in mind the following to help make sure that everyone AGREES.

Approach as a team	You and the client are on the same side: the organisations. You must work together to find the best solution to allow the organisation to meet its objectives
General opening	Don't go straight into detailed findings; start at a general level and demonstrate your understanding of the operation
Rank findings	Start with the most positive findings, working through to the least positive
Encourage action	Present the negative findings as opportunities to improve, but don't overdo it
Effects of finding	Make it clear what could happen to the organisation if action is not taken
Summarise	Finish with a brief summary and end on a positive note

10.3 Contents of the final report

Although the content and format of the final audit report will vary from organisation to organisation, all should at the minimum include sections describing the purpose, scope and results of the engagement.

Purpose	The objective of the audit engagement should be clearly stated. This makes the report easier to read and helps the reader understand and interpret it. Findings should be linked back to this objective.
Scope	The scope defines what specifically is audited. It identifies which activities are audited and also highlights any activities that are excluded from the audit.
Results	This should include: • Observations • Conclusions • Opinions • Recommendations • Action plans

In addition, the final audit report may include the following, optional, sections.

Background information	This could include information such as details of the organisation and the activities reviewed, and the outcome of previous audits of the same areas
Summaries	An executive summary may be included to present the main findings of the report for those who do not have time to read the entire report
Client accomplishments	Improvements in relation to the past audit of the area may be acknowledged
Client views	The client's opinion on the findings and recommendations may be incorporated into either the main body of the report, an appendix or as a covering letter. Executives may need to intervene if there is a disagreement between the client and internal audit

Moreover, high quality reports will have the following attributes:

Accurate	The report should be free from error
Objective	It should be fair, impartial and unbiased. It should be based on facts
Clear	The report should be logical, easily understood and free from jargon
Concise	It should be to the point and free from unnecessary detail
Complete	No information essential to the intended audience should be omitted
Timely	The report should convey a sense of urgency

The final communication should be reviewed and approved by the HIA who will also determine the distribution list (see below).

In large organisations where it may not be feasible for this to be done by the HIA in every case, then this responsibility may be delegated to an audit supervisor, lead auditor or auditor-in-charge.

10.4 Distribution of the final report

ISQIA 8000 Reporting and communication

Internal auditors are expected to disseminate engagement communications successfully.

Internal auditors must state the presence of limitations on distribution and usage of the results in time of communicating engagement results to third parties outside the organisation.

Developments and outcomes of consulting engagements may be communicated in a manner most suitable for the nature of engagement and requirements of the users.

Communications are accurately made if it does not incorporate errors, misstatement, or distortions and based on relevant facts. Objective communications takes into account all relevant facts and conditions and are assessed on the basis of fairness and impartiality and are free from bias and prejudice.

The HIA is responsible for communicating the final results to those who are able to ensure that the results are given sufficient consideration.

The full report should be provided to those people who can take corrective action on the issues raised in the report. Summary reports should be provided to more senior managers.

Communication may also go to:

- External auditors
- The board
- Others who are affected by, or interested in, the results

10.4.1 Amendments

If any amendments are made to the report after it has been issued, the HIA should issue a new report which highlights any changes. This should be distributed to everyone who received the original report.

ISQIA 9000 Observation and control

Senior management and the board must be kept informed with current progresses and required changes as following internal audit activity. Therefore, the head of internal auditor should prepare timely report focusing on the purpose of internal audit activity, the level of authority, responsibilities of internal audit staffs and evaluation of performance. It is important to highlight any divergences from the initial internal audit engagement plan.

The report should also include identified risk factors, possible fraudulent activities, governance issues and any particular requirements of senior management and the board.

10.4.2 Releasing the report

If the report is to be released to parties outside the organisation, the HIA should assess the risks to the organisation of doing so and obtain approval from senior management, the legal counsel or both.

Consulting reports should only be released in line with the established practices of the organisation.

Due to the nature of activities evaluated with audit input, many organisations allow only limited distribution of their consulting reports.

10.5 Management response

After the issue of the final report, management will be given the opportunity to provide their formal response to the report. This formally communicates back to the audit activity what is going to be done about the recommendations raised.

The head of internal auditors must ensure the report has been communicated to people who will act on the findings in this way.

11. Obtaining client feedback

Client feedback helps the internal audit activity understand how it is perceived by the client and how well it is operating. It allows for continuous improvement of the service offered by the activity to better meet client needs and expectations, and also provides the opportunity to enhance client/auditor relationships.

The internal audit activity should aim to always improve and should add value to an organisation.

Customers are key stakeholders of the internal audit activity, and so their opinion is crucial for measuring value added and client satisfaction. The standard elaborates on this area of the improvement programme of the activity as follows.

Client feedback is an important part of any engagement and should be incorporated into every engagement undertaken by the internal audit activity. This should happen at the end of the process after the final report has been issued. The Head of internal auditors should contact the client at this time to request this.

A simple way of measuring feedback is through the use of a client satisfaction questionnaire which would be provided to the key audit contacts at the end of the process. This could include questions such as:

- How disruptive to your normal operations did you find the audit process? Could anything have been done to improve this?
- Was the audit carried out in a timely manner? Could the timing have been scheduled better to reduce disruption?
- Was the auditor helpful and approachable? Did the auditor establish good working relationships with your staff and management?
- Did the auditor conduct the audit in a professional manner?
- How relevant do you think the findings are? Will their implementation improve effectiveness, efficiency or compliance?
- Was the audit process in line with your expectations?
- Do you have any suggestions for how we can improve our processes?

The outcome of the questionnaires should be used to improve the audit processes and to enhance customer relationships.

The auditor should be allowed to respond in writing to any negative feedback. Any major discrepancies may have to be resolved by the HIA by bringing the auditor and client together to discuss the problems.

12. Performance appraisal

ISQIA 9000 Observation and control

The head of internal auditor must design and execute a monitoring system when results are being communicated to organisation's management.

Staff performance appraisals should be carried out at the end of the audit engagement to evaluate its success and identify any training and development needs.

As well as evaluating the performance of the internal audit activity from the point of view of the client, staff performance appraisals should also be carried out to assess the current skills of the internal auditor and identify any training and development needs.

Appraisals such as this can improve the quality of the internal audit activity by assisting auditors in learning more effective techniques for carrying out their work. This also helps the auditor continue his own professional development and meet his own personal objectives.

12.1 Scheduling the review

Auditors' performance should be reviewed:

- Annually, by the HIA
- Following each specific audit, by the auditor-in-charge

Reviewing performance directly after an engagement is good as the performance is still fresh in the minds of the auditor and the reviewer, however, the variety of engagements can lead to a great variation in reviews.

The HIA will carry out an annual review of the auditor which will take into consideration all of the post engagement reviews that have occurred during the year. These reviews can provide a more accurate, longer term picture of the auditor.

12.2 Review topics

Audit engagements are all very different, and so the items discussed will vary from review to review. However, there are a number of core elements which will be discussed as part of any post-audit performance review.

- The quantity of work done
- Timeliness, i.e. the ability of the audit to keep to the schedule
- General grasp of audit procedures
- Specific understanding of the review completed
- 'People skills' with the client, staff and audit supervisor
- Quality of work performed, e.g. appropriate tests chosen, accurate computation, clarity, thoroughness, writing quality, sufficient testing, logical conclusions, supporting evidence etc..
- Special skills demonstrated, e.g. IT auditing
- General business knowledge

12.3 The performance review meeting

A face-to-face meeting should occur as part of the performance review process. This meeting should be approached in the following way:

- Schedule the meeting in advance
- Book the meeting for the appropriate length of time to cover all items on the agenda
- Open in a suitable manner, friendly small talk may be suitable in some cases though not for others
- Begin with a brief outline of what will be covered along with an indication of the overall ratings. Where possible always begin with a positive statement, and be as objective as possible when delivering negative news.
- If self-assessment is to make up part of the review, this should have been communicated to the auditor in advance to allow for preparation time.
- Be straightforward and honest – the auditor can only develop if you are honest about their current performance levels.
- Summarise at the end. This should cover both the main positive and negative points
- Get the auditor to commit to taking the agreed actions

Chapter 03: Sampling and statistics

1. Statistics

Mean, median, and mode are three kinds of "averages". The range is the difference between the largest and smallest values in the population.

Probability is about the chance of something happening. Events, or outcomes, may or may not be related to each other. A common distribution pattern is the normal distribution, which results in the bell-shaped curve. The height and width of this curve is determined by the standard deviation.

1.1 Mean, median, mode and range

1.1.1 Mean

The mean is the average you're used to; where you add up all the numbers and then divide by the number of numbers.

Mean is the sum of all the items in the sample divided by the number of items in that sample.

Let's calculate the mean for the below series of numbers:

17 27 17 19 17 23 19 33 17

First, add up all the numbers in the sample:

$$17 + 27 + 17 + 19 + 17 + 23 + 19 + 33 + 17 = 189$$

Then divide this by the total number of items in the sample (9):

$$\frac{189}{9}$$

The mean is **21**

1.1.2 Median

The median is the value that would be in the middle of the list, if all your items were listed in numerical order.

Median is the midpoint of all values in the sample, with an equal number of values above and below it.

Let's calculate the median for the same series of numbers as we used above:

17 27 17 19 17 23 19 33 17

First, arrange the numbers into numerical order:

17 17 17 17 19 19 23 27 33

In small samples like this is it easy to identify the middle value:

17 17 17 17 19 19 23 27 33

In larger samples, you may have the values stored electronically and use a spreadsheet to reorder the values into ascending order. In such large cases, you may not be able to easily identify the middle value using your eye; you will need another method of identifying the median.

The median can be found using a very simple formula:

$$Median = \frac{(Number\ in\ sample\ +\ 1)}{2}$$

So using this for the above series of numbers:

$$\frac{9+1}{2} = 5$$

Therefore the median is the 5th number in the line:

17 17 17 17 **19** 19 23 27 33

1st 2nd 3rd 4th **5th** 6th 7th 8th 9th

The 5th number is 19, therefore this is the median.

If there are an even number of items in the sample, say 10, then the formula will give you a half number:

$$\frac{10+1}{2} = \frac{11}{2} = 5.5$$

In this case, you would take the 5th and 6th number and the median would be the value half way between the two figures given. Let's say the 5th item was 18 and the 6th item was 20, then the median would be 19.

1.1.3 Mode

The "mode" is the value that occurs most often. If no number is repeated, then there is no mode for the list.

The mode is the most frequently occurring number in a sample.

Let's calculate the mode for the same series of numbers as we used above

17 27 17 19 17 23 19 33 17

The mode is clearly 17, as this occurs more times than any other number in this sample.

Sometimes you will find that there is no mode, this can happen when no number is repeated more frequently than any other, as is the case with the sample below.

1 9 23 17 6 81 32 14 12

Every number is used only once and therefore there is no mode in this sample.

1.1.4 Range

The range is the difference between the largest and smallest values in the population.

Let's look one more time at our series of numbers

17 27 17 19 17 23 19 33 17

The largest value in the sample is 33

The smallest value in the sample is 17

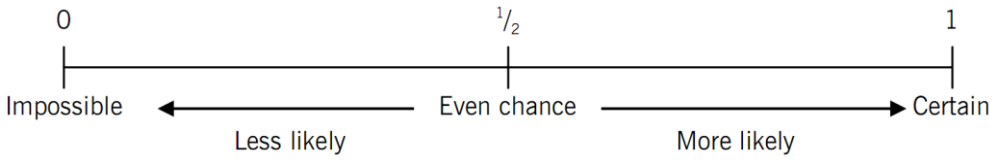
This means that the range is 33 – 17 = 16

1.2 Probability

Probability is about the chance of something happening. It uses estimation techniques to work out the likelihood of particular outcomes occurring and provides a basis for making decisions.

The chances of any event can be shown on a probability scale from 0 to 1.

- A probability of 0 tells us that the event will never happen – it's impossible
- A probability of 1 tells us that the event is certain to happen
- A probability of 1/2 tells us that the event has an even chance of happening



Unlikely events are closer to 0 and likely events are closer to 1.

Objective probabilities are calculated from experience or logic. For example, you could logically expect throwing 'heads' when flipping a coin to have a probability of ½, or you could actually experience it by flipping a coin 100 times and determining this probability.

Subjective probabilities are estimates based on judgment and past experience. This kind of probability indicates the level of confidence a person has that a certain event will occur.

1.2.1 Probability relationships

Events, or outcomes, may or may not be related to each other.

Mutually exclusive	They cannot occur simultaneously, e.g. you can't get heads and tails in a single coin toss.
Joint probability	Both events will occur e.g. you will get heads and roll six.
Conditional probability	The probability that one event will occur given that the other has already occurred.
Independent events	The occurrence of one effect has no effect on the probability of the other, e.g. rolling two dice.

1.2.2 Combined probability

Joint probability for two events is the probability of the second event occurring given the first happened. It is calculated by multiplying one by the other.

For example, if 40% employees are female, and 25% of staff have line management responsibilities, then the probability of an employee selected at random being a female with line management responsibilities is:

$0.4 \times 0.25 = 0.1$

The probability that one or both of two events will occur is the sum of their separate probabilities minus their joint probability.

Therefore, using the same example, the probability of the randomly selected employee being either female, or having line management responsibilities, or both is:

(0.4 + 0.25) – 0.1 = 0.55

1.2.3 Probability distributions

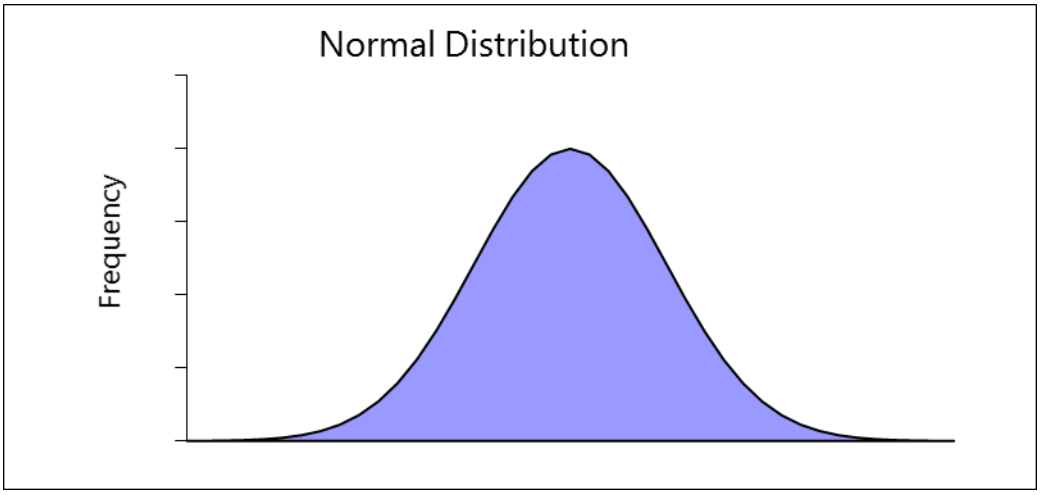
The probability of events occurring often follows a pattern. Common distribution patterns include:

Uniform distribution	All events occur equally. For example, on a dice a 6 is just as likely as a 1 or a 3.
Binomial distribution	There are only two possible outcomes, for example heads and tails.
Poisson distribution	The event may occur more than once with random frequency during the given period.
Normal distribution	Many events fall into this category. If the outcome of each event was plotted on a chart, the result would be a bell-shaped curve. This is such an important distribution we will look at it in detail below.

1.3 The normal distribution

The kind of probability we are concerned with is based on variation of a characteristic within a population. The population might be, say, men in the US and the characteristic might be, say height. Equally well, the population might be all the widgets a factory produces in a year and the characteristic might be their weight in grams. The important point about these two characteristics is that they vary from individual to individual and their variation is normally distributed.

Normal distribution of a population variable implies that its magnitude tends to clump around the mean, but there are also likely to be individual cases that are quite a long way from the mean. If we draw a graph to show the frequency with which actual measurements occur in a normally distributed variable, it will be a bell shaped curve such as the one below.



A good way to visualise the way the normal distribution works is to imagine looking down vertically on a soccer pitch with a large number of people standing on it. We have measured all these people's height and worked out the mean.

We persuade all the people whose height is equal to the mean to line up one behind the other along the half way line, starting from one of the touch lines; then the people who are one centimetre taller than the mean line up immediately to their right and those who are one centimetre shorter line up on their left, both starting from the same touch line. Then we repeat the process with those who are two centimetres taller and two centimetres shorter and so on, until everyone is in place.

If we then look down on the shape of our crowd, we will find that it is very close indeed to the curve shown above. We have drawn a graph using the touch line as the x axis and the centre line as the y axis. The people of mean height will be the most numerous and they will be at the centre of the curve. Taller and shorter people will be fewer in number and the greater the difference from the mean, the fewer people there will be. Eventually, as we move out towards the goal lines at either end, there might only be one or two people who are sufficiently tall or short to qualify.

It would probably take several thousand people to make this demonstration work. Even so, they would represent only a sample of the entire population of the country, so it is unlikely that we

would encounter anyone who was outstandingly tall or short. But such people do exist and we cannot say for certain where the final limits of human height lie. The same is true of all normally distributed variables and so the tails of the normal curve never actually meet the x axis of our graph.

1.3.1 Standard deviation

However, we can say some other very precise things about our normally distributed variable. We can work out a measure of the variable called the standard deviation. How this is done need not concern us here, so long as we understand what it tells us. The standard deviation gives us an indication of the dispersion of the variable; that is to say, whether the curve is very tall and narrow, with most of the population values very close to the mean, or very low and flat, covering a wide range of measurements. The smaller the standard deviation, the taller and narrower the curve.

The standard deviation is interesting when we come to consider probability. The area under a part of the curve defined by a given number of standard deviations from the mean is easily obtained from mathematical tables. So, for example, if we take the part of the curve that lies within two standard deviations on either side of the mean, we find that approximately 95% of the population will lie under it.

Going back to our height example, if the mean is 170 cm and the standard deviation is 10 cm, we can say that approximately 95% of people are between 150 cm and 190 cm tall. If we include everybody within three standard deviations, using the tables, we can say that over 99% of the population will be between 140 cm and 200 cm tall.

This is all very comforting and precise, but what does it have to do with probability, which, you may recall, was why we started on the normal distribution in the first place?

1.3.2 Probability

To deal with probability, we have to turn the concept on its head. We started off by describing the normal curve in terms of a very large number of people and we have discussed how it defines one of their variable characteristics: height in our example. We now think about what it can tell us about a single individual. While it cannot tell us anything absolutely precisely, it can tell us something useful with a certain degree of probability.

If we know, for example, that a person is a member of the population whose height we measured earlier, we can say with 95% probability that his or her height must lie in the range 170 cm to 190 cm. That is, we know that 95% of the population lie within that range, so a randomly chosen

individual must therefore have a 95% chance of being in that section of the population and, equally, of lying in that height range. Another way of using the same facts would be to say that our randomly chosen person has only a 5% chance of lying outside that height range.

2. Statistical and Judgmental Sampling

During audit engagements, restraints (such as time, money and resources) mean that it is usually not possible to look at everything.

Although a 100% review would give us 100% assurance, the cost of this is likely to exceed the benefits. It is also generally not possible to do all the work necessary to review every item that is subject to audit, nor would this be desirable due to the time and cost involved.

Therefore, we have to test only a sample and use the results to draw conclusions for the whole population.

The aim of sampling is to select a subset of items that provide a reasonably accurate reflection of the whole population.

Population. The total number of items from which a sample is chosen. The population may also be referred to as the 'universe' or 'field'.

The auditor's expectation is that the sample selected is representative of the population, i.e. it should have the same characteristics.

Sampling risk arises from the possibility that the auditor's conclusion, based on a sample, may be different from the conclusion that would be reached if the entire population were subjected to that same audit procedure.

Internal auditors need to make sure this risk is managed, so the greater their reliance on the results of the procedure, the lower the sampling risk they are willing to accept, so the larger the sample size will need to be.

2.1 Statistical Sampling

There are two main categories of sampling: statistical and judgmental.

Statistical sampling means choosing a scientifically random sample in such a way that the results can be given in terms of confidence level, or precision.

2.1.1 Sample size

The appropriate sample size for an audit test will depend on five key factors. These factors should be considered together to achieve the right balance and ensure that the sample objectives are met.

(1) Margin of error

No estimate taken from a sample is expected to be exact, inference to the population will have an attached margin of error. The margin of error is an estimate of the possible difference between the sample estimate and the population actual. The margin of error can be reduced by improved sample design, however in most cases this also means increasing the sample size. The lower the acceptable margin of error, the larger the sample required.

(2) Variability in the population

The amount of variability in the population i.e. the range of values or opinions, will also affect accuracy and therefore the size of sample required when estimating a value. The more varied the population, the less accurate the sample estimate and so the larger the sample size required.

(3) Confidence level

The confidence level is the likelihood that the results obtained from the sample provide a reasonable estimate of the characteristics of the overall population. The higher the confidence level required (i.e. the more certain you want to be) the larger the sample size.

(4) Population size

The larger the population size, the larger the number of items in the sample but the lower the proportion of that population that needs to be sampled to be representative.

(5) Population proportion

This relates to the number of items in the population that display the required attributes. This is a consideration if the purpose of testing is to sample for attributes rather than the calculation of an average value. This can be estimated from the information that is known about the population, for example the proportion of hospitals who consider long waiting lists to be a problem.

However, practical limitations will often be the chief determinant of the sample size.

The decisions surrounding the sample design and methodology should be discussed with all the parties involved to ensure their agreement to the process and avoid problems during clearance.

(Clearance is the process of agreeing the findings and recommendations with the client at the end of the engagement.)

2.1.2 Advantages and disadvantages of statistical sampling

Advantages	Disadvantages
• May yield desired results from minimum number of items • Yields quantified data • Includes a measure of sampling risk, level of • confidence and precision • Well adapted to computer testing • Provides more credible support for conclusions and recommendations	• Can be expensive and time consuming • May require staff training and software costs • May preclude insights about the population available from experienced audit staff

2.2 Judgmental sampling

Judgemental samples are selected based on the auditor's informed assessment of how many items should be in the sample to give a reasonably reliable result.

Where this method is used, the scope of the test in the working papers should clearly state that the sample was selected judgementally, and go on to describe exactly how they were selected. They will have been selected in one of the following ways

Systematically	Selecting every nth item, starting with item x
Unsystematically (haphazard)	Taking files from cabinet with no criteria
Using auditor judgment	Selecting large or unusual items from a report

Note that unsystematic sampling is not the same as random sampling. Random sampling will be truly random and so will involve some statistical element to ensure that every item has an equal chance of being chosen.

Unsystematic doesn't have this same assurance, it is natural to select from a cabinet at some kind of intervals, it would be unlikely you would chose four consecutive items from next to each other, but in a random sample this would be just as likely as any other combination.

2.2.1 Advantages and disadvantages of judgmental sampling

Advantages	Disadvantages
• Allows the auditor to use professional judgment to select the items that most need to be tested • Can be designed to achieve cost-effective, reasonably reliable results	• Can't produce statistically valid results • Cannot state a measurable sampling risk • May lead to auditing too many, or too few items • Reliant upon experience and skills of auditor for its effectiveness.

3. Sample Selection

There are a number of methods that auditors can use to select a sample. Different sampling techniques suit different situations.

3.1 Methods of sample selection

There are a number of methods that an auditor can use to select a sample.

Method	Definition	Uses	Limitations
Cluster	Groups or clusters exist in the population, for example schools or households. A sample of clusters is then taken and all units within that cluster are included.	Fast and cheap Does not require complete population information Good for face to face interviews Works best where cluster can be considered to be microcosm of the population	Increased levels of sampling error If clusters are large it can be expensive Larger sample size may be required due to increased sampling error

Random number sampling	Every item is allocated a number, then a random number table, or computer software such as IDEA is used to select the sample	Every item of the population has equal chance of being selected Produces fair estimates of population Easy to select and interpret sample	Complete and accurate population information required
Stratified random sampling	Similar to cluster except the auditor arranges the data in groups. Data is then selected randomly from each of those groups	Ensures all main groups are represented in the sample Can reduce sampling error	Good population information required Selection process is more complex
Interval sampling	Selecting every nth item starting at item x. For example, every 15th item starting at 40. Sample would include items numbered 40,55,70,85 ... and so on.	Easy to extract the sample Ensures the sample is spread over the whole population	Can be expensive and time consuming if sample is not located conveniently Can be used where periodicity in the population exists.
Haphazard sampling	Items are 'chosen at random' although it is not a random sample as judgment is still involved. Files are chosen using no criteria	Questionnaires are an example of this kind of sampling	Likely to contain bias Not as reliable due to judgment element

3.2 Sample techniques

Different sample techniques are better suited to different audit objectives. The below table shows what method best suits each audit objective.

Audit objective	Approaches
To determine if items possess an attribute, e.g. an invoice has been paid	**Attribute sampling** This is particularly well suited to compliance audits, where the auditor is trying to gauge levels of compliance. The aim of this kind of sampling is to identify specific attributes. The sample size can be chosen statistically based on rate of errors, confidence levels, population size, etc. or can be selected based on the auditor's opinion of the conditions.
To determine if items possess an attribute, e.g. an invoice has been paid without looking at too large a sample	**Stop and go sampling** The stop and go method avoids testing excessively large samples. It is best suited to testing populations that the auditor believes is relatively error-free. The auditor selects a small sample and if it displays the expected low error rates, then the auditor can choose to stop testing. The auditor can carry on and take a larger sample if the results are not in line with expectations
To identify a single instance of a suspected problem	**Discovery sampling** This is used where the aim is to find at least one example in the population. Auditors need to select a sample which they believe is large enough to make this likely Tables are available to assist with determining how large that should be. This method is well suited to looking for fraud. If the single instance turns out to be large (e.g. a large value fraud) then additional testing may still be needed to determine the scale of the problem.
To measure a variable characteristic, e.g. dollar amounts	**Variables sampling** Variables sampling is used to estimate the average value, or total value, of a population.

	It can be applied to populations made up of days, dollars, pounds etc.. For example, it could be used to calculate the cost of inventory components as follows: 1. Sample a number of the components 2. Work out the cost-per-item 3. Statistically determine the plus or minus range of the cost of the total inventory under review
To combine attributes and variables to determine the dollar amount of error in an account	**Dollar-unit sampling** This method combines aspects of attributes and variables sampling and provides some of the benefits of both. It can be applied to attributes, but expresses results as variables so can also be used for substantive tests. It differs from most other sampling techniques as the units are defined as individual dollars rather than specific units (such as inventory items). The items that are included in the sample to be tested are those that contain the dollars selected. This selection method ensures that every $1 in a population has an equal chance of being selected. This method is easy when using a computer and ensures that every material item will automatically be selected. However, without a computer this approach can be very time consuming. (Material items are those that are large enough, or otherwise significant enough to be of interest to the internal auditor).
To test a selection of the population without attempting to characterise the entire population	**Judgment sampling** This method of determining sample size relies on the auditor's knowledge and experience. It is best suited to fairly uniform populations or those subject to strong controls. It also allows the auditor to focus on those parts of the population with weaker controls, or that display certain characteristics.

Chapter 04: Gathering data and other engagement tools

1. Interviewing

The ability to hold successful interviews is a core skill for internal auditors. Much information can be found out if the auditor simply 'asks the question'.

The aim of the internal audit interview is to uncover facts. It should ideally be a relaxed discussion centred around what the interviewee does as part of their job. It should also be structured to ensure the interview does not veer off course and to keep the need for follow-up interviews to a minimum.

Although audit interviews may be part of daily life for internal auditors, this is unlikely to be the case for the interviewee. The auditor should not lose sight of this and should make the effort to put the auditee at ease. Whilst you may be trying to evaluate a system of controls, the auditee may feel you are trying to evaluate them. This can cause people to become defensive, which make it increasingly difficult to establish the facts. The auditor should ensure the full reasons for the interview are communicated to the interviewee, and any concerns they may have are addressed.

This is particularly important when there is an element of risk involved for the interviewee. For example, an interview relating to the suspected fraud of a colleague can be particularly stressful for an auditee. The job of the auditor is to ensure the required information is obtained, without backing the interviewee into a corner or forcing information out of them. An audit interview is not an interrogation. That said, the auditor should remain alert for any indications of fraudulent activity that may exist below the surface.

Auditors should develop several skills in relation to interviewing:

- Planning skills to ensure the interview is efficient and productive
- The ability to create rapport with the interviewee
- Empathy for the interviewee. This will help them to understand their point of view, and also assist the auditor in distinguishing facts from the opinions of the auditee

1.1 Stages of the interview

Successful interviews should be made up of the following stages:

Stage 1 Planning

Interviews should be carefully planned in order for relevant, useful, factual and complete information to be obtained.

Auditor should consider:

- Subject to be discussed
- Approach to take (this will differ based on the subject being discussed and the person being interviewed)

The planning stage can be broken down into seven key steps:

Step 1 Obtain background information about

- Activities to be discussed (prior audits, organisation charts, systems documentation etc.)
- Person to be interviewed

Changes in the organisation/operation that might affect the interviewee

Step 2 Clearly **define purpose** of interview with specific objectives

Step 3 Prepare **questions to achieve those objectives**. These can be open and closed, but not biased:

Open: invite interviewee to speak at length and gives them more control. Useful for developing rapport. Unhelpful if auditor requires a definitive yes or no.

Closed: Require a specific response, i.e. yes/no or a number, date etc..

Unbiased: provides no clue as to the expected response. Asking biased questions is a frequent mistake made by auditors.

Step 4 Organise questions into a **logical sequence**. This keeps the interview on track and improves the flow of conversation.

Step 5 If the interview is formal (for example a meeting with senior management) prepare an **agenda**

Step 6 **Tailor the objectives and questions** to the person's role in the company (senior management, operating management, operating personnel etc.)

Step 7 **Schedule** the interview. Inform interviewee of purpose of the meeting and agree time and length of meeting.

Stage 2 **Opening**

Start the interview on time, with a friendly introduction

Clearly state the objectives of the audit and specific purpose of the interview

Build rapport to help break down the barriers between the auditor and interviewee

Stage 3 **Conducting**

Be confident, but not intimidating and project a professional image with both words and body language

Avoid sarcasm, jargon or language that could be considered offensive or confusing

Take as few notes as possible and keep your focus with the interviewee. Watch their behaviour for any gestures that indicate discomfort or are not in line with what they are saying

Maintain interest in the interviewee and encourage them to express their concerns as well as the facts

Use follow-up questions, such as 'could you give me an example'

Summarise or restate difficult information the way you understand it to ensure you have not misunderstood

Engage in dialogue and make eye contact, don't simply read out a list of questions and write down their answers

Distinguish fact from opinion

If it is necessary, bring a second auditor to the meeting but take care to not come across as intimidating

Stage 4 **Closing**

Don't exceed the agreed deadline. As it approaches ask permission to wrap up the meeting and reschedule if you still have questions.

Summarise the key points from your notes

Describe the next step in the process

Provide contact information and ask interviewee to let you know if they think of anything else that may be helpful

Thank the interviewee for their time

Stage 5 **Documenting**

Review and organise your notes directly after the interview.

Write up your notes for inclusion in your workpapers. It is important to do this straight away whilst the events are still fresh in your mind to ensure you document it exactly as it happened.

Stage 6 **Evaluating**

The final stage involves evaluating the information you obtained during the interview to determine if:

- You met all your objectives and recorded all necessary information. If you did not achieve this you should identify what prevented you doing so?
- Your planning was sufficient, for example, there were no surprises due to lack of research, your questions flowed logically, the interview was well timed, in an appropriate place, and of sufficient length.
- You established rapport with your interviewee. Again, if not, what prevented you from doing so?
- You explained the purpose of the audit and the objectives of your interview in a way that put the interviewee at ease.

2. Questionnaires

Questionnaires are useful tools for quickly collating standard information from a large number of recipients, however they are limited in the level of detail they are able to provide.

Many of the questionnaires used by internal auditors are internal control questionnaires (see below), however they may also be used in control self-assessments (CSAs) and during preliminary work.

2.1 Internal control questionnaires (ICQ)

Internal control questionnaires (ICQs) are used to document the adequacy of process activities and controls.

They successfully document initial responses to the controls and allow information to be gathered from a large number of recipients; however they do not provide in-depth knowledge of those controls.

Internal auditors must carefully plan the format of the questions to be included in the questionnaire to ensure the information received is useful.

ICQs are usually yes/no style questionnaires where 'yes' indicates a system strength, and 'no' a weakness. A space for narrative follow up to the questions should also be included.

2.1.1 Advantages and disadvantages of questionnaires

There are a number of advantages and disadvantages to using questionnaires and they lend themselves better to some purposes than others.

The below tables illustrates the main general advantages and disadvantages to yes/no style questionnaires.

Advantages	Disadvantages
Easy to administer Provide uniform information from all respondents. This facilitates accurate comparisons Can be provided to large number of informants in disperse locations	Not appropriate to all situations/issues Do not provide in-depth information Limited opportunity for auditor to observe respondent's behaviour and environment. Some people will not respond to any kind of questionnaire for fear of repercussions of providing their views in writing. Others provide positive responses whether or not it is true in order to attempt to shorten the audit.

Questionnaires are best suited to gathering information about:

- Multiple units (e.g. branches) that have the same processes, risks etc.
- Regulatory compliance, or other yes/no matters

3. Checklists

Checklists help to ensure consistency and completeness in carrying out a task.

Checklists contain a list of items along with boxes or spaces for a checkmark. The item will be checked off when it has been confirmed. A simple example you may use in your everyday life would be a to-do-list. The tasks you need to complete are listed and checked off as you complete each task.

If an item on a checklist has been checked, this indicates a 'yes'. If the checkbox is left blank this indicates a 'no'.

Checklists can be very useful tools for internal auditors and can assist them in a number of ways:

- As a memory aid for the auditor to make sure all questions have been asked and all observations have been made
- As an information gathering device to rapidly obtain information from clients (like a mini-questionnaire)
- As a control to make sure all the relevant activities have been performed during the audit to ensure all the audit objectives have been met

4. Observation

The power of observation as an audit tool should not be underestimated; by observing a process directly it is possible to obtain information that can't be gathered by transaction testing or the review of documentation.

Observational skills, although partly inherent, should be developed. The more skill, knowledge and experience an auditor has in this area, the better they are able to gather significant audit information through purposeful observation.

Auditors may observe any number of things, for instance:

- People
- Processes

- Activities
- Inventories
- Facilities
- Safety systems
- Office layouts
- Equipment

The observations made then feed back into workpapers and can become the basis of findings and recommendations.

In some audits, observations made by CCTV (e.g. post room cameras in an audit relating to receipts of income) and photographs (e.g. a health and safety audit) can form the basis of audit findings and recommendations.

4.1 Effective observation

In order to carry out effective observation the auditor should:

- Prepare in advance. The more an auditor knows about the area or process before carrying out the observation, the better they will understand how it should work and will better know what to look for.
- Put observations into context. Observations are more meaningful when put into context. An auditor can do this by comparing those observations to prior observations of the process, to best practice guides, to the claims made by clients prior to the observation, to documents such as process notes produced by or for the client etc..
- Notice what is missing. As well as documenting what the auditor observes, it is also important (sometimes more so) to notice what is absent from the process, or what could not be observed.

4.2 Confirming observations

Observations alone are generally considered to be weak audit evidence; therefore they should be backed up by further evidence or analysis in order to have sufficient impact in the audit report.

One way of doing this is to involve the client in the observation and getting them to agree any findings. If this is not possible, this, along with the observation itself, should be recorded in the report.

4.3 Misleading observations

Although observations can provide the auditor with valuable insights about a process or department, it is important to be aware that some observations can be misleading. This happens because the people in the department know they are being watched, and will probably react to this by being on their best behaviour. As a result problems that regularly occur may not be made apparent to the auditor during the observation causing incorrect conclusions to be drawn.

5. Process mapping

Process maps visually show the steps of a process. The most common form of process mapping is the flowchart; a document that illustrates how the steps flow from one to the next.

Flowcharting software allows flowcharts to be created electronically. Basic flowcharts can be created using Microsoft Word or Excel. Specialized software such as Microsoft Visio allow for more advanced process mapping.

5.1 Using flowcharts

Flowcharts can be extremely useful tools for internal auditors, as charting the process allows them a visual, easy to follow, start to finish view of the operation. This makes it easier for the auditor to identify:

- The key stages in the process
- Stages which can be omitted
- Missing stages which, if added, would improve the process
- Sequencing issues, for example a review of the process may indicate that re-ordering some of the steps would be more efficient

This can be applied to any process, including the internal audit process itself. They can be used to develop, refine or audit processes.

5.1.1 Creating flowcharts

Sticky Notes can be a helpful tool in creating flowcharts of processes that involve lots of stakeholders. A session with all key stakeholders is held during which each step is written on a single note. The notes can be rearranged to identify the order in which they occur.

The process of creating flowcharts can help identify weaknesses in controls, for example:

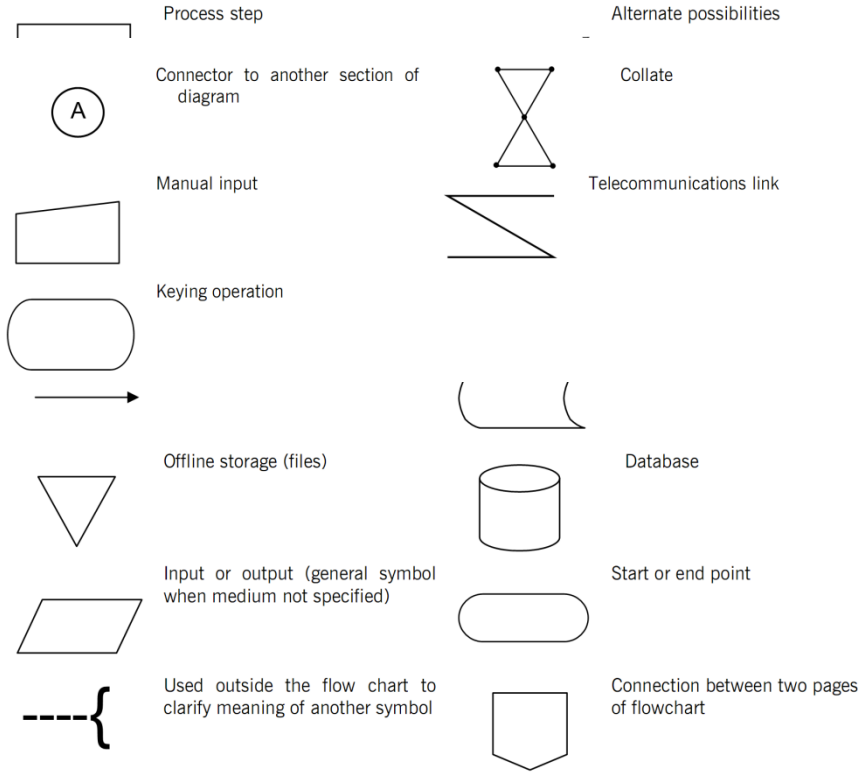
- Lack of segregation of duties

- Duplicate processes
- Failure to obtain appropriate authorisation
- Control loopholes – areas where circumvention of controls is possible

When the processes are then observed in practice, it may also become apparent to the auditor that the flowchart represents what should happen, not what actually happens in practice. This may also indicate problems in the system.

5.2 Standard flowchart symbols

Standard flowcharting symbols have been developed to improve consistency and aid the understanding of users or recipients of flowcharts. The following illustrates the symbols you are most likely to encounter in your career.



5.3 Flowchart formats

Flowcharts can take either a horizontal or vertical format. The chosen format may depend on:

- Available space on the page
- The emphasis of flow, e.g. through organisational functions, through processes

Flowcharts (in any of the formats) can be used to chart complex, as well as simple, processes. Effective use of footnotes allows for further descriptions of the steps and additional information to be communicated to the reader.

5.3.1 Horizontal flowcharts

Horizontal flowcharts flow across the page from left to right and focus on the steps in the overall process. Although the departments/functions involved are mentioned, they are not the focus of the flowchart. They are instead shown at the far left of the chart.

5.3.2 Vertical flowcharts

There are two types of vertical flowcharts; those which place the emphasis on process steps, and those which focus on functions.

Those which focus on process steps flow down the page, from top to bottom, and contain no reference to functions at all. This kind of chart can be helpful if descriptions of the steps of the process are required as there will space available on the page for this to be added next to the flowchart steps.

In contrast, vertical flowcharts which emphasise functions use a combination of vertical and horizontal structures and the functions are clearly identified at the top of the flowchart.

6. Problem solving

At the end of the sampling and testing process, the auditor will have a list of findings relating to lack of compliance or other failures to achieve business objectives. The auditor then needs to translate these findings into recommendations that will be agreed by management and, once implemented, solve the identified problems.

6.1 Five attribute approach

Well-developed audit findings have five specific attributes:

(1) Condition

(2) Criterion

(3) Effect

(4) Cause

(5) Recommendation

The five attribute approach to problem solving involves giving consideration to each of these attributes. We will know look at each of them in turn.

6.1.1 Condition

Condition means to look at what is currently in place.

The auditor should describe the situation that is considered to be a problem. This description should be free from bias or judgments and should stick only to the facts. These facts should be backed up with appropriate evidence wherever possible.

This is because opinions or judgments can be argued, but facts cannot (although they can be disproved if they are in error).

An example could be "23% of purchase orders had not been authorised". This could be supported by documented evidence run from the finance system.

The information contained in this description should also be carefully selected to suit the intended audience. For example, some managers may prefer a less formal style of communication, whereas another may expect to see lots of facts and figures. By matching style to recipient, auditors can provide the most convincing report of a finding.

6.1.2 Criterion

Criterion is a description of how things should be.

For example, in relation to the purchase order example above, the criterion could be 'All purchase orders should be authorised by the relevant budget holder'

The condition should be compared to the criterion to prove that it is deficient.

Selecting an appropriate criterion can require skill, experience and tact. In the example above it may be fairly easy if this is documented in the company policy and procedures. Sources such as this are ideal as they are easy to use and have sufficient authority behind them. In addition to company policies and procedures, other similarly good sources include:

- Industry regulations
- Legal requirements
- International Financial Reporting Standard (IFRS)

Where such sources are not available, auditors may use sources such as

- General internal control principles, such as segregation of duties

- Best practice
- Industry averages
- Common sense

However, these sources have only minimal impact compared to the authoritative sources discussed previously.

6.1.3 Effect

The auditor should strongly state the negative effect caused by the problem.

Change usually involves cost (time, money, resources etc..) and so management will only make changes if they feel it is worth it. To make sure the change is perceived to be worth the effort, the effect should be strong enough to give the report maximum impact.

For example, thinking about the authorisation of purchase orders again, a suitable effect may be 'If purchase orders are not authorised there is increased risk that inappropriate expenditure will be incurred or purchases for personal use will be made'.

To do this, the auditor must first assure himself that the problem is genuinely affecting, or will in the future affect, the organisation. If a report contains solutions to problems that are not affecting any stakeholders (management, employees, customers, suppliers etc..) then the credibility of the report will be brought into question.

In some situations, it may be that the condition alone is not a problem, yet combined with other related conditions it becomes problematic. It is also possible that the past effect cannot be determined. In such cases the potential effect should be reported as realistically as possible.

The effect needs to help you 'sell' your recommendation to management as something that can genuinely improve performance, generate savings etc. The best way to do this is to quantify the potential improvement in terms of cost savings, units of production, market share or other appropriate measure.

6.1.4 Cause

The auditor needs to determine what is causing the condition to occur and access the root problem underlying it.

Symptoms may have to be eliminated before it can be determined. If the root cause it not identified, the symptoms are likely to recur.

Determining the cause can be one of the most challenging tasks faced by internal auditors.

The cause of our purchase order example might be a number of things. It could be that a sufficient documented process has not been put in place that requires authorisation to be obtained. It could also be that the procedure is there but for some reason is being ignored. This is not the root cause; the auditor must establish why it is being ignored. Maybe it is not practical (perhaps due to staff locations) and it is being bypassed by staff in an attempt to 'get the job done'.

6.1.5 Recommendation

Finally, the auditor needs to review the condition, criterion, effect and cause and use this to deliver a credible recommendation to management.

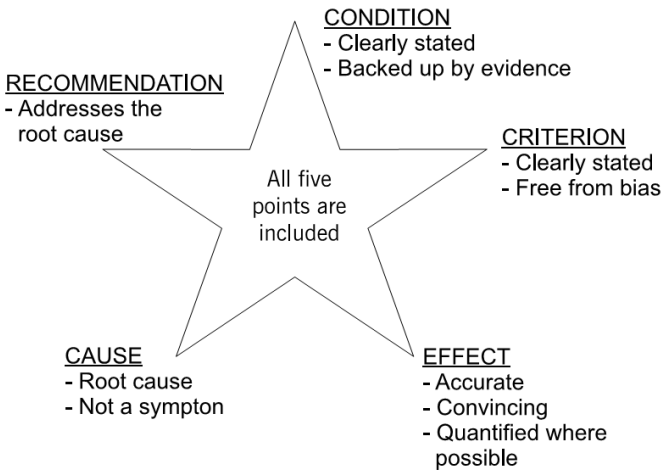
Once again revisiting our purchase order example, a suitable recommendation might be 'A policy should be put in place which requires all purchase orders to be authorised'.

The recommendation should provide management with guidance about the root cause that needs to be addressed. Management is then responsible for determining what specific actions to take to eliminate this cause.

Internal audit will then review the steps taken by management to determine if they are sufficient to resolve the problem.

6.2 Reporting

Auditors should review every recommendation in their draft report to ensure each one can be delivered in a way that management is likely to accept. This can be done by ensuring all five points have been included and that each part achieves its objective, as shown below.



Chapter 05: Analytical audit procedures

1. Analytical review

Analytical review is the term used to describe the work that internal auditors carry out on the data received during the audit engagement. Analytical review is used to help the auditor confirm that what is happening in practice is in line with what they would have expected to see.

After collecting data, auditors will need to analyse this data in order to make sense of it.

The auditor will need to make comparisons between what they would have expected to find and what was actually found during the audit engagement.

Analytical review techniques allow the auditor to do this. Analytical audit procedures may include:

- Comparison of current period and prior period information
- Comparison of current period information with budgets and forecasts
- Study of relationships of financial information with the appropriate non-financial information (for example, recorded payroll expense compared to changes in average number of employees)
- Study of relationships among elements of information (for example, fluctuations in recorded interest expense compared to changes in related debt balances)
- Comparison of information with similar information for other organisational units
- Comparison of information with similar information for the industry in which the organisation exists

This list is not exhaustive. Auditors may carry out many other analytical procedures, depending on the specific audit engagement they are carrying out.

Auditors should carry out analytical work wherever:

- An unexpected change is identified
- A change is expected, but it does not occur

In both cases the reasons for the change (or lack of it) should be determined.

2. Reasonableness tests

Reasonableness tests are used by auditors to determine if the results actually received are reasonable. Are they in line with what the auditor would expect? If they are not reasonable, then more work will need to be done to establish why. Spikes or dips in trends would also have to be investigated.

The main reasonableness tests you should have an understanding of are variance analysis, trend analysis, regression analysis, and ratio analysis.

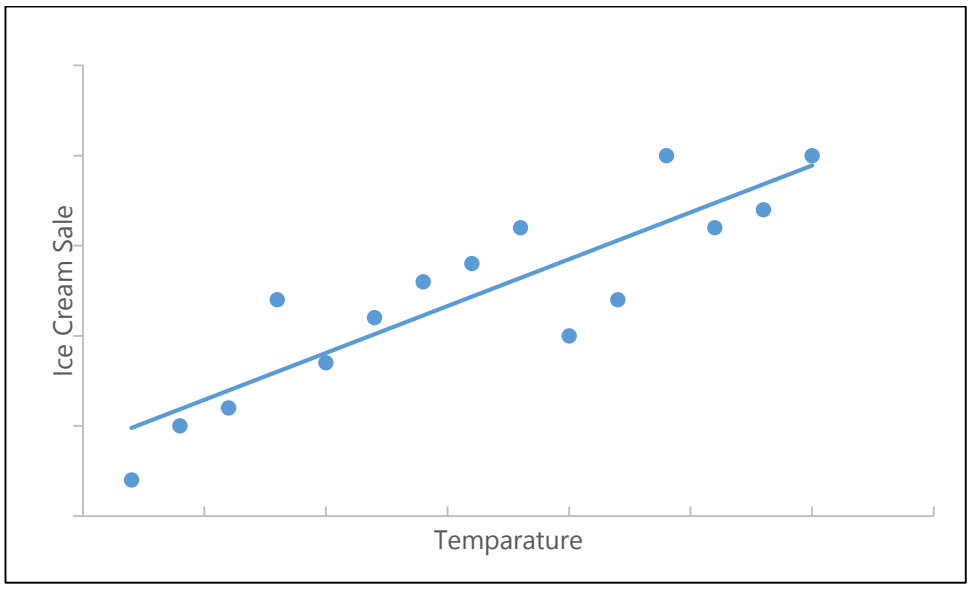
We will look at variance analysis, trend analysis and regression analysis in this section. Ratio analysis is a larger topic and will be looked at in section 3.

2.1 Variance analysis

Variance analysis means looking at the differences between expected and actual results. Reasons for the differences, or variances, would then be determined. An example of variance analysis would be in management accounting where budgets and forecasts are compared to actual expenditure.

2.2 Regression analysis

Regression analysis is a quantitative technique to check any underlying correlations between two variables (e.g. sales of ice cream and the weather). The relationship between two variables may only hold between certain values. (You would expect ice cream consumption to rise as the temperature becomes hotter, but there are probably a maximum number of ice creams an individual can consume in a day, no matter how hot it is.)

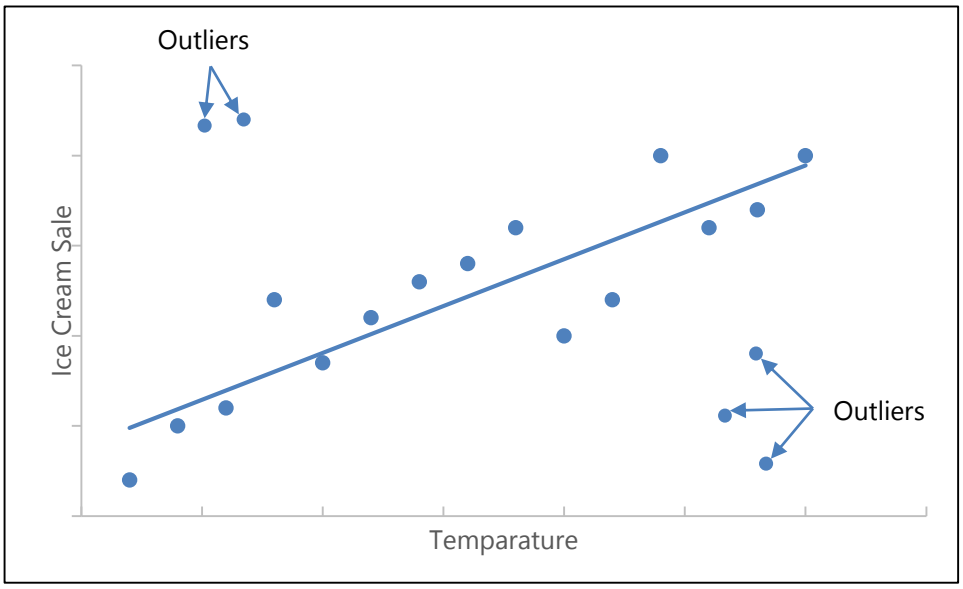


The relationship between the two variables can be plotted on a scatter diagram.

The dependent variable (ice cream sales) is plotted on the Y axis, and the independent variable (weather, measured here by temperature) is plotted on the X axis. The diagonal line highlights the pattern and shows the relationship.

Not all data will conform, however. Consider the scatter diagram below.

Although the pattern is still clear, there are a number of outliers.



The items below the line represent days where the ice cream sales are below the expected amount for a day of that temperature. An investigation for the reasons into the low sales may find that, despite being hot, it rained on those days.

The outliers above the line represent days when more sales of ice cream were made than would be expected.

Further investigation may show that the customers are workers based near the ice-cream store and these were the days when they were paid.

2.2.1 Regression analysis equation

A more accurate indication of the pattern between the two variables can be obtained using a formula for regression analysis.

$Y = a + bX$

Where Y = The dependent variable (ice cream sales)

X = The independent variable (temperature)

a = The value of Y when X is 0 (the point where the line would intersect the Y axis)

b = The increase in Y for each unit of X (the gradient of the line)

Working it through, let's assume:

a = 20 and b = 10

How many ice creams would be sold on a day where the temperature is 25 degrees?

Y = 20 + 10(25)

= 20 + 250

= 270

Auditors can use this in practice to evaluate the reasonableness of budgeted or actual results.

2.2.2 Quantifying the reliability

The above mathematical approach is very neat, but as we saw above, there are always exceptions to the rule.

This variance from the regression analysis can be accounted for by considering the value r in order to quantify the reliability of the regression.

If r = 1 there is perfect positive correlation

If r = 0 there is no correlation, it is completely random

If r = –1 there is perfect negative correlation

It is unlikely to find a relationship close to 1 or –1. This is because there are usually other factors involved. For example, ice cream sales could also be influence by rainfall and wind levels, as well as unrelated factors such as day of the week, or local events.

To look at relationships with more than one independent variable, auditors can use multiple regression analysis using a formula that contains additional b and X values:

$y = a + b_1X_1 + b_2X_2 + \ldots + b_nX_n$

2.2.3 Limitations of regression analysis

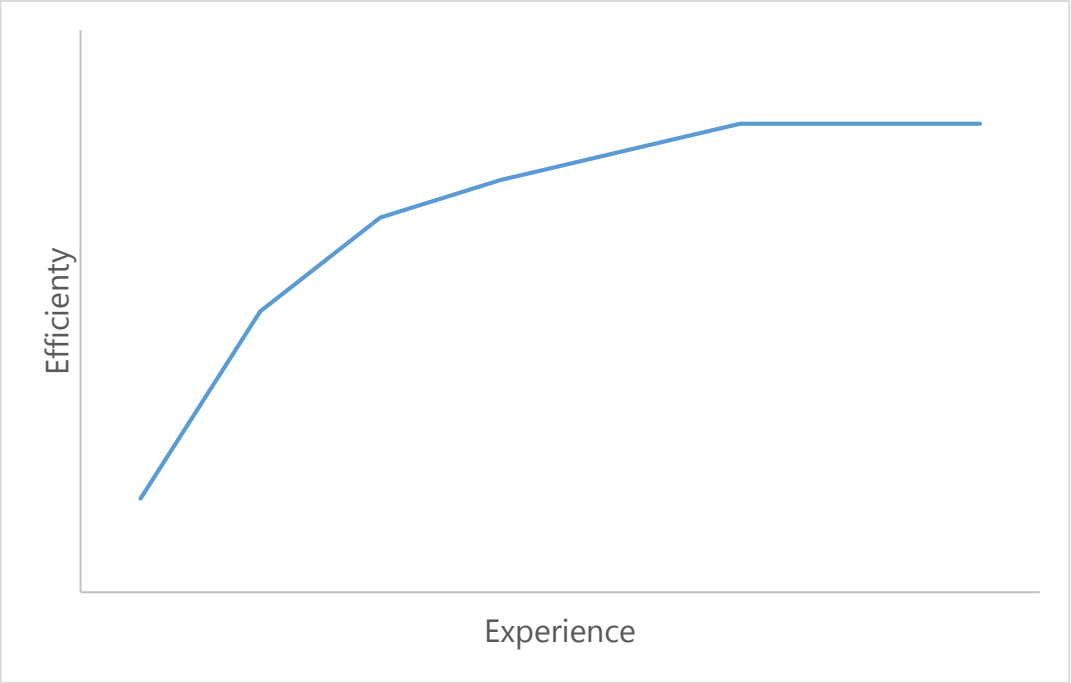
There are a number of limitations of regression analysis, including:

- Doesn't indicate that the reason for correlation
- Does not guarantee that the cause of change is in fact the independent variable. There could be other
- variables involved

2.3 Trend analysis

Trend analysis is used by internal auditors to review changes in an account, or other historical data. It is more likely to be used to look at statements of income and expenditure, rather than for balance sheets which show data at a specific time.

It can also be used for operating information. You are probably familiar with the way the learning curve effect has been used for many years as a means of estimating the future manufacturing costs of existing products. (The learning curve illustrates that as workers become more familiar with their jobs they learn to do them more efficiently. As a process is repeated, it is expected that costs will be reduced due to this increased efficiency.)



The principle can be extended to activities other than manufacturing, to the extent that the passage of time should allow any organisation to improve the cost efficiency of any of its activities and thus experience a continuing decline in real unit costs. This can be seen in the experience curve: as output increases, the cost per unit of output falls. This wider experience curve effect holds out the possibility of developing core competences through the acquisition of experience, though the probability that this will happen is low.

3. Ratio analysis

Ratios provide a means of systematically analysing financial statements. They can be grouped under the headings profitability, liquidity, gearing and shareholders' investment. It is important to calculate relevant ratios and to take into account the limitations of ratio analysis.

3.1 Uses of ratio analysis

Businesses carry out ratio analysis in order to measure the progress of the enterprise and of individual subsidiaries, so that managers know how well the company concerned is doing. Ratio analysis can be very useful to internal auditors in the same way, particularly when carrying out financial audits.

The key to obtaining meaningful information from ratio analysis is comparison: comparing ratios over time within the same business to establish whether the business is improving or declining, and comparing ratios between similar businesses to see whether the company you are analysing is better or worse than average within its own business sector.

3.2 Limitations of ratio analysis

Although ratio analysis can be a very useful technique, it is important to realize its limitations.

(a) Availability of comparable information

When making comparisons with other companies in the industry, industry averages may hide wide variations in figures. Figures for 'similar' companies may provide a better guide, but then there are problems identifying which companies are similar, and obtaining enough detailed information about them.

(b) Use of historical/out-of-date information

Comparisons with the previous history of a business may be of limited use, if the business has recently undergone, or is about to undergo, substantial changes. In addition, ratios based on published accounts suffer from the disadvantage that these accounts are filed some months after the end of the accounting period. Comparisons over time may also be distorted by inflation, leading to assets being stated at values that do not reflect replacement costs, and revenue increasing for reasons other than more sales being made.

(c) Ratios are not definitive

'Ideal levels' vary industry by industry, and even they are not definitive. Companies may be able to exist without any difficulty with ratios that are rather worse than the industry average.

(d) Need for careful interpretation

For example, if comparing two businesses' liquidity ratios, one business may have higher levels. This might appear to be 'good', but further investigation might reveal that the higher ratios are a result of higher inventory and receivable levels which are a result of poor working capital management by the business with the 'better' ratios.

(e) Manipulation

Any ratio including profit may be distorted by choice of accounting policies. For smaller companies, working capital ratios may be distorted depending on whether a big customer pays, or a large supplier is paid, before or after the year-end.

(f) Ratios lack standard form

For example, when calculating gearing some companies will include bank overdrafts, others exclude them.

3.3 Broad categories of ratios

Ratios can be grouped into the following four categories:

- Activity (revenue etc.)
- Profitability and return
- Debt and gearing (gearing is sometimes called leverage)
- Liquidity: control of cash and other working capital items

3.4 Activity ratios

As we noted above, activity ratios provide an indication of how soon inventory is convertible into cash. They are useful for measuring efficiency.

3.4.1 Accounts receivable payment period

This ratio measures roughly how long it takes for an organisation's accounts receivable to pay what they owe.

$$Accounts\ receivable\ payment\ period = \frac{Trade\ receivables}{Credit\ sales\ revenue}\ x\ 365\ days$$

3.4.2 Inventory turnover

The inventory turnover ratio indicates the number of times in a year the inventory is replaced.

$$Inventory\ turnover = \frac{Cost\ of\ Sales}{inventory}$$

The higher the ratio calculated, the more efficient the organisation.

The number of days it takes for the inventory to be turned over can be calculated by multiplying the answer calculated above by 365.

A lengthening inventory turnover period indicates:

- A slowdown in trading, or

- A build-up in inventory levels, perhaps suggesting that the investment in inventories is becoming excessive.

If the inventory days are added to the accounts receivables days, this should give us an indication of how soon inventory is convertible into cash, thereby giving an indication of the organisation's liquidity. We will look at a number of other liquidity ratios later in this chapter.

3.4.3 The accounts payable payment period

$$Accounts\ payable\ payment\ period = \frac{Average\ trade\ payables}{Credit\ purchases\ or\ cost\ of\ sales}\ x\ 365$$

The accounts payable payment period often helps to assess a company's liquidity; an increase in accounts payable days is often a sign of lack of long-term finance or poor management of current assets, resulting in the use of extended credit from suppliers, increased bank overdraft etc..

3.4.4 Asset turnover

Both the fixed assets turnover and the total assets turnover can be calculated to give an idea of how well assets are used to generate revenue.

$$Non-current\ assets\ turnover = \frac{Revenue}{Net\ fixed\ assets}$$

$$Total\ assets\ turnover = \frac{Revenue}{Total\ assets}$$

In both cases, the higher the ratio calculated, the better the organisation is at using assets to create revenue.

3.5 Profitability and return: the return on capital employed (ROCE)

A company ought of course to be profitable, and obvious checks on profitability are:

- Whether the company has made a profit or a loss on its ordinary activities
- By how much this year's profit or loss is bigger or smaller than last year's profit or loss

It is impossible to assess profits or profit growth properly without relating them to the amount of funds (the capital) employed in making the profits. An important profitability ratio is therefore return on capital employed (ROCE), which states the profit as a percentage of the amount of

capital employed. Profit is usually taken as profit on ordinary activities before interest and taxation (PBIT), and capital employed is shareholders' capital plus long-term liabilities and debt capital. This is the same as total assets less current liabilities.

The underlying principle is that we must compare like with like, and so if capital means share capital and reserves plus long-term liabilities and debt capital, profit must mean the profit earned by all this capital together. This is PBIT, since interest is the return for loan capital.

$$ROCE = \frac{(PBIT)}{Capital\ employed}$$

Capital employed = Shareholders' funds plus current liabilities plus any long-term provisions for liabilities and charges.

3.5.1 Evaluating the ROCE

What does a company's ROCE tell us? What should we be looking for? There are three comparisons that can be made.

(a) The change in ROCE from one year to the next
(b) The ROCE being earned by other companies, if this information is available
(c) A comparison of the ROCE with current market borrowing rates
    (i) What would be the cost of extra borrowing to the company if it needed more loans, and is it earning an ROCE that suggests it could make high enough profits to make such borrowing worthwhile?
    (ii) Is the company making an ROCE which suggests that it is making profitable use of its current borrowing?

3.6 Analysing profitability and return in more detail: the secondary ratios

We may analyse the ROCE, to find out why it is high or low, or better or worse than last year. There are two factors that contribute towards a return on capital employed, both related to revenue.

3.6.1 Profit margin

A company might make a high or a low profit margin on its sales. For example, a company that makes a profit of 25c per $1 of sales is making a bigger return on its revenue than another company making a profit of only 10c per $1 of sales.

The gross profit margin, operating profit margin and net profit margin can all be calculated to determine profitability.

$$Gross\ profit\ margin = \frac{Sales\ -\ cost\ of\ sales}{Sales}$$

The higher the ratio calculated, the higher the profitability. If the gross profit margin rises steadily over time, this is likely to be due to an increase in operational efficiency.

$$Operating\ profit\ margin = \frac{Operating\ profits}{Sales}$$

This ratio measures operational efficiency.

$$Net\ profit\ margin = \frac{Net\ profits}{Sales}$$

This is profitability using the profits after tax and interest as the relevant profit figure and so shows how profitable the organisation is after these have been taken into account, therefore providing a assurance that the organisation is capable of meeting its debt and tax obligations.

3.6.2 Asset turnover

Asset turnover is a measure of how well the assets of a business are being used to generate sales. For example, if two companies each have capital employed of $100,000, and company A makes sales of $400,000 a year whereas company B makes sales of only $200,000 a year, company A is making higher revenue from the same amount of assets. This will help company A to make a higher return on capital employed than company B.

Profit margin and asset turnover together explain the ROCE, and if the ROCE is the primary profitability ratio, these other two are the secondary ratios. The relationship between the three ratios is as follows.

Profit margin × Asset turnover = ROCE

$$\frac{PBIT}{Sales}\ x\ \frac{Sales}{Capital\ employed} = \frac{PBIT}{Capital\ employed}$$

It is also worth commenting on the change in turnover from one year to the next. Strong sales growth will usually indicate volume growth as well as revenue increases due to price rises, and volume growth is one sign of a prosperous company.

3.7 Other useful profitability and return ratios

3.7.1 Return on Investment (ROI)

The return on investment measures the ability of the organisation to use assets to generate profit.

ROI = Total asset turnover x net profit margin

The ROI is very dependent upon the industry in which the organisation operates.

3.7.2 Earnings per share (EPS)

EPS is widely used as a measure of a company's performance and is of particular importance in comparing results over a period of several years. A company must be able to sustain its earnings in order to pay dividends and re-invest in the business so as to achieve future growth. Investors also look for growth in the EPS from one year to the next.

$$Earnings\ per\ share = \frac{Total\ earnings}{No.of\ shares\ outstanding}$$

EPS must be seen in the context of several other matters.

(a) EPS is used for comparing the results of a company over time. Is its EPS growing? What is the rate of growth? Is the rate of growth increasing or decreasing?

(b) Is there likely to be a significant dilution of EPS in the future, perhaps due to the exercise of share options or warrants, or the conversion of convertible loan stock into equity?

(c) EPS should not be used blindly to compare the earnings of one company with another. For example, if A plc has an EPS of 12c for its 10,000,000 10c shares and B plc has an EPS of 24c for its 50,000,000 25c shares, we must take account of the numbers of shares.

(d) If EPS is to be a reliable basis for comparing results, it must be calculated consistently. The EPS of one company must be directly comparable with the EPS of others, and the EPS of a company in one year must be directly comparable with its published EPS figures for previous years. Changes in the share capital of a company during the course of a year cause problems of comparability.

Note that EPS is a figure based on past data, and it is easily manipulated by changes in accounting policies and by mergers or acquisitions.

3.8 Debt and gearing ratios

Debt ratios are concerned with how much the company owes in relation to its size and whether it is getting into heavier debt or improving its situation.

(a) When a company is heavily in debt, and seems to be getting even more heavily into debt, banks and other would-be lenders are very soon likely to refuse further borrowing and the company might well find itself in trouble.

(b) When a company is earning only a modest profit before interest and tax, and has a heavy debt burden, there will be very little profit left over for shareholders after the interest charges have been paid.

3.8.1 The debt ratio

The debt ratio is the ratio of a company's total debts to its total assets.

$$Debt\ ratio = \frac{Total\ liabilities}{Total\ assets}$$

(a) Assets consist of non-current assets at their balance sheet value, plus current assets.

(b) Debts consist of all payables, whether current or non-current.

The debt ratio measures the ability of the organisation to pay creditors, the higher the ratio, the higher the risk faced by creditors or investors.

There is no absolute rule on the maximum safe debt ratio, but as a very general guide, you might regard 50% as a safe limit to debt. In addition, if the debt ratio is over 50% and getting worse, the company's debt position will be worth looking at more carefully.

3.8.2 The debt to equity ratio

The debt to equity ratio measures the extent to which the long-term liabilities of the organisation can be covered by owners' equity.

$$Debt\ to\ equity\ ratio = \frac{Long\ term\ debt}{Total\ equity}$$

The level of debt to equity that is considered to be reasonable will vary greatly between industries.

3.8.3 Capital gearing

Capital gearing is concerned with the amount of debt in a company's long-term capital structure. Gearing ratios provide a long-term measure of liquidity.

$$Gearing\ ratio = \frac{Prior\ charge\ capital\ (long-term\ debt)}{Prior\ charge\ capital\ +\ equity\ (shareholders'\ funds)}$$

Prior charge capital is long-term loans and preferred shares (if any). It does not include loans repayable within one year and bank overdraft, unless overdraft finance is a permanent part of the business's capital.

3.8.4 Operating gearing

Operating gearing measures the proportion of fixed costs to total costs. High operating gearing means that a high proportion of cost is fixed. This has implications for business risk in that if revenue falls, there is little automatic relief in the reduction of variable costs. Operating gearing can be calculated as:

$$\frac{Contribution}{PBIT}$$

3.8.5 Interest cover

The interest cover ratio shows whether a company is earning enough profits before interest and tax to pay its interest costs comfortably, or whether its interest costs are high in relation to the size of its profits, so that a fall in profit before interest and tax (PBIT) would then have a significant effect on profits available for ordinary shareholders.

$$Interest\ cover = \frac{PBIT}{Interest\ charges}$$

An interest cover of 2 times or less would be low, and it should really exceed 3 times before the company's interest costs can be considered to be within acceptable limits. Note it is usual to exclude preference dividends from 'interest' charges.

3.8.6 Cash flow ratio

The cash flow ratio is the ratio of a company's net annual cash inflow to its total debts:

$$\frac{Net\ annual\ cash\ inflow}{Total\ debts}$$

(a) Net annual cash inflow is the amount of cash which the company has coming into the business each year from its operations. This will be shown in a company's statement of cash flows for the year.
(b) Total debts are short-term and long-term payables, together with provisions for liabilities and charges.

Obviously, a company needs to earn enough cash from operations to be able to meet its foreseeable debts and future commitments, and the cash flow ratio, and changes in the cash flow ratio from one year to the next, provides a useful indicator of a company's cash position.

3.9 Liquidity ratios: cash and working capital

A company needs liquid assets so that it can meet its debts when they fall due.

Liquidity is the amount of cash a company can obtain quickly to settle its debts (and possibly to meet other unforeseen demands for cash payments too). Liquid funds consist of:

(a) Cash
(b) Short-term investments for which there is a ready market, such as investments in shares of other companies. (Short-term investments are distinct from investments in shares in subsidiaries or associated companies.)
(c) Fixed term deposits with a bank or building society, for example six month deposits with a bank
(d) Trade receivables. (These are not cash, but ought to be expected to pay what they owe within a reasonably short time.)
(e) Bills of exchange receivable. (Like ordinary trade receivables, these represent amounts of cash due to be received soon.)

Liquidity ratios that can be used in order to determine how well the organisation is able to pay debt are the net working capital, the current ratio, and the quick ratio.

Net working capital represents the amount of money an organisation has to pay its short term debts by subtracting current liabilities from current assets.

Net working capital = current assets – current liabilities

Obviously the higher the results, the more money the organisation has available to pay its short term debts.

The current ratio is defined as:

Current assets / Current liabilities

In practice, a current ratio comfortably in excess of 1 should be expected, but what is 'comfortable' varies between different types of businesses. The larger the number calculated by this ratio, the more able the organisation to pay off short term debts.

The quick ratio, or acid test ratio, is:

'Current assets less inventory' / Current liabilities

This ratio should ideally be at least 1 for companies with a slow inventory turnover. For companies with a fast inventory turnover, a quick ratio can be less than 1 without suggesting that the company is in cash flow difficulties.

An excessively large current/quick ratio may indicate a company that is over-investing in working capital, suggesting poor management of receivables or inventories by the company.

We can calculate turnover periods for inventory, receivables and payables (receivables and payables days). If we add together the inventory days and the receivables days, this should give us an indication of how soon inventory is convertible into cash. Both receivables days and inventory days therefore give us a further indication of the company's liquidity.

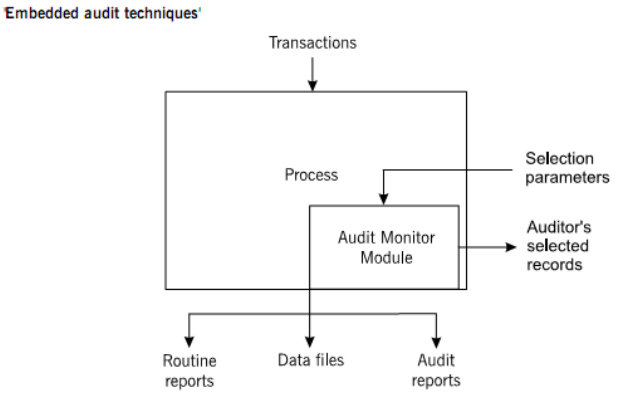
Chapter 06: Computerised audit tools and techniques

1. Embedded audit modules

Embedded audit modules sit within the system they are monitoring and check transactions as they actually occur.

Embedded audit modules are computer programmes that run alongside the software they are monitoring. They are usually used with computer systems that handle very high volumes of data and are permanently resident within the main processing system. This means it can be possible to monitor transactions as they actually occur, rather than looking for irregularities months after the event.

The embedded audit module examines transactions as they enter the system. When a transaction that meets the selection criteria occurs, transaction details are logged before the transaction is allowed to continue for further processing. The audit log file is periodically scanned, analysed and reports are produced for follow up. Embedded audit facilities usually have the ability to select



transactions that fulfil a range of criteria, which may be altered by amending the selection parameters.

1.1 Advantage of embedded audit techniques

The main advantage of using embedded audit techniques is that potential problems are highlighted as soon as they occur.

This has advantages for many people in the organisation:

Auditor	Can identify problems early on and help prevent problems escalating. Do not have to wait for physical audit and rely on sample testing to identify issues.
Management	Allows management to react quickly to any problems and prevent any serious consequences that may have otherwise occurred.
Top Management	Provides assurance that fraudulent activity will be identified. This is a key benefit for top management as under Sarbanes-Oxley legislation, they can be held personally accountable for any fraud in the financial statements and/or inadequate controls.
Wider stakeholders in organisational processes	Provides stakeholders with access to reliable, timely data.

1.2 Disadvantage of embedded audit techniques

The biggest problem with an embedded audit module is that it is difficult to add it to a system once that system is operational.

The design of the module needs to be considered carefully to ensure:

- It intercepts transactions at the most appropriate stage of processing
- The operation of the module does not degrade system performance
- The audit selection parameters and log files are protected against unauthorised alteration.

Embedded audit module requirements will need to be specified before work is started on system design, and cost justification for the added complication will also have to be provided.

2. Generalised audit software

Generalised audit software, such as IDEA, assists auditors in reviewing information that is stored digitally.

Generalised audit software (GAS) is designed to assist auditors in reviewing information that is stored digitally. It allows IT auditors to obtain evidence directly on the quality of records produced

and maintained by application systems. There is a wide range of software available for carrying out computer based audits including IDEA, ACL and SAS (Statistical Analysis System). Other data analysis programmes such as spread sheets also support computer based auditing.

GAS can be used to perform the following tasks:

Review records	GAS can access and read digital records and carry out checks on them to ensure they are complete, consistent and correct. For example, the software could review payments to suppliers and identify anomalies for further review such as • Very large payments • Several identical payments to the same supplier of the same day (possible indicator of order splitting to bypass authorisation limits) • Unusual payment patterns • Duplicate payments
Verify calculations	GAS can provide assurance that calculations have been properly computed by re-performing them. This can be useful for checking large calculations such as those used in the monthly payroll, for example.
Compare data on different files	GAS can quickly carry out large comparisons of data, such as those between current period and prior period inventory to identify slow moving items.
Selection of audit samples	Samples can be quickly chosen from large populations. This can be truly random or in line with specific criteria specified by the auditor (e.g. only pick items over a certain size).
Summarise / re-sequence data	GAS can quickly rearrange data, for example by size, date, location etc.
Compare audit data with company records	For example credit statements could be compared with accounts payable files.

2.1 Benefits/obstacles

There are a number of benefits of Generalised audit software; however, there are also a number of obstacles to adopting GAS.

GAS Benefits	Obstacles to adopting GAS
100% sampling of population so all suspect transactions can be identified. Unusual transactions can be identified no matter how large the population. Time taken to perform audit reduced. Relatively easy to use and learn. Higher level of accuracy than using manual processes. As all tasks use the same interface, it is easy to carry out new tasks using familiar processes learned for previous tasks. GAS maintains test logs of the work carried out using it. This makes the work much easier for supervisors or other auditors to review.	Possible resistance from IT staff. If staff fears that the auditing software will disrupt or block their own production systems, they may prevent it from accessing their data. Financial costs of purchasing and maintaining software as well as associated training costs.

2.2 Data extraction

Electronic auditing using audit software allows computer files, for example databases, to be searched in any number of ways for any number of items. This avoids the lengthy following of paper trails associated with more traditional methods of auditing.

Generalised audit software can be used to carry out data extraction for a wide variety of purposes. Specialized analytical software tools are also available for this purpose.

3. Spreadsheet analysis

A spreadsheet is an electronic piece of paper divided into rows and columns. The intersection of a row and a column is called a cell. A wide range of information can be stored in a cell. You are probably familiar with spreadsheets from experience in your day-to-day job.

Spreadsheets are tables made up of rows and columns that form cells where they interact. The cells may contain:

- **Text.** A text cell usually contains words. Numbers that do not represent numeric values for calculation purposes (e.g. a part number or serial number) can be added as text by entering an apostrophe before the number, e.g. '451. (Note this is the Excel instruction. Other packages may differ.)
- **Values.** A value is a number that can be used in a calculation.
- **Formulae.** A formula refers to other cells in the spreadsheet and performs some sort of computation with them. In Excel, a formula always begins with an equals sign. There are a wide range of formulae and functions available.

Spreadsheets provide a tool for calculating, analysing and manipulating numerical data. Spreadsheets make the calculation and manipulation of data quicker and easier. For example, it can be set up so that totals are calculated automatically or graphs of data can be rapidly produced to demonstrate any relationships that may exist within the data.

Spreadsheets are both useful auditing tools, and business tools that are subject to review by internal audit.

Some common applications of spreadsheets within organisations include:

- Management accounts
- Cash flow analysis and forecasting
- Reconciliations
- Revenue analysis and comparison
- Modelling business processes
- Cost analysis and comparison
- Budgets and forecasts

These are key tools for helping an organisation achieve its objectives and so are subject to review by internal audit.

Although Excel is perhaps the most well-known spreadsheet package, there are a number of alternatives. It is important that organisations select the package which best meets their requirements.

3.1 Spreadsheet risk

Spreadsheets have developed rapidly over the years and they are now a key business tool. Given the important role they play within organisations, and the extent of reliance placed on them, it is crucial that the information held within them is correct, compete and reliable.

Spreadsheet risk is the risk that the information is wrong. It is the risk of errors occurring within the spreadsheet.

Modern spreadsheets used by organisations contain extremely large volumes of data. In addition, this data is often held over a long period of time; the same spreadsheet can be used and updated by an organisation for many years. As data is added to this spreadsheet many figures will be updated as calculations are automatically carried out by the equations and formulae within the spreadsheet. The longer this goes on, the greater the likelihood of errors becomes. One small typo could lead to numerous errors as figures are updated based on this.

As future data is added, such errors are then compounded and the entire spreadsheet can become corrupt making the data outputs meaningless. This is of particular concern where a number of different users all update the same spreadsheet.

Due to the key data stored in spreadsheets, they are often the focus of compliance audits, particularly following Sarbanes-Oxley. Internal auditors should monitor the accuracy of spreadsheets and help the organisation use spreadsheets appropriately, perhaps through the facilitation of training.

The immense size of spreadsheets used by organisations makes manually safeguarding against spreadsheet risks very difficult. Each one may contain hundreds of rows and columns and hundreds of thousands of cells. The scope for error, or even fraud, in such large spreadsheets is great.

Spreadsheets do have some controls against error build in, for example Excel flags illogical formulae.

However, the range of possible options in spreadsheets makes it impossible for the built-in controls to identify all possible errors and exceptions. Human error, such as the transposition of numbers, is impossible to protect against and can be very difficult to identify.

4. Automated workpapers

Automated workpapers are electronic documents created in software templates and stored on servers or mainframes. These documents are transmitted to different computers through electronic networks.

There are several automated workpaper software packages available including Lotus notes, and Auditor assistant.

Specialized software may not always be necessary however. Some organisations have very successfully set up their own electronic workpapers using a combination of Word, Excel, flowcharting software and a scanner.

4.1 Advantages of automated workpapers

There are many advantages of using automated workpapers, including:

Cost savings. Reduces the costs associated with paper, printing, document storage and maintenance of storage space

Convenience. Quicker and easier to transfer documents electronically rather than physically

Efficient communication. It is easy to transmit electronic data simultaneously to multiple recipients

Document links. Linked documents make it easy to move from an assertion to the backing documentation or evidence quickly and easily with a single click, rather than rummaging through documents.

Consistency. Automated workpapers use templates, therefore consistency of the audit file and adherence to quality standards can be easier to achieve. This also means that information is easier to record/store by the auditor and easier to locate by the reviewer, or the auditor at a later date.

Multimedia. Graphs, charts, diagrams, photos, videos and scanned items can be easily incorporated into the workpapers.

Security. Electronic files can be backed up to multiple servers in different locations and files can be protected by password. Web files can be protected by being set as read only files. This ensures

the documents are protected from theft, and from accidental or malicious changes being made by unauthorised personnel. The very fact they are electronic rather than physical also means that they are easier to protect from physical damage that could be caused by fire, flooding or other environmental damage.

4.2 Obstacles related to automated workpapers

As with anything, as well as advantages, there are a number of drawbacks associated with setting up automated workpapers.

Training. Automated workpapers will mean a fundamental shift in working processes, therefore training will be vital. This training will have to be planned, scheduled and budgeted for. If training is not provided by the vendor, it is advisable to bring in a training professional.

Transition process. The difficulty of the transition process will depend on the paper format currently used by the auditors. If current procedures are not standard, then standard templates will have to be created as part of the process of setting up the automated system. It may also be necessary to customize the software to match the needs of the organisation.

File deterioration and obsolescence. Files stored in CD and DVD format are more vulnerable to deterioration over time than paper. Also, as software goes through upgrades, or becomes obsolete, recovering the files can become difficult.

Chapter 07: Risk and control self-assessment

1. Risk and control self-assessment

Control self-assessment is an efficient way for auditors to assess and evaluate control procedures. It uses self-assessment surveys and facilitated workshops and aims to integrate business objectives and risks with control processes.

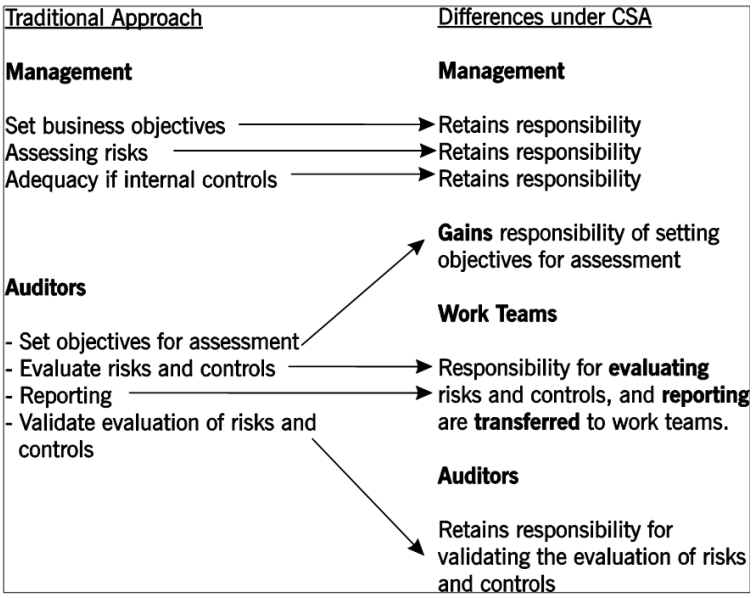
Control self-assessment (CSA) uses self-assessment surveys and facilitated workshops to assess and evaluate control procedures.

It allows managers and internal auditors to collaborate in the assessment and evaluation of control procedures.

Organisations that use CSA have a formal documented process to allow management and work teams to

- Identify risks and exposures
- Assess the control process that mitigate/manage those risks
- Develop action plans to reduce risks to acceptable levels
- Determine the likelihood of achieving the business objectives

CSA differs from traditional methods of auditing by shifting some of the responsibilities away from the auditors towards others such as work teams set up within the organisation. The diagram below illustrates how the responsibilities change when a CSA approach is used.



Control self-assessment is also referred to as control/risk self-assessment, or CRSA.

2. Approaches to CSA

There are three main approaches to CSA: Facilitated team workshops; questionnaires, and management produced analyses.

2.1 Facilitated team workshops

Facilitated team workshops attempt to gather information from work teams representing different levels of the business unit. They are facilitated by either the client or an internal auditor.

Objective based workshops	Attempt to identify the best way to meet a business objective The workshop will involve looking at the controls in place and identifying any risks not covered by these controls The aim of this type of workshop is to ensure the controls are working effectively
Risk based workshops	Identify the risks of achieving an objective Teams identify the risks of success and determine if sufficient controls are in place to mitigate them

Control based workshops	Consider how well current controls work. The controls and risks are documented by the facilitator (rather than identified as part of the workshop) and the goal is to evaluate how well the team thinks they are working
Process based workshops	Look in detail at selected activities involved in a specific process, such as the steps of a payroll process The aim is to analyse, revise, or verify the effectiveness of the process

2.2 Questionnaire approach

Questionnaires, or surveys, are a fast, cost effective method of gathering information in a yes/no format. They are most appropriate where the people questioned are based in numerous locations or where feedback is required from a large volume of people.

Surveys may also be used by internal auditors to gather preliminary information on risks and controls for discussion in the workshop.

Questionnaires should be written using language that will be understood by the recipient using words that have a clear meaning to them. (Note: this doesn't necessarily mean simple language. Complex terms and jargon may be appropriate if they form an essential part of the role of the recipients.)

Questionnaires should be short and simple, and ask the easiest questions first. If possible, a question should not cover more than one topic.

Questionnaires can also be very useful tools for conversation in an interview.

2.3 Management produced analyses

Most other processes used by management groups to produce information about processes, risk and control can be described as management produced analyses. Such analysis is usually prepared by a team or individual on behalf of management.

Internal auditors may use this information, or elements of it, alongside other information in order to improve their knowledge of organisational controls. This may then feed into the organisation's self-assessment.

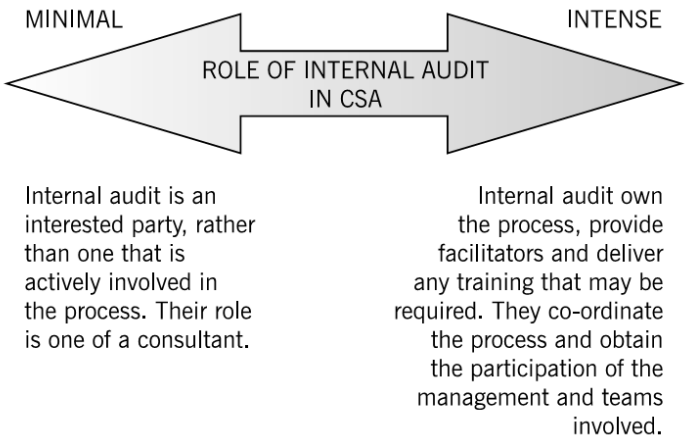
An example of a situation where a management produced analysis could be used would be following the occurrence of a significant fraud in the organisation. Management would investigate as to how the fraud had come about and what problems existed in the controls to allow the fraud to occur. The outcome of the investigation would be a management produced report documenting the reasons it occurred and measures taken to prevent it happening again.

A second example of a management produced analysis could be a review of the internal control implications of implementing a new system.

Management produced analyses are used less frequently than workshops or questionnaires as a CSA approach.

3. The role of internal audit

The role of internal audit in control self-assessment can vary hugely from intense down to minimal involvement.



The involvement of Internal audit usually lies somewhere between the two extremes. As the level of involvement increases, the HIA should monitor the objectivity of the internal audit staff and take any necessary steps to manage that objectivity.

4. Outcomes of CSA

A number of outcomes can arise from control self-assessment programmes, not all of these will be positive.

Positive outcomes of CSA	Negative outcomes of CSA

Business unit staff develops an understanding of risk assessment and control processes. This increases their ability to meet business objectives. Informal controls are more easily identified and evaluated by operational staff. Encourages staff to take ownership of the control process and so effective and timely remedial action is more likely to be taken. The organisation's objectives-risk-control infrastructure is subject to greater monitoring and continuous improvement By acting as facilitators and providing training on risks and control internal auditors become more involved in and knowledgeable about the self-assessment process. The internal audit activity gains more information about the organisation's control processes allowing them to allocate their resources to high risk areas or those with significant control weaknesses. Highlights management's responsibility for the risk management and control processes of the organisation. This prevents them trying to deflect these responsibilities to others, e.g. auditors.	Provides more information than analysis. Follow-up workshops to review the results and plan for improvements may be overlooked. May raise expectations that are not (or cannot be) acted on by senior management. Some participants may feel angry or humiliated if facilitators are not sufficiently sensitive. A sense of ownership in participants may not be achieved if written surveys are not followed up face-to-face. Failing to sufficiently involve workshop participants. Starting the CSA process without proper preparation (background reading, training facilitators etc..) will inevitably cause the process to be unsuccessful.

Chapter 08: Financial audit engagements

1. Financial audits

Both internal and external auditors carry out financial audits. However, the work they carry out, their responsibilities and their objectives are very different. Internal auditors carry out financial audits that focus on the organisation's internal controls, whereas external auditors focus on the organisation's financial statements.

Financial audits carried out by internal auditors focus on the internal controls of the organisations. The need for auditors to carry out audits such as these has been greatly increased in light of the Sarbanes-Oxley legislation.

1.1 Responsibilities relating to the financial statements

Financial audits are carried out by both external and internal auditors, although their objectives and focus are very different. The below table sets out the respective roles of senior management, external auditors and internal auditors in relation to the organisation's financial statements:

Senior Management	External Auditors	Internal Auditors
Owner of the control environment and financial information (including notes in the financial statements and accompanying disclosures)	Provide assurance to the users of financial statements that the information reported fairly presents the financial condition and result of operations of the organisation in accordance with IFRS.	Provide assurance to senior management and the audit (or other) committee of the governing board, that controls surrounding the processes that support the development of the financial report are effective.

Although both external auditor and internal auditors carry out financial audits of an organisation, their purpose and responsibilities differ greatly. The difference between external and internal auditors is illustrated below.

	Internal audit	External audit
Objective	Designed to add value and improve an organisation's operations.	An exercise to enable auditors to express an opinion on the financial statements.
Reporting	Reports to the board of directors, or other people charged with governance, such as the audit committee. Reports are private and for the directors and management of the company.	Reports to the shareholders or members of a company on the truth and fairness of the accounts. Audit report is publicly available to the shareholders and other interested parties.
Scope	Work relates to the operations of the organisation and focuses on controls.	Work relates to the financial statements.
Relationship	Often employees of the organisation, although sometimes the function is outsourced.	Independent of the company and its management. Usually appointed by the shareholders.
Planning and collection of evidence	Strategic long term planning carried out, to achieve objective of assignments, with no materiality level being set. Some audits may be procedural, rather than risk-based. Evidence mainly from interviewing staff and inspecting documents (i.e. not external).	Planning carried out to achieve objective regarding truth and fairness of financial statements. Materiality level set during planning (may be amended during course of audit). External audit work is risk-based. Evidence collected using a variety of procedures per Statements on Auditing Standards (SASs) to obtain sufficient appropriate audit evidence.

2. The role of internal auditors

As the CEO and other top executives are now personally responsible for the content of the organisation's financial statements and the underlying controls, their need for reassurance that suitable and sufficient controls are in place has increased. Internal auditors have an important role in providing this assurance.

Under Sarbanes-Oxley legislation, and the related SEC rules, the CEO and CFO (or other top executives) are personally responsible for:

- The accuracy and completeness of the financial statements; and
- The controls that provide the assurance for them to be comfortable certifying the financial reports and controls

The legislation requires them, for every quarterly and annual report, to certify that:

- They have reviewed the report and believe its assertions are true, complete and not misleading
- That they are responsible for setting up and maintaining disclosure controls and procedures
- That they have collectively disclosed any deficiencies in the controls and any fraud involving managers or other significant employees
- Whether or not there might have been any significant changes affecting the internal controls after the date of their most recent evaluation

They will therefore need to be reassured that the relevant controls are in place to feel comfortable in making these certifications.

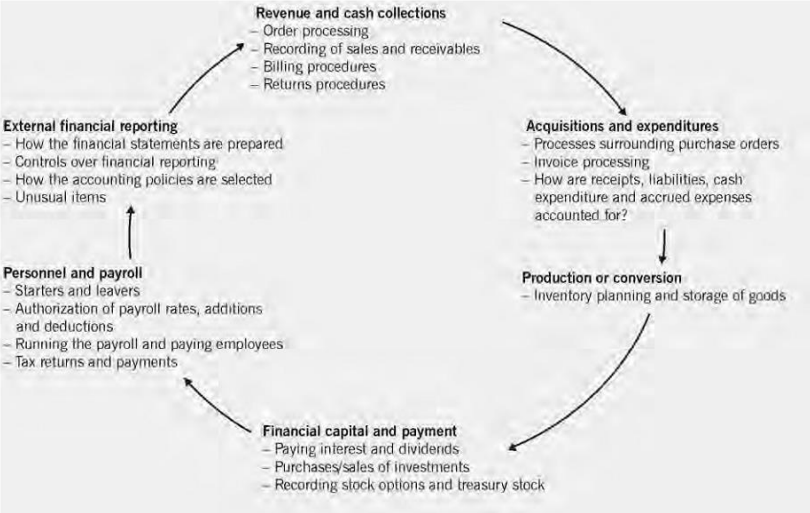
Internal auditors have a crucial role in providing them with this assurance. They can do this by carrying out internal audits that focus on the financial controls that underlie the quarterly reporting process. They should then recommend improvements to the policies, procedures and processes of reporting.

2.1 The financial audit engagement cycle

The importance of controls covered by financial audit engagements mean that it is necessary to review these areas regularly to ensure the relevant controls continue to be in place. Many internal

audit functions with therefore adopt a cycle approach to financial audit engagements to ensure each area is reviewed on a regular basis.

The below diagram shows a cycle that could be followed along with some examples of areas that may be considered as part of the reviews of those areas.



When determining the work to be carried out in each specific areas, the auditor has to take into account the level of audit risk and the perceived level of materiality.

1.1.1 Audit risk

> ***ISQIA 6000 Risk and governance***
>
> Internal audit activity must consider evaluating the organisational risk management policies and procedures in order to recommend suitable improvement.

Audit risk is the risk that the auditor may unknowingly fail to modify the opinion on the materially misstated financial statements, i.e. it is the risk they give the wrong opinion.

Audit risk = Inherent risk + Control risk + Detection Risk

Inherent risk is the susceptibility of an assertion to a misstatement and that could be material individually or when aggregated with other misstatements.

Control risk is the risk that a misstatement that could occur in an assertion and that could be material, individually or when aggregated with other misstatements, will not be prevented or detected and corrected on a timely basis by the entity's internal controls.

Detection risk is the risk that the auditor's procedures will not detect a misstatement that exists in an assertion that could be material, individually or when aggregated with other misstatements.

Although the concept of audit risk is generally an external audit term, it is equally relevant to internal auditors.

If the level of audit risk is high, the external auditors are at risk of inappropriately signing off the reports. In order to help prevent this, the internal auditors will need to increase the amount of work they do in this area. This will help to ensure that any irregularities are identified and to ensure that strong controls operate in this area. This will help to reduce the level of audit risk the external auditors will face when they carry out their statutory review of the financial statements.

2.1.2 Materiality

Materiality relates to what the auditor considers to be important in the context of the whole financial statements. Materiality is a concept relating to the significance or importance of an amount, transaction or discrepancy.

If the item is large, significant, has a noticeable impact or is in some other way significant then it is said to be material.

Auditors are only interested in those items considered to be material.

The concepts of audit risk and materiality are important at the following stages of the audit:

- Planning the audit
- Designing audit procedures
- Evaluating whether the financial statements are presented fairly in all material respects.

2.2 Carrying out the financial audit engagement

When reviewing any transactions that will have an impact on the financial statements of the organisation, the internal auditor will usually be interested in gaining assurance over the following.

Occurrence: The transactions that have been recorded did actually occur and relate to the entity under review

Completeness: All items that should have been recorded were recorded

Accuracy: The items have been recorded correctly

Cut off: Items were recorded in the correct period

Classification: Items were recorded in the proper accounts.

To help you see how this might work in practice, imagine you are carrying out a review of Payroll, and you are looking specifically at the payment of employees. How might you going about reviewing this?

The framework above tells us that we will want to confirm the following:

- The payments recorded were all actual payments made to genuine employees; no payments are made to ghost employees (occurrence)
- No payments were made but not recorded (completeness)
- The employees have been paid the correct amount and the payments recorded are in line with those
- actually made (accuracy)
- The amount paid to employees in June is recorded in the June accounts (cut off)
- Payments made to permanent employees working in the Security division are correctly charged to the Security accounts as payments to permanent employees. They are not recorded as payments to temporary staff, for example, nor are they charged to a different department (classification)

3. Internal control

ISQIA 4300 Control Activities

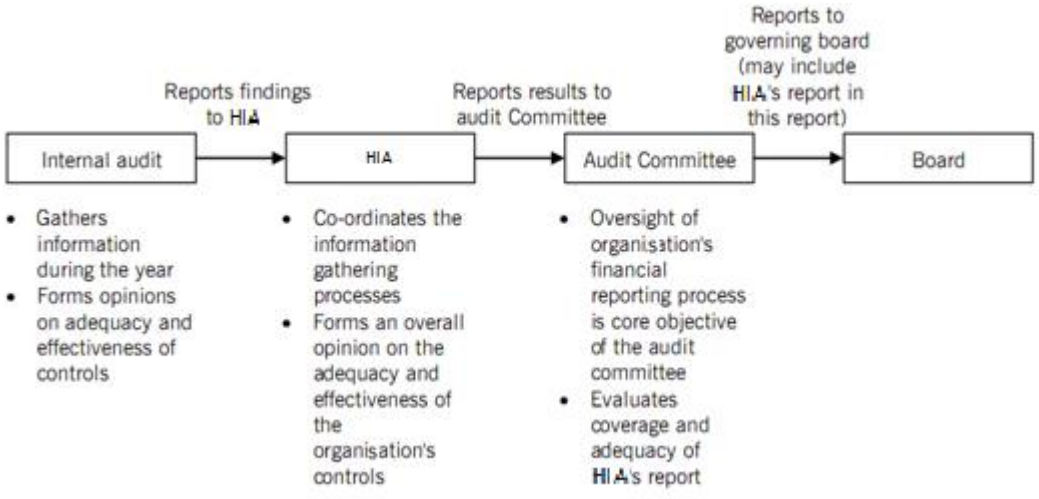
Controls within organisation must be evaluated in terms of effectiveness and efficiency and appropriate recommendations for scope of improvement must be identified and communicated on timely basis to senior management and the board.

Internal auditors must report their opinion on the adequacy and effectiveness of internal controls to the audit committee and the board.

3.1 Reporting internal control

Internal auditors form an opinion on the effectiveness and adequacy of the organisation's internal controls based on the information they have collated throughout the year. This opinion has to be reported to the audit committee as a key objective of the audit committee is oversight of the organisation's financial processes to ensure their reliability and fairness.

The HIA will therefore report the overall evaluation of the systems to the audit committee who will evaluate the coverage and adequacy of the HIA's report and possibly include it in their own report to the governing board.



3.2 Framework for internal control

The recommended framework for internal control is the Committee of Sponsoring Organizations' (COSO)'s Internal Control – Integrated Framework.

COSO's framework states that

- The definition of internal controls should not be limited to accounting controls or financial reporting. It should be a broad definition
- Other aspects of the business, such as resource protection, operational efficiency and effectiveness and compliance with rules, regulations and organisational policies also have an impact on financial reporting
- Internal control is the responsibility of management and requires participation from all persons within an organisation in order to be effective
- The control framework is linked to the business objectives and is flexible enough to be adaptable.

3.3 Effectiveness of internal control

We began this section on internal control by looking at the how the internal audit activity's assessment of internal controls is reported from the HIA to the audit committee and eventually the governing board.

The board has to rely on the management of the organisation to maintain effective controls. They therefore need to ensure

- An effective risk management process is in place. Risk should be managed throughout the organisation and any major risks should be discussed with the board.
- There is a strong ethical environment and culture. This should flow right through the organisation from the board and senior management down. It should be backed up by training, strong communication and a zero tolerance approach to fraud.
- The control system is effective. There are suitable controls in place, the controls work, and senior and line management have accepted responsibility for those controls. Any problems are quickly and competently rectified.
- Strong monitoring is in place. Senior management and the audit committee are in support of internal audit, the board is independent and there are open lines of communication between internal and external audit, all members of senior management and the audit committee. Control processes are monitored by management.

Even the most effective internal controls cannot protect against everything that may go wrong. This includes the intentional override of controls by dishonest management. Other problems might include poor decision making, incompetent managers or environmental factors.

1.4 Role of internal audit

ISQIA 5000 Gathering and analysing data

Internal audit activity should be set on priority basis which is responsibility of the head of internal auditor. Audit programmes are based on types and levels of risk associated with internal audit engagements, types of organisation and objectives of organisational goals. (See also Appendix)

Internal auditors have two roles in the assessment of internal controls.

1. The HIA must determine if the audit plans for the year and the risk assessment of internal audit are sufficient to ensure success. This will involve ensuring adequate resources are available.

2. The HIA must also allocate the necessary resources to carry out the audit and then ensure suitable procedures are followed to be able to provide senior management and the board reasonable assurance that the controls surrounding processes are sufficient.

The HIA should consider financial reporting, corporate governance, and corporate risk control processes as part of the resource allocation process.

Internal audit engagements begin with identifying potential exposures to risks. The work plan is then based on these risks to determine what controls and procedures have been put in place by management to mitigate those risks. A significant proportion of internal audit work therefore directly relates to internal controls.

Chapter 09: Security and privacy audit engagements

1. Physical security

Management are responsible for establishing appropriate controls over the organisation's assets. These controls should ensure that the assets are physically secure. In the case of buildings and premises, this could be something as simple as ensuring there are suitable access controls, such as locks on the windows and doors.

Physical security controls include those relating to:

- Physical access
- Environmental risks
- Fire and flood protection

1.1 Site design and access

Physical security can be enhanced through careful site design. The following factors should be considered.

Location

Data centres, or facilities at risk to vandalism (e.g. drug development testing units which may be targeted by animal rights activists), should be located in an inconspicuous location.

Access

Access to buildings (and restricted areas within them) should be carefully controlled and monitored. We will see shortly some methods that can be used to control access.

The number of entry points should be kept to a minimum.

Emergency exits should be alarmed and locked from the outside (but not from the inside!)

Surveillance

Sensitive areas should be monitored with CCTV. Out of hours access should be monitored using motion detectors.

Fire and environmental damage safeguards

Wiring should be encased wherever possible, keeping exposed wiring down to a minimum.

Fireproof cabinets/vaults should be used to store documents and electronic media.

Risk of environmental damage can be minimized by ensuring temperature and humidity levels are carefully controlled.

1.1.1 Restricted areas

Access to buildings, areas within the building, or other secure areas can be restricted using a number of measures such as those illustrated in the table below.

Magnetic access cards	Cards with a magnetic strip similar to those used on credit cards are swiped in order to gain access to the building. Each card can be customized to the individual user to ensure they can only get access to the areas of the building that they are authorised to use. Date and time restrictions can also be placed on the cards.
Numerical keypad code entry systems	Access is gained through entering a code made up of a series of numbers. These cannot be customized to the user in the same way magnetic strips are, and anyone with the code can gain access to the building. They are also riskier as individuals may tell others the code. These are appropriate for low-risk areas used by many individuals.
Biometric access systems	Retina scan or fingerprint recognition technology is used to identify physical characteristics. Such systems are not 100% accurate and the error rate will have to be considered before determining if this is an acceptable device for the organisation. These are appropriate for areas to which only a small number of individuals can gain entry.

1.2 Specific risks

There are a number of areas where specific controls should be put in place to prevent damage to the organisation's buildings and information. This includes safeguards against fires and loss of power supply. The below illustrates these risks and the safeguards that the organisation should put in place to mitigate these risks.

Threat	Risks	Safeguards and controls
Fire	Loss of lives, buildings and information	**Smoke detectors and fire alarms** should be installed throughout the organisation **Fire extinguishers** of various types should be available throughout the organisation Selected staff members should be appointed as **fire marshals** and provided with the relevant training **Fire drills** should be carried out at regular intervals All of the above controls should be monitored and tested regularly
Loss of power	Loss of data and information Security failure (where controlled by electronic methods)	Organisations can choose to safeguard against this threat in one of two ways **Short term solution** **Uninterruptible power supply (UPS)** systems and surge protectors allow computers and other electronic systems to shut down correctly in the event of a blackout. This protects the systems from the loss of data, but does not allow them to continue to operate for long. **Long term solution** **Generators** provide power for longer periods of time. However they are more expensive to install and maintain than the short term solutions listed above. Generators are used for large systems and critical applications.

Of course these are not the only threats over the continued operation of the business and any number of things can happen that have a direct impact on day to day operations.

These could include unexpected failures which could occur in any organisation, such as a burst water pipe, or specific threats relating to the organisation in question. For example, an organisation which carries out tests using animals as part of its research may be at risk of attack by animal rights protectors and activists. A bomb threat in such an organisation, for example, could have a severe impact on the organisation's operations. Security in organisations such as this will be of high priority.

Wherever possible these threats should be controlled through appropriate processes and procedures. These should help to prevent against the threats occurring and reduce the extent of damage suffered if they do arise.

1.2.1 Systems controls

Equipment breakdowns and inaccurate processing can have a major impact on the operations of an organisation.

It is therefore vital that controls are put in place to reduce the instances of these. Such controls might include:

- A written log of all preventative measures in place should be produced
- Documented procedures should be put in place which detail what should be done in the event of equipment failure. These procedures should be provided to all relevant staff and supporting training provided where necessary
- Incident logs within the system should inform IS management of the number and scale of errors occurring on each shift
- Preventative maintenance programmes, as per the manufacturer's recommendations, should be installed to provide periodic maintenance to the systems

1.3 Role of the internal auditor

The internal auditor should review the controls over physical security to ensure that sufficient appropriate controls are in place. Tests they may carry out to check this include:

Access

Review the access security measures that are in place and make a judgment over whether or not they are sufficient:

- Are all entrances covered?
- Is access given to all suitable staff?
- How is unauthorised access prevented?
- How regularly are access codes changed?
- Are there any restricted access areas that require additional controls etc.?

Fire precautions

Make sure there are suitable controls and procedures in place for the event of a fire.

- Are there sufficient fire escapes? Are they alarmed? Are they well signed? Make sure they have not been padlocked shut.
- What procedures for evacuation are in place? Have these procedures been communicated to staff? Is all staff aware of the procedures? How regularly are they tested?
- Are there sufficient fire alarms and smoke detectors? How regularly are they tested? What happens if they fail a test (i.e. how quickly would they be brought back to being operational?)
- Where are the fire extinguishers (or other fire suppression devices) located? Who is authorised to use them? What training have they received and are they up to date with this? How are they tested? How can we be sure they are working properly?
- Review document and electronic media storage. How vulnerable is it to fire/flood damage? What backup procedures exist? Where are backups held?

Systems

- Hold interviews with staff to find out how equipment works and what would happen if something failed.
- Find out what recovery processes are in place and determine if they are adequate. How are these processes tested? Who is included? Are they aware of their responsibilities?
- Determine the expected level of downtime and compare this to the amount of downtime actually experienced.
- Review system failure logs to determine how much time is lost to malfunction.
- Cross check error logs to maintenance logs.
- Review maintenance cycle to determine if sufficient. Is the timing appropriate?

Environment

Determine what controls over humidity and temperature are in place. How are they maintained? Are they working correctly?

There may also be many more tests you can carry out depending on the specific engagement and the organisation concerned.

The auditor must carry out observation and testing to make sure the processes are actually being followed. The documented processes may be in place, but the control fails if it is not followed in practice.

2. Data security

A second aspect of security is data security. It is important that the data and information of an organisation are protected in order to guard against access by unauthorised personnel who could damage the data, either intentionally or maliciously, or leak confidential information outside the organisation.

2.1 Access to data

Management is responsible for establishing appropriate and effective controls to protect data to make sure:

- The data can only be accessed by authorised users
- The level of access given to an individual is linked to their business needs
- All changes to the data are recorded in an audit
- Attempts to access the system by unauthorised users will be logged and the user will be denied access

The most common method organisations use to protect their data is with passwords, however, there are a number of inherent problems with passwords

- People write them down. This problem is becoming increasingly significant as modern life requires individuals to remember so many different passwords to access so many different things. Measures in place to strengthen passwords (see below) such as regular changes or complex formats compound this problem further.
- They are easy to guess. They are often nicknames, a sports team, or sometimes simply 'password'

Password access systems can be enhanced where the following measures are in place

- Periodic enforced change of password, for example every 90 or 180 days
- Will not allow change of password to be to a recently used password
- Requires certain characters, e.g. mix of upper and lower case letters, numbers, and special characters (such as # or $)
- Prevents the use of words recognizable as the user's name, obvious words like 'password', or combinations attempting to get around this rule, such as 'P@$$w0rd'
- Suspends user account after a certain number of failed login attempts
- Additional passwords required for restricted information. For example, one password is needed to access the HR system but the salary screens within it can only be accessed by providing a second set of log in details

2.2 Responsibilities of internal audit

It is the responsibility of management (not auditors) to make sure risks are assessed and suitable policies and controls are in place and abided by.

Internal auditors, however, also play a vital role in relation to data security through the following responsibilities:

- To keep up to date with systems in the organisation and be aware of any new systems set up. They should ensure they have received the relevant training on all systems
- To be able to recommend changes to the system or control, such as a different security system, or improved levels or methods of training for the users
- To continuously monitor data security controls, such as password administration, violations etc..

2.3 Data storage issues

Data should be carefully backed up, and where possible copies should be held in different locations (ideally off-site) to ensure that nothing is lost. A careful cataloguing and labelling system should also be used to ensure the data is not lost or mistakenly updated.

Auditors should ensure the data storage controls of the organisation are sufficient to manage these risks by:

- Reviewing the labelling system. Is it logical? Are files are named appropriately to prevent accidental use of incorrect files? Are the naming conventions sensible?
- Determining the availability of data files. Who has access to this data?

- Ensuring data is sufficiently backed up and could be recovered if necessary. Where is the data stored?
- Where are backups held? Is this sufficient?
- Assessing temperature and humidity controls to ensure data is not accidentally damaged.
- Identify the extent of damaged data due to inadequate drive space.

2.4 Business continuity planning

Business continuity planning (BCP) means developing a plan for how you would stay in business should a disaster occur, and how you would recover from that disaster.

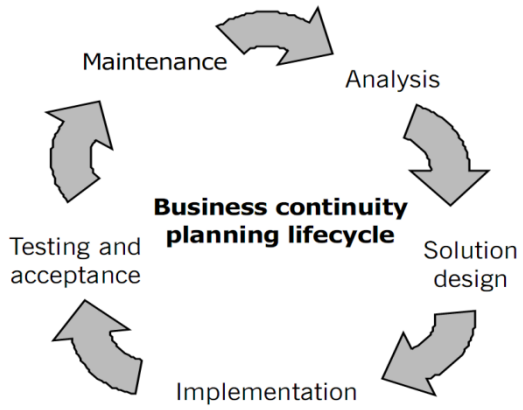
The aim is to develop a plan which allows the business to be in operation again as soon as possible with the minimum disruption.

Disaster, in the context of BCP, relates to a critical problem which prevents the organisation carrying out its normal operations, for example a major systems failure.

The aim of BCP is to mitigate the business risks encountered as a result of a mission-critical functional failure.

Development of the BCP should be an on-going process as illustrated by the diagram below.

The BCP itself should consist of a series of actions and processes to be followed should a disaster occur. They should flow sequentially and clearly identify responsibilities for carrying out each action.



In addition to a documented BCP plan for continued operation in the event of a disaster, for business continuity planning to have the best chance of success, the organisation should also have an off-site data-storage facility and agreements with alternate sites to which operations could be moved in the event of a disaster.

2.4.1 Role of internal audit in BCP

Internal audit need to assess how well the organisation is prepared for disaster and must decide whether or not they think the business would recover and how quickly it would do so. To form an opinion, the auditor needs to know:

- If the organisation can function if system access is disrupted
- How severe the impact of this would be
- What disaster plans are in place
    - Does the plan cover all eventualities?
    - Has it been documented and provided to relevant staff?
    - Have relevant staff been trained and made aware of their responsibilities?
    - Has it been tested?
    - Is it up to date?
    - Are the back-up facilities referred to in the plan ready to go should they be needed?

The internal auditor can use this information to identify any flaws in the process and make helpful recommendations for improvement.

3. Privacy audit engagements

Breach of privacy can have serious repercussions for an organisation, such as legal problems, reputation damage and loss of customer trust. It is therefore vital that management establishes suitable controls to ensure privacy is protected.

Privacy, however, is not a simple thing to define as it can mean many different things to different people. It can vary depending on culture, country, legal framework and political environment.

Generally, privacy can encompass:

- personal privacy (physical and psychological)
- privacy of space (not being under surveillance)
- privacy of communication (not being monitored)
- privacy of information (collection, use and disclosure of information by others).

Personal information is any information that can be linked back to a specific individual, either alone or by its combination with other information.

Personal information does not have to be recorded to be classified as personal information. If it is recorded it can be in any form of media – all would still not change the fact that it is personal information. This information can also be factual or subjective.

Examples of personal information include an individual's name, address, bank account details, employee records, social status, records of disciplinaries and salary information, as well as many other records and information.

3.1 Privacy laws

In order to carry out a successful audit of privacy, the auditor must be aware of, and have an up-to-date understanding of privacy laws. The relevant legislation will differ depending on the country in which the audit is carried out. Examples of relevant legislation include:

- The Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Council of Europe)
- The Canadian Personal Information Protection and Electronic Documents Act
- The Health Insurance Portability and Accountability Act of 1996
- The Data Protection Act 1998 (UK)

Internal auditors must identify which laws are relevant, the exact nature of those laws and their impact on the organisation. Any risks the organisation is exposed to as a result of these laws and regulations should be defined. In-house or external experts can be used to help them achieve this.

Auditors should be aware that their independence may be impaired if they assume any responsibility for developing and implementing a privacy programme. If they have any concerns over this, they should discuss the matter with the HIA.

3.2 Expectations of the auditor

When carrying out a privacy audit, an internal auditor typically can be expected to:

- Identify the types and appropriateness of personal or private information gathered by the organisation
- Identify the collection methodology used
- Determine what the organisation will use the information for and ensure this is consistent with its intended use and any laws it may be subject to Internal auditors must ensure they have the relevant legal and technical knowledge and capacity to allow them to do this, and use third party experts if necessary.

Chapter 10: IT engagements

1. IT audits

Internal auditors should evaluate the risk exposures relating to the organisation's governance, operations and information systems. When carrying out an IT audit, the internal auditor's role will involve confirming the reliability and integrity of the Computerised systems that are used to produce financial and operational information, and looking at the controls within those systems.

IT audits could take place in relation to any department within an organisation, however some of the departments most likely to be investigated by an internal auditor undertaking an IT audit are:

- Administrative services
- Communication services
- Security systems (IT and physical)
- Database and engineering services
- Information services
- Documentation services

1.1 Information Systems Risk

Modern organisations place a vast amount of reliability upon their information systems. Functions such as finance, payroll and HR are highly dependent upon their systems to produce accurate and reliable information. But how can we be sure that these systems are working properly? And what would happen if they went wrong? It is the role of the IS auditor to find out the answers to the questions.

Given this level of reliance, the risk of error due to poor information systems, inappropriate controls over access and security, or failure to back-up, is a fundamental one. These risks can lead to errors in reported financial or other operational data, fraudulent activity, security breaches, customers or employee (for instance in the case of a payroll system error) dissatisfaction, or non-compliance with security of data legislation.

Information system risk is clearly an important area over which careful controls should be implemented to ensure exposures to these risks are minimized.

1.1.1 Changes to the IS environment

Technology moves fast and new developments and updates are constantly being made. It is therefore likely that changes in the IS environment will regularly occur and these changes have the potential to be significant. Obviously, such changes increase the levels of risk that may be present within the information systems. Internal auditors should evaluate the risk exposures relating to the organisation's governance, operations and information systems. When carrying out an IT audit, the internal auditor's role will involve confirming the reliability and integrity of the Computerised systems that are used to produce financial and operational information, and looking at the controls within those systems. Auditors should ensure they are aware of changes in the IS environment and make sure adequate change controls, such as audit trails and access restrictions and logging, are in place to ensure this risk is managed.

1.2 Contingency planning

A Contingency plan is a plan devised for a specific situation when things could go wrong. They are also known as back-up plans and form part of business continuity planning.

Contingency plans include specific strategies and actions to deal with a particular problem, emergency or state of affairs. They also include a monitoring process and triggers for initiating planned actions. They are required to help organisations recover from serious incidents in the minimum time with minimum cost and disruption.

An organisation often has key IS systems on which it relies heavily in order to carry out its business. The systems considered key will vary between organisations, but examples might include the accounting system, payroll system or HR systems used by an organisation.

Systems such as these require contingency plans to ensure business can still continue should the system go down or become corrupt. For example, if the payroll system goes down as the monthly pay run is due, a contingency plan is necessary to ensure the employees still get paid.

Internal auditors should ensure contingency plans are in place for key systems and review them to ensure the plans are adequate and have been sufficiently tested.

1.3 Hardware

Hardware is the general term for the physical components of a computer system. Three key pieces of hardware are described below.

Mainframes	Mainframes are powerful computers that are mainly used by large organisations for critical applications. They are usually connected to lots of terminals and peripheral devises (such as high-volume printers).
Workstations	Workstations can either refer to PCs or to minicomputers. Minicomputers are generally more powerful than PCs or laptops. They vary greatly in terms of size and power and may be connected to several terminals. The minicomputer may serve as the central computer in small organisations.
Servers	Servers are computer systems that provide services to other computer systems (clients). As well as hardware, servers usually contain an operational software element. Servers have a similar purpose to mainframe computers, however they are physically smaller and the information it contains is delivered to a smaller network of workstations.

1.4 Operating systems

An operating system is the software that runs the computer, for example Windows. It is an interface between the hardware and the applications, e.g. Word or Excel.

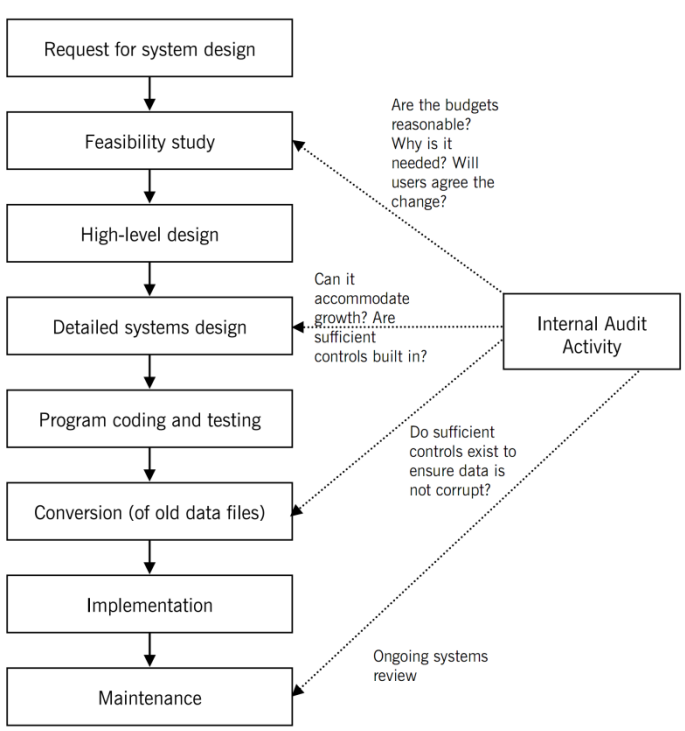
Different operating systems are appropriate for different types of computers.

If an operating system on a mainframe or a network crashed, many employees would not be able to access their work. This risk means that operating systems should be given consideration by internal auditors.

1.5 Systems development methodology

IS systems have a lifecycle running from the request for its design through to maintenance. Internal audit may be involved in the whole process. The design of systems is a crucial time for internal audit involvement as it gives them the opportunity to ensure risks and controls are properly considered and appropriately managed right from the outset, rather than the reactive role they may play with existing systems. This gives the operational staff more assurance that

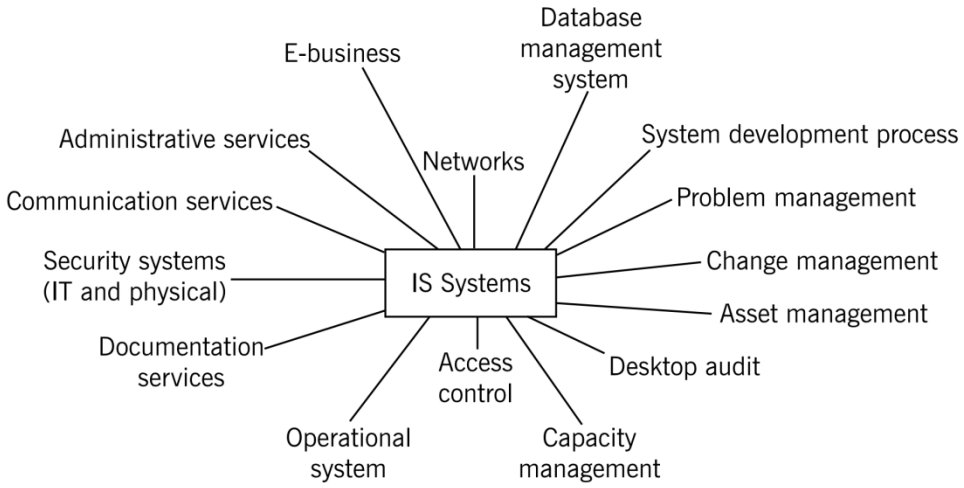
they can rely on their system, and make reviews by internal audit easier. However, care must be taken to ensure the internal audit activity does not put itself at risk of self-review. This can be achieved by ensuring that the auditors involved carry out a consulting (rather than decision making) role only, and by using different members of the audit team to review the system once it is up and running to those involved in the initial development.



Development is best carried out by a design team that can ensure all stakeholders' needs are considered.

1.6 Carrying out an IT audit

IT audits could take place in relation to any department within an organisation. The diagram below shows the various areas of IT in the organisation which might be subject to a test of controls by internal auditors.



Information systems are complex, and it is likely that it will be necessary to have an IT specialist in the internal audit team to undertake audits of IS controls, as some of these controls will be programmed into the system. The internal controls in a Computerised environment include both manual procedures and procedures designed into computer programmes. Such control procedures comprise two types of control, general controls and application controls.

General IT controls are policies and procedures that relate to many applications and support the effective functioning of application controls by helping to ensure the continued proper operation of information systems. They commonly include controls over data centre and network operations, system software acquisition, change and maintenance, access security, and application system acquisition, development and maintenance.

Application controls are manual or automated procedures that typically operate at a business process level. They can be preventative or detective in nature and are designed to ensure the integrity of the accounting records. Accordingly, they relate to procedures used to initiate, record, process and report transactions or other financial data.

1.6.1 General controls

GENERAL CONTROLS	EXAMPLES
Development of computer applications	Standards over systems design, programming and documentation Full testing procedures using test data

	Approval by computer users and management Segregation of duties so that those responsible for design are not responsible for testing Installation procedures so that data is not corrupted in transition Training of staff in new procedures and availability of adequate documentation
Prevention or detection of unauthorised changes to programmes	Segregation of duties Full records of programme changes Password protection of programmes so that access is limited to computer operation staff. Restricted access to central computer by locked doors, keypads Maintenance of programmes logs Virus checks on software: use of anti-virus software and policy prohibiting use non-authorised programmes or files Back-up copies of programmes being taken and stored in other locations Control copies of programmes being preserved and regularly compared with actual programs Stricter controls over certain programmes (utility programmes) by use of read-only Memory
Testing and documentation of programme changes	Complete testing procedures Documentation standards Approval of changes by computer users and management Training of staff using programmes
Controls to prevent wrong	Operation controls over programmes Libraries of programmes

programmes or files being used	Proper job scheduling
Controls to prevent unauthorised amendments to data files	Password protection Access to authorised staff only Amendments require approval by senior staff member
Controls to prevent unauthorised amendments to data files	Password protection Access to authorised staff only Amendments require approval by senior staff member
Controls to ensure continuity of operation	Storing extra copies of programmes and data files off-site Protection of equipment against fire and other hazards Back-up power sources Disaster recovery procedures e.g. availability of back-up computer facilities. Maintenance agreements and insurance

The auditors will wish to test some or all of the above general IT controls, having considered how they affect the computer applications significant to the audit.

General IT controls that relate to some or all applications are usually interdependent controls, i.e. their operation is often essential to the effectiveness of application controls. As application controls may be useless when general controls are ineffective, it will be more efficient to review the design of general IT controls first, before reviewing the application controls.

1.6.2 Application controls

The purpose of application controls is to establish specific control procedures over the accounting applications in order to provide reasonable assurance that all transactions are authorised and recorded, and are processed completely, accurately and on a timely basis.

Application controls include the following.

APPLICATION CONTROLS	EXAMPLES
Controls over input: **completeness**	Manual or programmed agreement of control totals Document counts One-for-one checking of processed output to source documents Programmed matching of input to an expected input control file Procedures over resubmission of rejected data
Controls over input: **accuracy**	Programmes to check data fields (for example value, reference number, date) on input transactions for plausibility: • Digit verification (e.g. reference numbers are as expected) • Reasonableness test (e.g. sales tax to total value) • Existence checks (e.g. customer name) • Character checks (no unexpected characters used in reference) • Necessary information (no transaction passed with gaps) • Permitted range (no transaction processed over a certain value) Manual scrutiny of output and reconciliation to source Agreement of control totals (manual/programmed)
Controls over input: **authorisation**	Manual checks to ensure information input was: • Authorised • Input by authorised personnel
Controls over processing	Similar controls to input must be in place when input is completed, for example, batch reconciliations. Screen warnings can prevent people logging out before processing is complete

Controls over master files and standing data	One-to-one checking Cyclical reviews of all master files and standing data Record counts and hash totals used when master files are used to ensure no deletions Controls over the deletion of accounts that have no current balance

Controls over input, processing, data files and output may be carried out by IT personnel, users of the system, a separate control group and may be programmed into application software. The auditors may wish to test the following application controls.

TESTING OF APPLICATION CONTROLS	
Manual controls exercised by the user	If manual controls exercised by the user of the application system are capable of providing reasonable assurance that the system's output is complete, accurate and authorised, the auditors may decide to limit tests of control to these manual controls.
Controls over system output	If, in addition to manual controls exercised by the user, the controls to be tested use information produced by the computer or are contained within computer programmes, such controls may be tested by examining the system's output using either manual procedures or computers. Alternatively, the auditor may test the control by performing it with the use of computers.
Programmed control procedures	In the case of certain computer systems, the auditor may find that it is not possible or, in some cases, not practical to test controls by examining only user controls or the system's output. The auditor may consider performing tests of control by using computers, reprocessing transaction data or, in unusual situations, examining the coding of the application programme.

As we have already noted, general IT controls may have a pervasive effect on the processing of transactions in application systems. If these general controls are not effective, there may be a risk that misstatements occur and go undetected in the application systems. Although deficiencies in general IT controls may preclude testing certain IT application controls, it is possible that manual procedures exercised by users may provide effective control at the application level.

2. Communications, transfers and e-commerce

Vast amounts of information travels using information technology, for example via emails, internally using intranets, or globally via the internet. Transactions are carried out remotely using e-commerce and meetings held remotely using web technology. This information may be at risk from hackers, viruses and unauthorised access if adequate and sufficient controls are not in place. This section looks at the main risks and controls associated with electronic communications, transfers and transactions.

2.1 Networks

A network is an interconnected system. It consists of two or more computers that are linked together in order to share resources.

There are a number of types of networks that you should be familiar with; LANs, WANs, VANs and MANs

LAN **Local Area Network**	LANs connect computers and related devises (e.g. printers) in a relatively small area. It is generally limited to a geographic area, such as a single building. It allows users to share data and devises. The connections can be either physical or wireless, and can also connect to the Internet.
WAN **Wide Area Network**	If LANs (which are limited in distance) connect to each other, they become WANs. These connect larger geographical areas, e.g. an entire organisation, or the entire state of Florida.

	WANs can also connect using wireless transmission and are available to mobile computers. WANs are extremely complicated. However, to a user it may not look much different to a LAN.
VAN **Value Added Network**	VANs are private networks that lease communication lines to subscribers. VANs traditionally transmitted data formatted as Electronic Data Interchange, but they now also often transmit XML formatted data.
MAN **Metropolitan Area Network**	MANs are data networks designed for a town or city.

2.2 Voice communications

Some industries, e.g. airlines, rely on continuous, uninterrupted communications. Failure of systems such as these could have fatal consequences, whilst false or fraudulent messages could lead to unnecessary and expensive emergency landings.

Internal auditors should review systems that transmit this kind of communication data in order to assess its integrity, security, reliability and performance.

When reviewing these systems, auditors should consider the following exposures and methods to control them.

Exposures	Controls
System downtime Response time – what effect might a delay in transmission have? Security – can unauthorised personnel 'listen in'? Corrupted, lost or duplicated data Fraudulent messages planted in the system	Network-monitoring software to identify problem points in transmission lines and equipment Data encryption Message sequencing to spot gaps and duplicates Self-checking algorithms that can detect changes in messages

2.3 Internet

The Internet has revolutionized the way many organisations conduct their business, however, it also exposes the organisation to a number of risks such as viruses or hackers and intruders who enter their internal network through transferred files or email attachments.

Features of the Internet include:

Hypertext Transfer Protocol	This is the http at the start of internet addresses. It is used by all Web servers on the Internet
Uniform Resource Locators (URLs)	The URL is the unique 'name' of the website. This is what makes 'links' possible.
HTML (Hypertext Markup Language)	This is the basic code that formats Web documents (bold, italics, capitals etc.).

Internet service providers (ISP), such as AOL, maintain servers within the Internet. You can access the internet through their servers if you are signed up to a package with them.

Anyone who is connected to the Internet is at risk from viruses and hackers, and are exposed to E-crime such as theft of identity or clearing out of online bank accounts. Obviously for organisations which have many machines connected to the Web, and vast amounts of electronic data, this risk could become significant.

2.3.1 Electronic transfers and interfaces

Funds and data can be transferred electronically using electronic funds transfers (EFT) and electronic data interchanges (EDI).

Electronic fund transfers allow payments to be made electronically rather than manually. They are a fast, cheap method of processing payments.

An **electronic data interchange** is the communication of data from one computer to another using standardized document formats.

The main risks associated with EDIs relate to the **loss of data** and the security of information.

The controls an organisation may put in place to manage these risks include:

- Setting up access for authorised users only, with different access rights (e.g. read only, make transactions, authorise transactions).
- Message protection whilst in transit, e.g. encryption, to prevent interception / tampering.
- Message authorisation to protect the integrity of the message.

2.3.2 E-Commerce

E-commerce is now an accepted, and often expected, aspect of modern commercial life.

E-commerce is the process of conducting commercial activities over the Internet.

Transactions over the internet can be business-to-business, business-to-customer, or business-to-employee.

There are a number of risks involved in e-commerce.

Major risks include:

- Damage to software, files or databases from viruses, Trojans etc.
- Human error, e.g. accidental deletion of data, or clicking on a link they had presumed to be safe
- Access by hackers
- Technical failure, e.g. software bugs
- Infrastructure failures, e.g. server crashes
- Credit card and payment fraud
- Hoaxes – can clog up emails systems and cause problems similar to a real virus
- Physical damage to the IT infrastructure, e.g. due to fire or flooding
- Data protection – legal privacy requirements
- Rapid technological changes
- Incorporating changes to surrounding business processes and organisational structures

The major components of e-commerce audits might include:

- Assessing the internal control structure
- Providing reasonable assurance that goals and objectives can be achieved
- Determining if the risks are acceptable
- Understanding the information flow
- Reviewing interface issues (hardware to hardware etc.)
- Evaluating the business continuity and disaster recovery plans

3. Security

Computers face risks such as hackers, viruses and other unauthorised access to data which could, for example, lead to the leak of confidential information, or cause fraud to be carried out against the organisation.

Computer security is an on-going concern, although there are a number of measures that should be put in place by organisations to reduce the risk of malicious corruption to their systems or data and information.

3.1.1 Access control

Access control is a method of securing systems to prevent them being accessed by unauthorised parties by requiring user ID information. Password protection when logging on to your work network is a simple example.

Access control is also known as authentication.

3.1.2 Firewalls

Firewalls create barriers to prevent unacceptable incoming transmissions while permitting authorised communications. They do this by using rules to sort incoming messages to ensure only acceptable message are received.

They make take the form of either a hardware devise or a software programme.

There are three types of firewalls you should be aware of:

Packet filter firewalls	These identify the source and destination addresses of all information and either allow or block the information based on an established set of user-defined rules.
Gateway firewalls	These filters work by applying security mechanisms to the specific application selected.
Proxy servers	Proxy servers are private network firewalls that intercept all messages that enter or leave the network and hide the true network address

3.1.3 Virus protection programmes

Virus protection programmes identify incoming items which may potentially carry viruses. They then attempt to prevent the virus causing any damage.

Such programmes develop rapidly to keep up with the fast pace with which virus programmers create new ways of causing damage to computers.

3.2 Information protection

Information can be protected using encryption. Encryption disguises data by encoding it and making it unintelligible to readers without unscrambling software.

Encryption allows data to be securely transmitted over networks, including the Internet.

3.3 Application authentication

Application authentication is where a software application is able to prevent unauthorised access to itself. For example, Microsoft Windows has this in that it creates accounts for authorised users with required identification.

Web applications can also authenticate users.

4. Databases

A database is a collection of data organised to serve many applications. The database provides convenient access to data for a wide variety of users and user needs.

A database management system (DBMS) is the software that centralises data and manages access to the database. It is a system which allows numerous applications to extract the data they need without the need for separate files.

The way in which data is held on a system affects the ease by which data is able to be accessed and manipulated. Many modern software packages are built around a database. A database provides a comprehensive set of data for a number of users.

Databases can be either flat or relational.

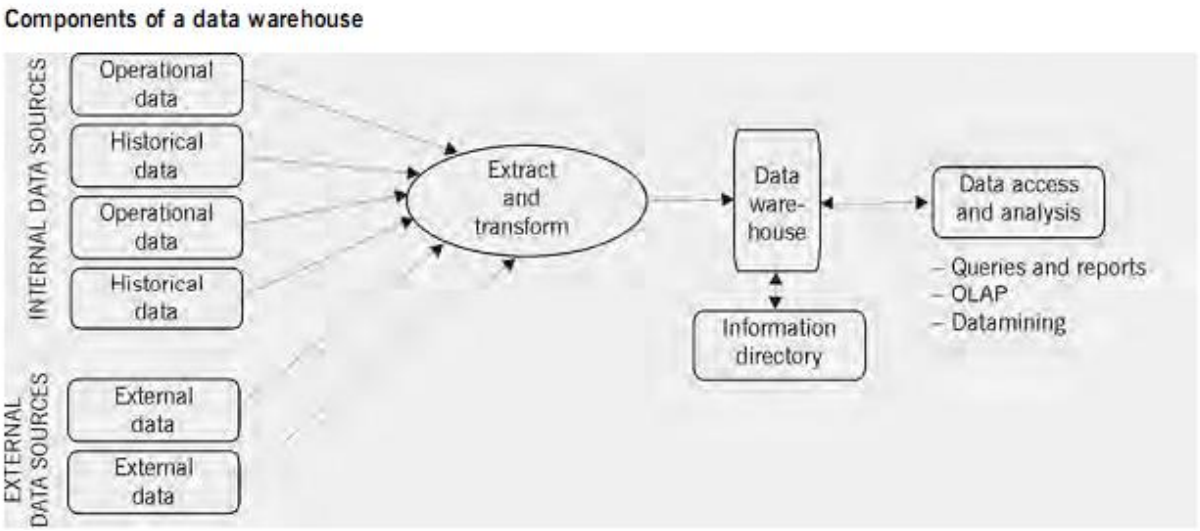
Flat databases incorporate all data in a single database. This can lead to large databases with redundant entries.

Relational databases link smaller databases so they can share data. The user only needs to enter data in a relational database once, however it can then be accessed a number of times in all the smaller databases.

Technological advances mean the size and capabilities of databases is continually expanding, with many now capable of storing picture, audio and video files as well as words.

Very large databases are called data warehouses.

A **data warehouse** consists of a database containing data from various operational systems, and reporting and query tools.



Data mining is the process of extracting useful information from a data warehouse.

Data mining software looks for hidden patterns and relationships in large pools of data.

4.1 Auditing and databases

Auditors regularly make use of databases.

5. Software licensing

Software programmes are issued to organisations on license. Copying the software for use by another user, without purchasing an additional license, is illegal.

Software programmes used by organisations have to be purchased in order to be legitimate. Copying software is illegal and violates the intellectual property rights of the developer of that software.

Organisations that use many copies of the same programme can buy licenses for all the users who might be using the programme on the organisation's network.

Internal auditors are responsible for verifying that these licensing requirements have been met.

6. Enterprise-wide resource planning

Enterprise resource planning (ERP) is an integrated computer-based system used to manage internal and external resources such as

- Financial resources
- Tangible assets
- Materials
- Human resources

The purpose of the ERP is to facilitate the flow of information between all business functions within the organisation and manage the connections to outside stakeholders. They consolidate all business operations into a uniform and enterprise wide system environment.

6.1 Implementing ERP

The implementation of enterprise-wide resource planning (ERP) in an organisation often leads to an entire reorganisation of the business.

It is important for the internal auditor to be involved from the very start of the implementation process to ensure that all risks are identified and suitable controls are built into the systems and processes.

The internal controls may drastically change and the internal auditor should help management and operational staff involved to fully understand any changes to methods and controls and the impact of these changes.

6.2 Challenges faced in the implementation of ERP

Implementing enterprise-wide resource planning can bring with it many challenges, for example:

- Operational efficiency can be harder to understand due to the complexity of hardware and engineering
- It can be difficult to secure acceptance of the new technology from the end users
- Training can be costly, in terms of time, money and the effort directed towards it

A widely used enterprise-wide resource planning software package is SAP.

Chapter 11: Other assurance engagements

1. Audits of third parties and contract audits

ISQIA 7300 Outsourced Internal Audit service

It is the responsibility of the organisation to maintain appropriately sufficient and effective internal audit activity when such activity has been outsourced to an external audit firm or service provider.

Organisations occasionally use contractors to provide a service. This may be a small ad-hoc piece of work, or the outsourcing of an entire department, such as IT, catering or payroll. In either case, there will be a contract involved and the work is done by personnel that do not work directly for the organisation, i.e. third parties. These contracts and the work carried out by these third parties are subject to review by internal audit.

A third party audit is the auditing of work performed by contract professionals that includes outsourcing and co-sourcing costs.

Contract audits may be carried out for a number of reasons:

Effectiveness. To ensure the organisation's objectives are being met. The audit would involve ensuring that:

- there is sufficient need to justify the contract
- contracting is the best way of meeting this need
- the organisation is receiving the best quality at the best price

Economy. To ensure that the contractor was selected for the best combination of quality, time and costs.

Efficiency. To ensure the contract is being managed in the most efficient way.

Compliance. To ensure the policies, requirements and details of the contract are being complied with.

1.1 Lump sum (fixed price) contracts

Under a lump sum contract, the contractor provides the service for a fixed cost. The aim of the client is to transfer all risks to the contractor for a fixed price. The fixed price will be based on a number of bids from potential contractors.

Although these types of contracts are usually simple, complications can occur leading to a change of scope and increased expenditure. Additional costs may then be passed on.

Poor quality / performance

With this kind of contract, the contractor will make a good profit if costs turn out to be a lot less than expected.

If things do not go to plan however, the contractor will face lower profits or possibly a loss.

This suggests that the contractor will be highly motivated to manage costs in order to maximise their profits. This may lead to poor quality work or poor performance by the contractors.

Additional costs

Despite transferring risks to the contractor, the client may still face additional expenditure if the contractor can demonstrate that the extra costs related to genuinely unforeseen problems.

This may also motivate contractors to under-bid then boost their position with additional cost claims.

These risks can be reduced by ensuring that the contract is clearly defined at the outset, costs are identified as accurately and completely as possible and the risks assumed by both the contractor and the client are clearly defined.

When reviewing such a contract, the auditor might look at

- Level of competition for the contract
- Charges for work not done or equipment not received
- Escalation clauses (provision for increasing charges to reflect specified conditions, e.g. inflation)
- Authorisation for additional expenditure or work
- Overhead expenses charged separately
- Sufficiency of work performed in relation to original requirements

1.2 Cost-plus contracts

Cost-plus contracts are suitable where there are a number of unknown factors. Under this kind of contract, the client pays the contractor a fixed fee and the contractor then claims for costs such as labour, equipment, maintenance etc.. The additional costs are usually based on the initial costs plus a fixed fee or a fee based on percentage of costs. This is beneficial to the client as the costs match the activities and so prevents the contractor making excessive profits.

If there is no incentive for the contractor to properly manage costs, the client will be forced to cover these costs.

The contractor may therefore

- Carry out work that is really not needed
- Purchase excessive amounts of equipment
- Purchase materials inefficiently

If the fee is based on a percentage of costs, the contractor has a greater incentive to increase costs in this way.

The risks can be reduced by including some costs within the fixed fee to encourage the contractor to manage costs properly.

To ensure the exposure to this risk is minimized, auditors should review the contract against what is happening in practice very carefully, looking at things such as:

- Method of billing overhead costs
- Poor cost controls by the contractor. No effort to obtain best prices and failure to pass any discounts on to the client
- Excessive charges for using contractor-owned equipment
- Excessive hiring of staff
- Excess billing over contractor costs
- Unreliable cost accounting and reporting
- Excessively high standards
- Poor physical protection of materials or equipment, lack of control over employees in regard to absences and overtime, poor quality or performance, wasteful used materials, idle rented equipment or other negligence that raises costs

1.3 Unit-price contracts

A price is agreed for each unit of work. Such contracts work best where large numbers of identical products/services are provided.

When reviewing such a contract, the auditor may be asked to look at risks including:

- Number of units completed in relation to number of units recorded
- Changes to the original contract
- Relationship between actual costs and prices
- Record keeping methods
- Increases in unit prices

2. Quality audit engagements

Quality audit engagements aim to assist an organisation in improving its quality and productivity.

Total Quality Management (TQM) is an 'integrated and comprehensive system of planning and controlling all business functions so that products or services are produced which meet or exceed customer expectations'. TQM is a philosophy of business behaviour, embracing principles such as employee involvement, continuous improvement at all levels and customer focus, as well as being a collection of related techniques aimed at improving quality such as full documentation of activities, clear goal-setting and performance measurement from the customer perspective.

The goal for a quality audit is to help an organisation increase its quality and productivity. To do this the auditor will have to focus on the organisation's procedures.

The procedures need to be defined, controlled and communicated to all relevant parties, then followed by all appropriate employees.

All members of the organisation need to be involved to secure long-term success.

When carrying out quality audits, auditors will:

- Identify any actual and potential risks
- Identify ways of rectifying or preventing quality problems
- Identify areas where continuous improvement could be made
- Assess the quality and sufficiency of staff training
- Check that staff comply with the organisation's processes and procedures and any regulatory or legal requirements
- Remove any out-dated activities or unnecessary controls from the processes and procedures

2.1 Purpose of quality audits

Quality audits are carried out to provide an organisation with reasonable assurance that the quality plans in place are sufficient to achieve the level of quality they are aiming to achieve.

In order to do this, the auditor has to ensure that the procedures are not only adequate, but also that they are being followed. There must also be conformance to specifications, compliance with relevant laws and regulations, and that data systems can maintain and convey accurate and adequate information relating to quality for the organisation.

By doing this, the organisation will be better equipped to identify deficiencies and required corrective action as well as opportunities for continuous improvement.

3. Due diligence audit engagements

Due diligence audits are usually voluntary and may be necessary when an organisation intends to carry out a large financial transaction, such as the purchase of a property or acquisition of another business. They are one-off investigations into that transaction, property or business.

Due diligence engagements are usually required when the organisation plans to acquire another business or property or engage in a substantial financial transaction. The aim is to determine whether that transaction should actually go ahead.

Due diligence review is one off investigations into a person, business or financial transaction.

Due diligence reviews are considered to be best practice and, as such, are usually voluntary. However, there could be a legal requirement for such a review in some cases, for example suspected theft of intellectual property.

The two most common reasons for performing a due diligence audit are:

(1) Financial (mergers, acquisitions, banking, securities)

(2) Real estate (property etc.)

The information and documentation that can be used in a due diligence audit varies from country to country. You should confirm the restrictions in the country in which your organisation is based before undertaking such a review. In the USA for example, only public documents can be reviewed. In other countries private information may also be allowable, providing the appropriate confidentiality agreements are in place.

Auditors must take due care when carrying out such an audit. This basically means doing what a reasonable person would do.

Due care is the level of caution that an individual exercises when performing the due diligence audit and reporting the results.

This concept is particularly important when civil litigation is involved.

3.1 Who is involved?

There are three types of personnel usually involved in a due diligence engagement team

Internal auditors	Will look at the processes involved and the capabilities of the organisation. This may include reviewing operations, internal controls and compatibility.
External auditors	Will look at the transactions involved
Lawyers	Responsible for identifying any legal problems, law suits etc..

Their joint goal is to accurately and timely gather the sufficient information and ensure this covers all areas of risk and opportunity. Coordination between the parties is crucial if this is to be achieved.

The due diligence process establishes whether the expected benefits of the transaction are likely to be realized.

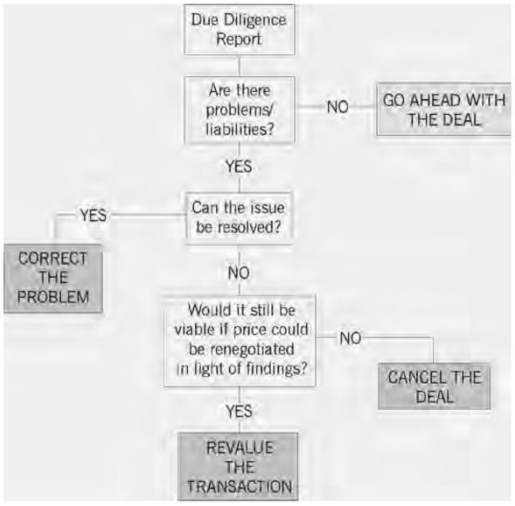
It may also make benefit realization more likely by improving the efficiency and effectiveness of the implementation of the transaction.

3.2 Engagement report

The final report should focus on facts, not opinions, and be backed up by supporting documentation and evidence.

- Include an executive summary. This summary should clearly identify any factors which could assist in the negotiation of a more favourable deal.
- Be structured by business cycle e.g. HR, Finance, Sales and Marketing etc.
- Be fully backed up and linked back to supporting documentation and working papers

The report should be presented in the format which best communicates the results.



The senior management of the organisation will then use the report to make a decision about whether or not to go ahead with the transaction. The diagram shows the decisions they may make.

4. Performance audit engagements

Performance audits review the success of an organisation in meeting those objectives most importance to it by looking at how it sets, measures and uses its key performance indicators.

Managers need to be able to:

- Assess/measure performance
- Identify deficiencies
- Identify the cause of those deficiencies
- Take corrective action

However, it is not possible to efficiently and effectively track all parts of an organisation.

The focus has to be on those measures that relate to the most important objectives of the organisation. These factors are known as key performance indicators (KPIs).

KPIs should be created and applied by management. These KPIs allow them to retain control over the organisation. KPIs can be categorised as follows:

Category	Purpose	Example
Quantity	Measures quantitative performance	Number of units produced per week

Accuracy	Measures quality performance	Number of sold items returned
Cost	Specifies benchmarks	Labour costs per unit
Timeliness	Associated with production schedules or	Average time to produce single unit
Capital	project completion	Return on investment
Revenue	Measures monetary value attached to sales	Revenue per unit

KPIs can provide an excellent basis for audits of performance, allowing the auditors to perform efficient, cost-effective audits.

Auditors should consider the following:

- Has the organisation set KPIs?
- How appropriate are the KPIs for measuring how well the organisation meets its objectives?
- Have they been carefully worded to ensure they are properly understood and interpreted by employees?
- How appropriate is the timing of the measuring of KPIs? Would it be more beneficial to measure earlier, or later in the process?
- Do the KPIs control performance effectively? KPIs should be capable of identifying problems and improving them.

5. Operational audit engagements

Operational audit engagements review the efficiency, economy and effectiveness of specific operations.

The effectiveness and efficiency of operations is one of the areas defined by the COSO integrated framework over which internal control can provide reasonable assurance.

Operational audits deal specifically with the efficiency, economy and effectiveness of operations.

Efficiency means making sure things are done in the right way

Economy means ensuring the operations are cost effective

Effectiveness means ensuring the right things are done.

Operational auditing looks at how well (i.e. how efficiently and effectively) organisations meet their objectives.

This might include reviewing

- the organisation's policies and procedures
- the ability of management
- the organisational culture
- efficient and effective use of resources
- communication networks
- tone at the top
- goal congruence (is everyone in the organisation working towards goals which relate to and support the overall objective?)

6. Compliance audit engagements

Compliance audit engagements review the extent to which the organisation complies with applicable laws and regulations.

Compliance with applicable laws and regulations is one of the areas defined by the COSO integrated framework over which internal control can provide reasonable assurance.

Internal auditors carry out compliance reviews and follow ups in specific areas of the organisation. These reviews are generally much less subjective than many other audit engagements. The point of these reviews is to ensure that specific standards, legislation or other regulations are properly complied with.

6.1 Regulatory compliance programmes

The aim of compliance programmes is to

- Identify and prevent and unintentional violations
- Identify and deter intentional violations
- Uncover illegal activities
- Assist in proving insurance claims and determining liability
- Enhance and create corporate identity

Internal auditors should review the organisation's compliance with regulations.

Standards and procedures

Organisations should establish compliance standards and including:

- Written code of conduct identifying prohibited activities. This should be easy to understand and clearly written. It should provide guidance to employees and contain checklists, question and answer sections, and references to other sources of information.
- An organisation chart identifying who is responsible for implementing compliance programmes
- A global compliance programme reflecting local laws and conditions should also be in place for international organisations.
- There should be no incentive or reward for unethical or illegal behaviour in the organisation's rewards systems. Any such inclusion would discourage compliance.

Additional methods of improving compliance

The organisation should also take the following steps to ensure the programme is successful:

Responsibilities

- Overall responsibility should be given to an individual of high-level personnel in the organisation.
- CEO and senior management should have involvement in the programme and should lead by example (tone at the top).
- No responsibility should be given to any individual who is known, or should be known, to be likely to become involved in illegal activities.

Communication

- The standards and procedures should be communicated to all employees.
- Training should be provided where necessary.

Monitoring and reporting

- Employees should be encouraged to report wrongdoings without fear of retribution.
- A hotline should be set up for employees to report suspect activities. To be most effective this should

  - be backed up by policies protecting employees from retribution

  - not be manned by a legal representative

- not be provided by an off-site ombudsman

- not require the employee to provide a written report.

- Systems that may detect criminal activity should be monitored and audited.
- Ethics questions could be used to uncover wrongdoings.

Discipline and review

- Violators should be sufficiently disciplined in line with the individual case.
- Controls should be put in place to prevent similar future occurrences.
- Compliance programmes should be regularly reviewed and improved. Employees' contributions should be encouraged.

6.2 Environmental compliance audits

If organisations do not comply with environmental laws and regulations, they may be subject to fines and other penalties. This could lead to further problems such as reputational damage through bad publicity, particular where the failure to implement proper standards has led to injury or death.

In addition, demonstrating compliance (and exceeding the minimum requirements) can have other benefits for the organisation, such as increased custom and loyalty from ethically aware consumers.

Environmental, health and safety (EH&S) risks should be identified and included in the entity-wide risk assessment. The HIA is responsible for ensuring such risks are considered.

There are a number of different environmental audits you may come across in your career.

Compliance audits	Do the activities and operations comply with legislation/ regulation?
Environmental management systems audits	Do the systems operate sufficiently to manage future environmental risks?
Transactional (due diligence) audits	Risk management tool to be used when the organisation is purchasing land
Treatment, storage and disposal	Tracking hazardous substances

Pollution prevention audits	Look at operations to identify areas where waste and pollution could be reduced
Environmental liability accrual audits	Quantify and report accrued liabilities for environmental issues
Product audits	Look at compliance within the production processes.

If risks are found not to be managed sufficiently, the HIA may change the schedule of engagements to further evaluate those risks.

Many environmental audits are carried out by teams that report to the EH&S executive. As the EH&S executive is also responsible for the facilities themselves, there could be a conflict of interest in this area.

Such teams rarely have contact with the HIA and the internal audit activity, although this is beginning to improve. The HIA should encourage a close working relationship with the chief environmental officer and the audit plan should be coordinated with environmental auditing activities.

The HIA should also occasionally schedule an audit of EH&S.

The HIA should evaluate whether the environmental auditors that report into the EH&S department are in compliance with audit standards and a recognized code of ethics. The HIA should also evaluate the placement within the organisation and the independence of the environmental audit function to ensure the audit committee (or other board committee) receives sufficient information about risks.

Chapter 12: Consulting engagements

1. Consulting engagements

Internal auditors sometimes assist clients by working in an advisory capacity. This kind of work is known as a consulting engagement.

Internal consulting is defined by COSO as including both internal consulting and assurance engagements. The nature of consulting services carried out by the internal audit activity must be defined in the audit charter.

Consulting engagements arise for a number of reasons.

- Given the overlap between assurance and consulting engagements, the need for one can be highlighted by the results of the other.
- Consulting engagements often arise in response to a request from audit clients for help in reviewing a process they intend to change, for example due to the implementation of a new IT system or a change in organisational or departmental structure.
- Consulting engagements can also arise when a new product or service is implemented in the organisation. In these situations, internal auditors can provide their objective opinion on the planned activities and procedures. It is possible for an auditor to do this without impairing their objectivity by ensuring only suggestions, not decisions, are made by the auditor.
- Finally, internal auditors may enter into formal engagements (such as those that external auditors have) with the organisation. Such engagements normally last a significant amount of time.

1.1 Distinguishing between assurance and consulting engagements

The difference between assurance and consulting engagements is not always clear and, as we noted above, there can be overlap between the two.

The below table aims to help you understand some of the key differences:

	Assurance engagements	Consulting engagements
Carried out by	Internal auditor	Internal auditor and client
For benefit of	Senior management, board, audit committee etc.	Operational management
Typically involves	Reviewing internal controls, risk management and governance processes, or checking compliance with legislation	Controls to be considered in the design of new systems, benchmarking, improving efficiency or effectiveness
Engagement is	Mandatory	Optional
Results are	Formal, reported and followed-up	Informal recommendations, agreed with the client, no mandatory follow up but may be monitored if specified in the consulting arrangement

1.2 Objectivity and independence

Internal auditors must take great care when carrying out consultancy engagements to ensure their objectivity and independence are not compromised. If there is any damage to their objectivity or independence, this would reduce their ability to carry out effective internal audit engagements in the future.

Internal auditors can minimise the risk of this occurring by:

- Ensuring that the internal auditors do not assume any management responsibilities. This is mainly avoided by ensuring that advice only is given, and no final decisions are made by the auditor.
- Not allowing auditors to review their own work. For example, if an auditor has been involved in the set-up of a new system in a consulting capacity, when that system is due to be reviewed as part of an internal audit engagement the review should be carried out by a different member of the internal audit team who had no involvement in the consulting activities.

2. Internal control training

Internal controls are an important element of any system, and work with controls is a fundamental part of an internal auditor's role. Everyone in an organisation has responsibility for internal controls.

Control – Any action taken by management, the board, and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved. Management plans, organises, and directs the performance of sufficient actions to provide reasonable assurance that objectives and goals will be achieved.

COSO's Internal Control – Integrated Framework suggests that everyone in an organisation has involvement with internal controls. If everyone is responsible for internal controls, then everyone (including the organisation itself) would benefit from some training in this area.

As experts in controls, internal auditors are the idea l people to provide training on internal controls.

2.1 Benefits of training staff

Training audit clients is beneficial not only to the individuals receiving the training, but also to the internal audit activity itself. This is because a well-structured workshop on COSO controls would help audit clients to understand the importance of audits. It may even make them more comfortable with the audit process. If staffs have a better understanding and more positive opinion of audit, they may be more willing to co-operate during audits, and provide information more freely to the auditors. This will help the whole audit process flow smoothly.

COSO states that internal control systems have three main objectives:

(1) Efficient and effective operations

(2) Accurate financial reporting

(3) Compliance with laws and regulations

Training in this area would help staff to understand why internal controls are so important, and appreciate the impact that could occur were those controls inadequate.

2.2 Components of COSO training

COSO training would also provide audit clients with a detailed understanding of each of the five components of the COSO framework. These five components are:

(1) **Control environment** – discipline and structure in the organisation provides the basis for the internal control system.

(2) **Risk assessment** – risks that may affect objectives should be identified and analysed by management (not internal auditors)

(3) **Control activities** – controls such as policies and procedures are in place to mitigate identified risks and ensure objectives are met

(4) **Information and communication** – there are suitable methods for identifying and communicating timely information to allow people to carry out their responsibilities.

(5) **Monitoring** – achievement of objectives is monitored, both by management and other parties outside the process (such as audit).

3. Business Process Review

Business process reviews focus on a specific process, rather than department or function, and review the efficiency and effectiveness of that process throughout the whole organisation.

Traditionally, the various departments of an organisation (e.g. finance, marketing, sales etc.) were very separate. However, new organisational models contain processes that cut across departmental (and geographical) boundary lines.

This shift in structure creates a challenge for internal auditors as their work has usually been focused on specific areas, departments, locations, or accounts. Business process audits provide the solution for measuring the efficiency and effectiveness of cross-functional processes. Such audits focus on specific processes, for example ordering, receiving and paying for supplies, throughout the whole organisation.

In a process oriented organisation, an audit executive may be assigned to each process, supported by a team of process oriented auditors.

3.1 Benefits of process reviews

There are a number of benefits to adopting a business process approach:

- Internal audit reports will be of greater interest to senior management as they focus on processes that directly impact on the survival and growth of the organisation
- This interest means they can be directly informed of any audit findings

- Audit staff gain a better, and more complete, understanding of the entire process
- By developing this overview of the entire process, internal auditors are well placed to resolve problems in the process, and advise as to how they can be resolved
- Both internal auditors and operational staff are interested in the welfare of the process, and so may work together more co-operatively.

4. Benchmarking

A benchmark is a goal that an organisation is aiming to achieve. It can be carried out in a number of different ways (internal benchmarking, industry benchmarking etc.) in order to identify where the current process lies in relation to this ideal (the benchmark). A strategy for improvement can then be put in place in order to achieve this ideal.

Benchmarking is the process of gathering data about targets and comparators that permit current levels of performance to be identified and evaluated against best practice. Adoption of best practices should improve performance.

In order for benchmarking to be effective it has to be realistic (not unattainable, or too simple to achieve), measurable, and beneficial to the organisation (e.g. helps it increase market share).

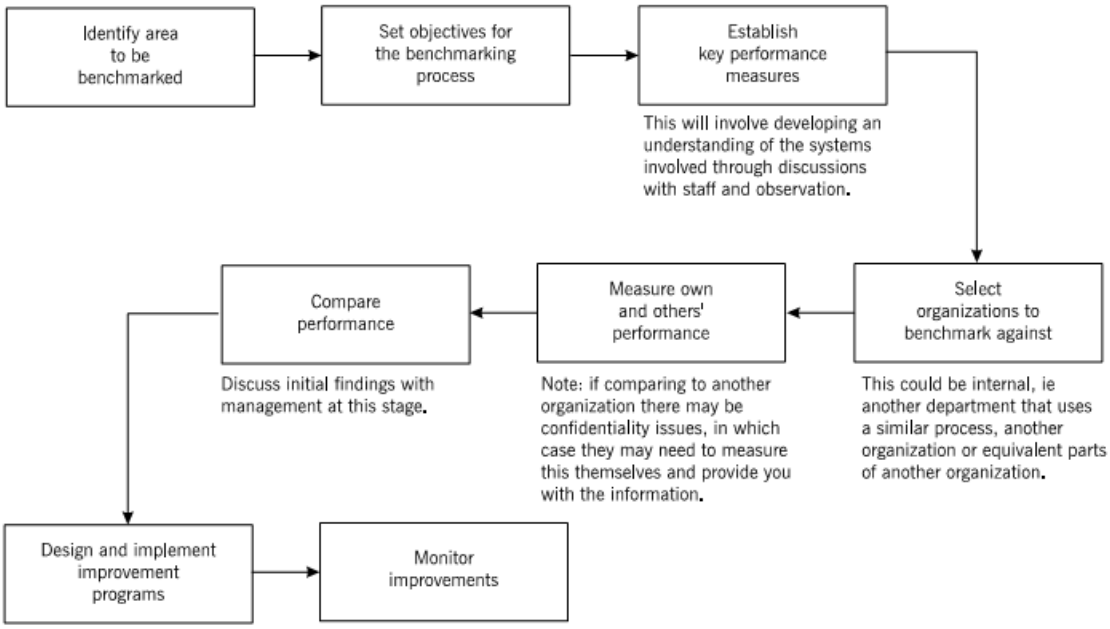
Evaluating the benchmarks set within the organisation is an appropriate service for internal auditors to carry out. Benchmarking is linked to TQM (Total Quality Management) and so it is most likely that auditors would be called upon to evaluate benchmarks as part of total quality audits.

The below illustrates the different ways that benchmarking can be carried out within an organisation.

Internal benchmarking	**Makes comparisons within the department or process itself.**
Competitive benchmarking	Information is gathered about the performance of a direct competitor.
Industry benchmarking	An industry wide measure is used as the benchmark.
Generic benchmarking	This compares the process with a similar process in a completely different industry.

Best-in-class benchmarking	Looks at the best external practitioner of the activity to be benchmarked, regardless of their industry.
Process benchmarking	This kind of benchmarking focuses specifically on the processes rather than the outcomes.

The below diagram illustrates the benchmarking process.



5. Performance measurement systems

It is important for managers to be able to measure their performance in order to know how well they are achieving their objectives and where improvements can be made. Internal auditors can be involved with performance measures both by assisting clients in their development of performance measures, or reviewing the performance measures as part of an audit engagement.

Management can measure performance using key performance indicators (KPIs).

In order to be effective KPIs should be:

- Measurable
- Selective (it is not possible to measure everything)
- Linked to the major objectives of the organisation

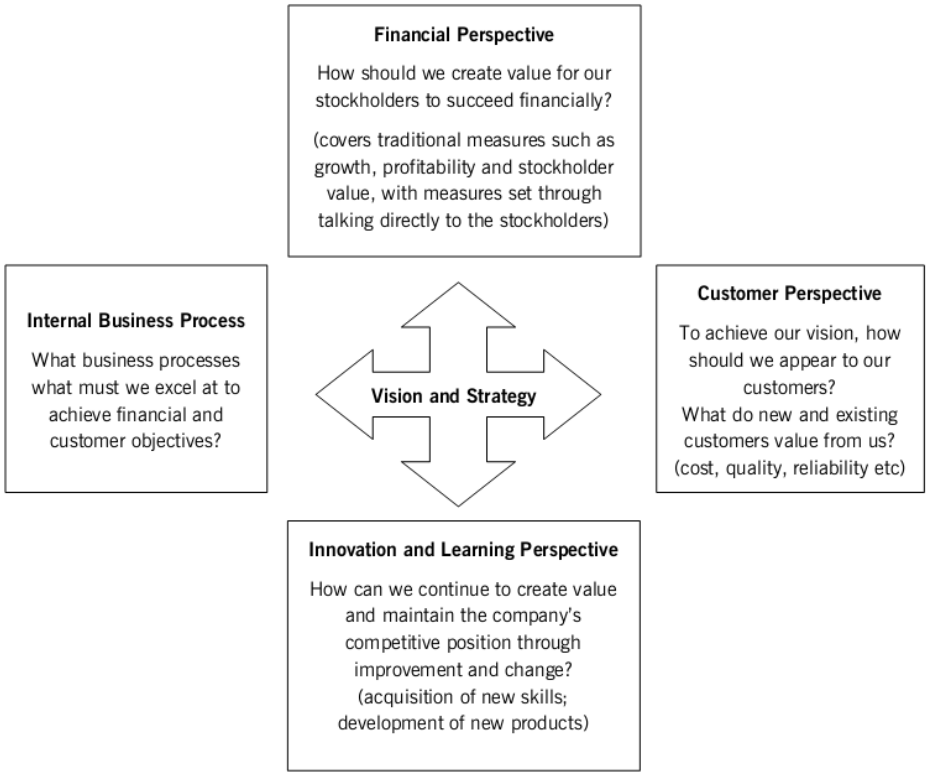
Internal auditors can work with clients to develop performance measures as well as review them in an audit.

5.1 Performance scorecards

Performance scorecards are a set of KPIs. The KPIs on such a scorecard may focus on quantitative measures of ongoing performance rather than measures that apply only to the longer term prospects of the company.

5.1.1 Balanced scorecard

The balanced scorecard, in contrast to the above, is made up of four sets of measures (perspectives) that look at the organisation's achievements in a much wider context.



The scorecard is **balanced** because it requires managers to think in terms of all four perspectives, rather than focus on just one (usually the financial perspective).

The four perspectives of the balanced scorecard, and the possible measures that could be considered under each, are:

	Possible measures
Financial perspective	Market share, sales growth, value-added stockholder value analysis
Customer perspective	On time deliveries, customer rejection rates
Business process perspective	Control measures will focus on core competences, skills, productivity and cost
Learning and growth perspective	Time-to-market for new products and percentage of revenue from them

Chapter 13: Fraud

1. What is fraud?

Fraud is an attempt to gain some benefit through dishonest actions, either through misrepresentation or concealment of the truth.

Fraud – Any illegal acts characterised by deceit, concealment, or violation of trust. These acts are not dependent upon the application of threat or violence or of physical force. Frauds are perpetrated by parties and organisations to obtain money, property, or services; to avoid payment or loss of services; or to secure personal or business advantage.

The term 'fraud' covers a whole range of irregularities and illegal acts. This can include ethical violations (violating company codes etc.) as well as criminal acts. The wide range can make it difficult to define exactly what constitutes fraud; however, fraud will always contain the following elements:

Intent	The person carried out the fraud intentionally
Misrepresentation	The act carried out (or intentionally not carried out) was deceitful, or false
Reliance	Knowledge of the victim is used to plan the fraud
Victim participation	The victim usually trusts the perpetrator with some power that enables the fraud to be committed
Concealment	The perpetrator tries to cover up, or hide, the action

1.1 Types of fraud

There are two distinct types of fraud; fraud that harms the organisation, and fraud that benefits the organisation.

Fraud that harms the organisation could be something like an employee submitting a travel expenses claim form for a journey that was never made.

Fraud that benefits the organisation could be a financial statement fraud such as valuing assets much higher than they are actually worth.

1.1.1 Fraud that harms the organisation

Fraud that harms the organisation is usually carried out for the benefit (directly or indirectly) of an employee, or another individual or organisation. ISQIA guidance provides a number of examples of what might fall into this category of fraud. These examples include:

- Accepting bribes or kickbacks
- Diverting a potentially profitable transaction that would normally generate profits from the organisation to an employee or outsider
- Embezzlement: Misappropriation of money or property and falsifying financial records to cover it up. This can be difficult to detect.
- Intentional concealment or misrepresentation of events, transactions, or data
- Submitting claims for goods or services not actually provided to the organisation
- Intentional failure to act in circumstances where action is required by the company or by law
- Unauthorised or illegal use of confidential or proprietary information
- Unauthorised or illegal manipulation of IT networks or operating systems
- Theft

1.1.2 Fraud that benefits the organisation

Fraud that benefits the organisation does so by exploiting an unfair advantage which may also deceive an external party. There will also often be an element of indirect personal gain, such as promotions or bonuses.

ISQIA guidance also gives a number of examples of what might fall into this category of fraud. These examples include:

- Improper payments, such as illegal political contributions, bribes, and kickbacks, as well as payoffs to government officials, intermediaries of government officials, customers, or suppliers
- Intentional and improper representation or valuation of transactions, assets, liabilities, and income, among others
- Intentional and improper transfer pricing (e.g. valuation of goods exchanged between related organisations) by purposely structuring pricing techniques improperly, management can improve their operating results to the detriment of the other organisation

- Intentional and improper related-party activities in which one party receives some benefit not obtainable in an arm's length transaction
- Intentional failure to record or disclose significant information accurately or completely, which may present an enhanced picture of the organisation to outside parties
- Sale or assignment of fictitious or misrepresented results
- Intentional errors in tax compliance activities to reduce taxes owed
- Prohibited business activities, such as those that violate government statutes, rules, regulations or contracts.

1.2 Why do people commit fraud?

People may commit fraud for a number of reasons. They may be in financial difficulty, they may believe that they are entitled to the benefits they obtain through fraud, or may simply stumble across an opportunity they can't resist. However, lots of employees may be in financial difficulty, yet they do not make the decision to defraud their organisation. So what makes some people carry out fraud? In order for fraud to occur, there must be three conditions in place: Opportunity, motive and rationalisation.

Opportunity Something that makes the fraud possible	Poor control designs, or lack of controls can be easily taken advantage of A circumstance that causes the controls of a well-controlled system to fail presents a brief opportunity for fraud Controls can be overridden or circumvented by people in authority
Motive A reason to carry out the fraud	Desire, such as greed or addiction Pressure, for example from debts Power, as is often the case with computer hackers who are motivated simply by proving they can do it
Rationalisation A way of convincing themselves that it is ok to commit the fraud	I'm entitled to it Everyone bends the rules, if senior management can do that, I can do this I'm only borrowing it, I will pay it back when my debt situation improves

	Genuine belief: This may occur when something considered unacceptable is common-place in the employees culture, or was tolerated by their previous employer

Of course just because the three elements exist, it does not necessarily mean that fraud will definitely be carried out. Some people will still choose not to commit the fraud. However, in order for fraud to take place, all three conditions must be present.

As internal auditors, there is little we can do about the motives and rationalisation of potential fraudsters. What we do know about, however, is **controls**. Our strong knowledge of internal controls places us in the ideal position to be able to identify **opportunities** for fraud that may exist within the organisation.

In addition to being aware of signs that indicate fraud, internal auditors should know how to prevent fraud and have an understanding of fraud schemes and scenarios. We will look at the roles of audit in the next section.

1.3 Roles of audit

Internal auditors play an important role in **detecting** and **deterring fraud** in the organisation. This is generally achieved through the assessment of the effectiveness and efficiency of the **controls** the organisation has in place to deter fraud during engagements, and also by remaining alert for any signs of actual or potential fraud.

Although they have this responsibility, the **management** of the organisation remain responsible for establishing suitable controls to prevent and deter fraud. Internal auditors support this through their role.

Internal auditors are required to have **sufficient knowledge** to **evaluate** the **risk of fraud** and how it is managed by the organisation. They are not, however, expected to have the expertise of a person whose primary responsibility is detecting and investigating fraud.

Internal auditors should detect the indicators of fraud and gather sufficient information to assist senior management in deciding whether full investigations by expert fraud teams is required. Such investigations are costly so the information should conclude as to whether the benefits of investigation will exceed the costs.

A second role of internal auditors is to carry out additional investigation around the fraud in order to gather data and to ensure the suspected perpetrators are not alerted to the investigation.

This indicates that internal auditors have two specific roles in relation to fraud:

(1) To maintain awareness of the potential for fraud during audit engagements

(2) To carry out fraud investigations when required

2. Fraud awareness

When carrying out an audit engagement, internal auditors must retain an awareness of the potential of fraud throughout the entire engagement and be aware of any indicators of this possibility.

Auditors need to be aware of fraud and the potential for it to be committed within the organisation. They should be vigilant for fraud when carrying out and audit engagement.

Internal auditors have a responsibility to:

- Notice indicators of fraud
- Design appropriate steps to ad dress significant risk of fraud
- Employ audit tests to detect fraud
- Determine if any suspected fraud merits investigation.

2.1 Notice indicators of fraud

We have already looked above at the different types of fraud that could occur within an organisation and have seen how it can either benefit or harm the organisation.

We noted that all frauds include particular common elements: intent, misrepresentation, reliance, victim participation and concealment.

Internal auditors should ensure they have a good understanding of what constitutes fraud and where it might take place.

We also demonstrated in Section 1 that, in order for a fraud to exist, three conditions must be met: **opportunity**, **motive** and **rationalisation**.

Auditors should ensure they are familiar with each of these concepts and must ensure they notice situations where the conditions for fraud may exist.

2.1.1 Red flags

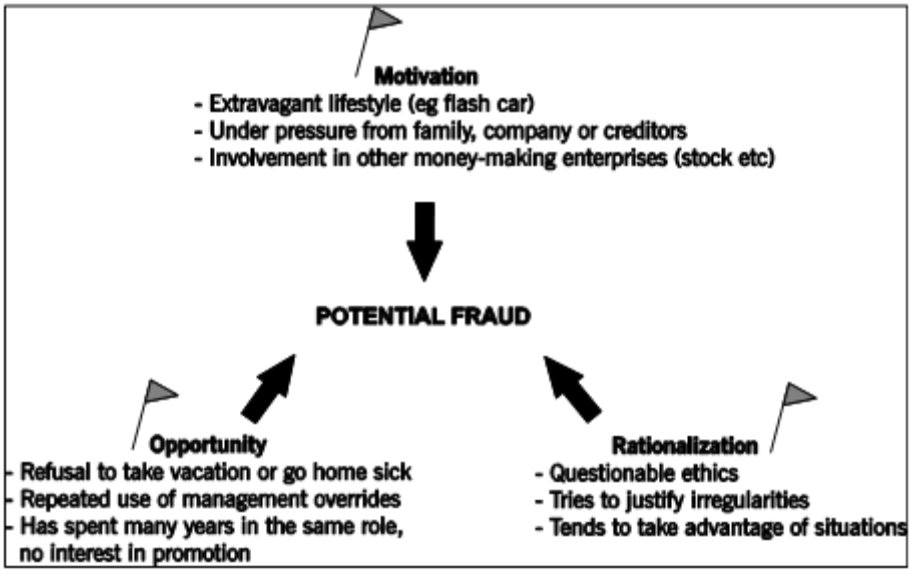
A red flag is anything which alerts an internal auditor to the potential of fraud. Note that red flags do not indicate that fraud is definitely occurring (or has definitely occurred); they are, as their name suggests, warnings only.

Auditors should remain vigilant for red flags during every internal audit engagement they carry out. Wherever a red flag is identified, further work should be carried out to determine whether fraud is likely to have occurred, or to prove otherwise.

If the investigation into the red flag leads to the uncovering of evidence which suggests fraudulent activity may have occurred, then the auditor should report this immediately to the HIA. The decision as to whether a full scale fraud investigation, or forensic audit, is required will then be made.

Perpetrator red flags

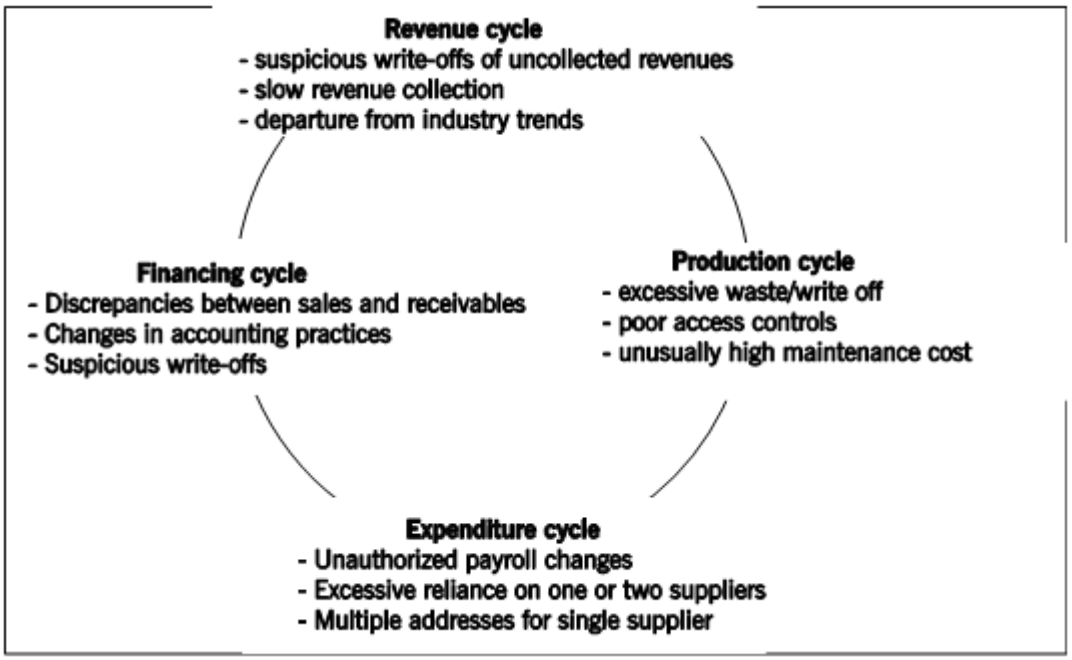
Perpetrator red flags help to indicate individuals that may be committing fraud within an organisation. Remember, in order to commit fraud, three conditions need to be present: opportunity, motive and justification. Red flags can alert auditors to individuals that are in possession of all three conditions, and so may be in a position to carry out (or already have carried out) fraud.



The size of the fraud and the position of the perpetrator are believed to be correlated, the higher up in the organisation the fraudster works, the higher the value of the fraud they tend to carry out. This is likely to be because managers have many more opportunities for fraud.

Audit cycle red flags

These red flags are characterised by the point in the audit cycle in which they are identified. Some examples are shown below



Environmental red flags

Environmental red flags indicate the conditions in the organisation's environment that make fraud more likely.

Examples include

- Intense competition and economic pressures
- Poorly regulated (or recently deregulated) industries
- Previous instances of fraud or corruption in the industry
- Cultural trends of dishonesty
- Financial pressures on the organisation
- Reorganisations (can cause disruptions to controls providing opportunities for fraud)
- Poor communication and training around the organisation's ethical code
- International organisations face greater numbers of inherent red flags due to the decentralised structure and multicultural focus

- Organisations which rely heavily on computer technology also have a number of inherent red flags due to the security issues surrounding the IT.

Industry specific red flags

The industry in which the organisation operates will influence the extent and likelihood of particular red flags the auditor may be able to observe.

The majority of frauds are carried out in four specific industries:

- **Financial services :** this is a highly competitive industry with access to huge sums of cash
- **Manufacturing :** complex processes and poor oversight can increase the opportunities for fraud
- **Insurance:** easy access to cash, and claims can be easily falsified
- **Energy:** assets can be difficult to value and profits difficult to evaluate making it easy to manipulate. Decentralised and international structures also provide greater opportunities.

Financial statement red flags

Internal auditors, as well as external auditors, may be required to look at the financial statements of an organisation. If they contain anything problematic, the organisation would generally prefer this to be identified by internal auditors and corrected, therefore avoiding any embarrassment or negative publicity that may have been suffered if the problem was left for external audit to find.

Some examples of red flags in this area include

- Highly complex transactions (may indicate creation of false revenues)
- Transactions around the period end (may indicate false revenues)
- Changes to inventory counts (affects asset value)
- Fictitious assets (again inflates the value of assets)
- Manipulation of reported results, e.g. treating an expense as an asset
- Inadequate disclosures

2.2 Design appropriate steps to address significant risk of fraud

At the planning stage of the audit, the auditor should give some thought as to what fraud risks are most likely to be encountered, so that appropriate steps can be taken to en sure suitable controls are in place to prevent frauds and identify if any are occurring.

A cost/benefit approach should be taken with this; no organisation is completely free of fraud risk. Controls should be designed to reduce the risk to an acceptably small level in relation to the investment they require and the consequences they prevent.

In order to design the procedures in such a way, auditors will need the authority to access, review and comment on all documents, policies, procedures, reports and transactions within the organisation. This right should be stated in the internal audit charter.

2.3 Employ audit tests to detect fraud

There are three types of audit tests that are particularly suitable for the detection of fraud: trend analysis, proportional analysis and electronic verification of transactions.

2.3.1 Trend analysis

Auditors analyse trends for any disruptions and then carries out further work to identify the cause of that disruption. Sometimes the cause is found to be a fraud.

2.3.2 Proportional analysis

This kind of analysis compares related data by looking at the ratio of one to the other to see if it is reasonable. If the ratio is not in line with what is expected, then further work will need to be done to establish the reasons for this. Again, it is possible that the reason could be as a result of a fraud.

2.3.3 Electronic verification of transactions

Computers allow auditors to verify much greater numbers of transactions than would be possible manually. The computer is used to compare transactions to their effects in order to highlight any unusual conditions. The unusual conditions can then be looked at further to determine if they were as a result of fraud.

2.3.4 Detection of fraud

The tests above do not detect fraud in their own right, they detect anomalies which may or may not be caused by fraud. The auditor will have to do more focused testing and research into the

cause of the anomaly to establish whether or not fraud has actually occurred. There is, in most cases, a reasonable cause for these unusual results.

If the internal auditors do detect fraud as a result of their work, they should ensure the appropriate people are informed.

The auditor should also follow-up to ensure the responsibilities of the internal audit activity have been met.

2.4 Determine if any suspected fraud merits investigation

If the internal auditor has detected a fraud as part of their work, they must then determine if this suspected fraud merits investigation. This will depend on a number of factors including the scale of the fraud, the likelihood of similar or related frauds being committed, and the cost of investigation.

3. Fraud investigation

At some point in your internal auditing career, you may be required to carry out a fraud investigation. This will involve establishing the facts and extent of the fraud and reporting the results to the relevant parties. It will also involve reviewing the processes to determine any controls that need to be strengthened to avoid the recurrence of similar fraud in the future.

The objectives of a fraud investigation are to:

- Establish the facts
- Rapidly assess the situation to stop the loss as soon as possible
- Establish the essential elements of the crime to support a successful prosecution
- Identify, gather and protect evidence
- Identify and interview witnesses
- Identify patterns of actions and behaviour
- Determine probable motives that often will identify potential suspects
- Provide accurate and objective facts upon which judgments concerning discipline, termination, or prosecution may be based
- Account for and recover assets

- Identify weaknesses in control and counter them by revising existing procedures or recommending new ones and by applying security equipment when justified.

3.1 Who should be involved?

An internal audit team should be put together to carry out the fraud investigation. The team will consist of internal auditors, legal counsel and specialist investigators.

The members of the internal audit activity selected for the team will depend on the particular fraud. For example, it may be appropriate to have people qualified in accounting, law or with specialist computing skills. If the required disciplines are not available within the internal audit activity, then sufficiently qualified outside providers should be used.

If management is suspected of being involved in the frau d, the board and audit committee should be involved as well as internal auditors, legal counsel and specialist investigators. Forensic specialists may also be included if there are possible criminal or civil actions as part of the fraud.

Once the HIA is satisfied that the team has all the necessary skills, knowledge and training to perform the fraud investigation, then they are ready to start.

The first steps are to identify the red flags and potential fraud opportunities for the activity. The existence of the three conditions of **opportunity**, **motive**, and **rationalisation** will also have to be established.

3.2 Establish the facts and extent of fraud

The following steps should be taken during a fraud investigation:

Step 1 Assess the likely level and extent of complexity in the fraud

Step 2 Determine the knowledge, skills and other competencies needed to carry out the investigation effectively

Step 3 Design procedures to identify the perpetrators, and the extent, techniques and cause of the fraud

Step 4 Co-ordinate with specialists, such as management personnel, legal counsel and others over the course of the investigation

Step 5 Be aware of the rights of the suspected perpetrator and other personnel and the reputation of the organisation itself

Just like with any other audit, the auditor will need to document the fraud investigation thoroughly.

Documentation obtained as part of such an investigation might include, amongst other things:

- The objective of the investigation
- How the investigation was carried out
- Details of how the fraud itself was carried out
- Information on the parties concerned (name, department, position, etc.)
- Details of the evidence collected
- Details of assets related to the fraud – money, property etc. and their value
- Interview and interrogation notes
- Documents, memos, photographs etc.
- Effectiveness (or ineffectiveness) of computer controls
- Relevant legal information

3.3 Report outcomes to appropriate parties

The HIA is responsible for reporting fraud and should do so as soon as the internal auditors have established with a **reasonable certainty** that fraud exists. A report to senior management and the board must be made by the HIA **immediately** once this reasonable certainty has been confirmed.

The HIA should ensure that sufficient investigation has taken place to secure reasonable certainty before any report is made. At the end of the detection process, it may also be appropriate to issue a preliminary or final report indicating the conclusion of the internal auditor, and whether a full investigation should be carried out.

This report should also include a summary of the recommendations and observations upon which they formed their conclusion.

3.4 Complete a process review

At the end of the fraud investigation, the internal auditor should

- Determine if controls need to be put in place, or strengthened, in order to reduce the chances of similar frauds occurring in the future

- Design engagement tests to help identify similar frauds in the future
- Continue to maintain a sufficient knowledge of fraud so that future indicators of fraud will be identified

4. Tools and techniques for fraud identification

There are a variety of tools and techniques that can be used by internal auditors when carrying out a fraud investigation.

4.1 Discovery sampling

Discovery sampling means the sampling of data or documents with the aim of identifying errors and irregularities.

Establishing a suitable sample size for discovery sampling can be difficult as it is hard to get a balance between a sample that is large enough to be predictive but that is also reasonable. The aim is to make the sample large enough that it should include at least one instance of suspected fraud.

The two most commonly used methods for discovery sampling are dollar-unit discovery sampling (DUDS) and random sampling.

Computer assisted audit techniques may make it possible to look at 100% of the population, rather than have to rely on samples, depending on what is being reviewed.

4.2 Interrogation Techniques

Interviewing and interrogation are not the same thing. They have different aims and also very different approaches

4.2.1 Interview techniques

Interviewing techniques were covered in detail earlier where we looked at the six step process of Interviewing, now it can be used by internal auditors to obtain information, and the importance of being relaxed, approachable and creating a rapport with one interviewee.

4.2.2 Interview behaviour red flags

When carrying out interviews, internal auditors should remain constantly alert to any **red flags** that may present themselves. There are a number of interview behaviours that have the potential to be red flags. These include

- Unwillingness to make eye contact
- Inconsistent answers that possibly contradict each other
- Restless behaviour
- Anxious behaviour
- Closed body language

As with any red flags, it is important to remember that these do not definitely indicate the interviewee is a participant in fraud or is otherwise untrustworthy; they may be sweating simply because it is hot, or they may not make eye contact because they come from a culture where eye contact is not considered to be appropriate in such situations.

4.2.3 Difference between interviewing and interrogating

If an interview is carried out as if it is an interrogation, the organisation could face legal action being taken against it. Therefore it is important for internal auditors to understand the difference.

Interviews are carried out in order to gain information. They should be comfortable and open, with questions having a logical order. They are usually held in the interviewee's own working environment.

Interrogations on the other hand aim to obtain evidence or a confession. Similar questions will be asked again and again to identify changes and discrepancies. The pattern of questioning is unpredictable. These are carried out on neutral territory and can be very confrontational at times.

4.3 Computer analysis

Audit software can be used to analyse data and identify irregularities. This can help indicate transactions which could potentially be fraudulent. The internal auditor can then look further into these transactions to determine if there is a reasonable explanation.

The two main ways computers can help are through **numerical analysis** and **regression analysis**.

Numerical analysis is based on **Benford's Law** which states that the number 1 will be the leading digit 60% of the time. Since people generally believe numbers appear randomly, their fraudulent payments would probably be numbers that break Benford's Law,

Regression analysis statistically models relationships between variables. This could be used to spot unusual transactions and irregularities.

Embedded audit techniques can also be very useful in identifying fraudulent transactions.

5. Forensic auditing

Forensic auditing is a specialist skill which involves collecting evidence that is suitable for use in court. Internal auditors are not expected to have such specialist skills in relation to fraud or gathering evidence for use in courts of law, and so experts must be used to provide this service. This is usually carried out by fraud audit teams.

Fraud audit teams are usually made up of:

- Certified fraud examiner (certification is from the Association of Certified Fraud Examiners- ACFE)
- Security investigators
- Human resources (HR) personnel
- Legal counsel
- External consultants, such as computer experts
- Senior management, except in cases where a member of senior management is suspected of involvement in the fraud

5.1 Skills of forensic auditors

As well as investigation and auditing skills, forensic auditors also need a strong understanding of the rules and standards of legal proceedings. They need to be able to both gather the appropriate evidence and then present it convincingly in court.

To be able to convey the evidence convincingly, the forensic auditor should be skilled at identifying gaps and carefully organising detailed and technical data to create the story of the fraud. This will run from the original motivation and opportunity through to how it was done and the outcome of the fraud. It should be an easy to follow story that is well supported by appropriate evidence.

The rules of evidence of the court where the case is being heard must be adhered to by the forensic auditor. The forensic auditor must also be able to prevent the evidence being lost or destroyed by the perpetrator, or corrupted in a way that jeopardizes the reliability of the evidence preventing it from being used in court.

The investigation and legal skills of forensic auditors al so makes them great consultants as they are expert at identifying potential control weakness that could be exploited by fraud perpetrators.

5.2 Electronic evidence

The information systems of the organisation can provide a variety of data that could be used as evidence in forensic reporting, including:

Financial records	Identify irregularities
Client lists	Fictional or inactive customer accounts
Email logs	Unusual correspondence
Personnel records	Many possible red flags, including employment histories, employee screening, or the lack of records of someone on the payroll can identify a ghost employee
Word documents	Unusual correspondence
Systems logs	Identify irregularities or unusual contacts
Operations logs	Unexpected activity levels
Internet history reports	Evidence of harassment or hate crime activities

5.2.1 Cyberforensics

Cyberforensics, or computer forensics, means using computer investigation and analysis to gather digital evidence for use in court.

The biggest difficulty with this kind of work is ensuring that the integrity of the data and evidence is not damaged by the investigation. This is because access to the system itself can inadvertently change significant access dates in files (e.g. date last accessed will be updated to the date it was accessed by the investigation team, rather than by the suspected perpetrator). To prevent this, investigations usually start by isolating the computer to be investigated and making a digital copy of its hard drive. The original is stored securely to retain the chain of evidence, and the investigation is carried out on the copy.

Chapter 14: Monitoring engagements

1. The need for follow-up

ISQIA 2100 Monitoring Engagement

Head internal auditors must ensure appropriate monitoring of internal audit engagement so as to ensure:

(i) Achievement of objectives

(ii) Quality assurance

(iii) Human resource development

(iv) Minimisation of risk exposure

The proficiency and experience of internal auditor and the nature of internal audit activity will determine the level and degree of monitoring activities that should be performed by head of internal auditor. It is head of internal auditor's discretion whether to delegate the review performance to an experienced internal audit staff. All evidence during monitoring must be appropriately documented and retained.

At the end of the internal audit engagement, the internal auditor will need to schedule a follow-up. The purpose of this is to establish what action has been taken against the recommendations made in the original report.

Follow-up is a process by which the internal auditors determine the adequacy, effectiveness, and timeliness of actions taken by management on reported engagement observations and recommendations, including those made by external auditors and others. Follow-up occurs at the end of the internal audit engagement.

The internal audit activity has a responsibility to follow-up on any internal audit engagements they carry out. Therefore it is necessary for the internal audit activity to have formal, published follow-up procedures in place. The requirement for follow-up is set out in Performance Standard 2500 Monitoring Progress.

There is also a practical reason for doing so. The aim of the engagement will have been to improve the effectiveness of control, improve risk management etc. This aim is not met by the issuing of the report. The improvements are only made when the findings are translated into specific actions

for management and management then carry out those actions. Follow-up allows the internal audit activity to monitor the progress and see that the changes actually take place, thereby ensuring that the aims of improved controls and risk management have in fact been met.

A further reason for follow-up is that it helps to ensure that the required action is taken by management. If management know that the engagement will be followed up, they are more likely to make the relevant changes and take appropriate remedial action against any issues identified.

To ensure management understand the audit process that they will experience during and after an engagement, the internal audit activity's **written charter** should clearly state that the activity **has the right to perform these activities.**

2. Planning a follow-up

Follow-up processes, just like audits, need to be planned. They are not all the same and the approach taken each time may be very different. Factors such as the significance of the recommendations raised in the original report, and the extent of resources required to make the recommended changes will impact on the nature, timing and extent of follow-up process that is required.

2.1 Nature, timing and extent

The first stage in planning a follow up is carried out by the HIA who will set the nature, timing and extent of follow-up required. These decisions will be affected by a number of factors:

Significance of the finding	Significant observations are those which could prevent the organisation achieving its objectives. They could have extremely serious repercussions for the company. Management should promptly establish procedures to deal with such issues. Follow-up of such matters can also be complex, therefore requiring more time and resources than for a minor issue. Minor issues will require management's response to mitigate a risk, but can be quickly and easily checked by the auditor at follow-up.
Effort and cost of correction	If the cost of corrective action the anticipated benefits, it would be better to re-discuss the issue with management to identify a more cost-effective solution.

Impact of failure of corrective action	How likely is the corrective action to be successful, and what are the implications if it fails?
Complexity of corrective action	Some audit recommendations are very simple to implement. Others may be very long and complicated. Obviously, the amount of follow-up work required to check on progress of a complex recommendation will be greater than that needed for a simple recommendation.
Timescale	Significant findings should be responded to immediately, ideally as soon as the issue is identified. This would mean corrective action is already taking place whilst the audit is still in progress. Less significant findings may be responded to over a longer time frame. Management can implement the recommendation gradually. Very minor issues may not need to be followed up at all. Such recommendations are usually revisited next time an audit engagement is carried out in that area. The timeframe for implementation should be agreed between the HIA and management along with a target date for completion when the original report is finalised.

In addition, the department will also need to consider the costs and resources required for effective follow-up.

2.2 Responsibilities

Following an internal audit engagement a series of observations and recommendations are reported. Management is responsible for deciding the appropriate action to be taken in response to those findings. The action they take must lead to timely resolutions of the observations and recommendations reported.

The head of internal auditors is responsible for reviewing the response provided by management, and this review will be done by internal auditors via the follow-up process.

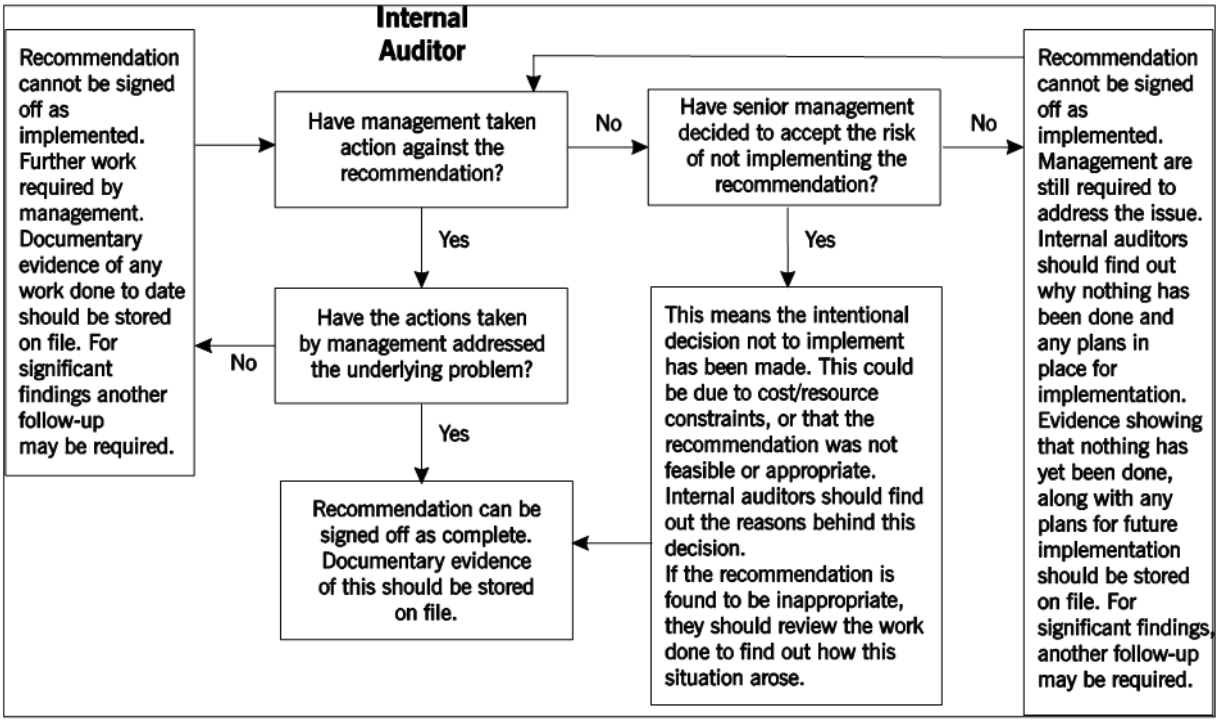
2.3 Monitoring outcomes

During the follow-up process, the internal auditor will speak to the client, and possibly operational staff, and carry out testing in order to determine what action has been taken and establish whether or not that recommendation has been implemented.

The auditor will also assess how well the initial problem observed has been addressed by the implementation of the **recommendation**.

Where it is found that a recommendation has not been implemented, the internal auditor must establish the reasons for this. They should also determine

- If there are any plans to implement the recommendation going forward. Why was it delayed?
- If any alternative remedial action was taken and the impact this has had in addressing the original observed problem.
- If the decision has been taken by senior management or the board not to implement the recommendation and assume the risk of doing so. The reasoning behind this decision should also be established.



The way that progress against recommended actions is monitored will depend on the specific change being implemented. Careful planning should be carried out to ensure this is done in the most effective way.

Issues to be considered during the planning stage include:

WHO?	Who will carry out the follow-up?	Responsibilities allocated to specific internal auditing personnel Where support is required from other areas, those areas should be contacted and efforts co-ordinated
WHAT?	What will be monitored?	Objectives of recommendation broken down into measurable, observable criteria Management must be made aware of, and agree with, the needs of internal audit. For example, if the internal auditor requires time with various members of the operational team, or if access to a specific computer system will be needed, the management must be made aware of these needs so that they can ensure staffs are available and access rights set out.
HOW?	How will it be monitored?	On-going basis suitable for some recommendations, e.g. regular update / report from management For more significant recommendations it may be more appropriate to schedule a complete follow-up engagement For more minor recommendations a questionnaire or conversation may be all that is required. Some simple recommendations can be followed-up remotely with no need to involve operational staff. For example, a requirement to make a policy available for all staff may be quickly followed-up by a search of the staff intranet.
WHEN?	When, or how often, will the monitoring take place?	Should take place after the agreed time frame and estimated completion date Urgent matters should be resolved immediately

		Large complex solutions may be made up of many recommendations and so a series of follow-up engagements may be more appropriate

3. Conducting a follow-up

Carrying out a follow-up is often in practice a little like carrying out a mini audit engagement. Just as you did then, you are required to obtain evidence, document findings and form a conclusion. This could involve carrying out a follow-up engagement, or simply receiving a periodic report from those responsible for implementing the recommendations.

During the follow-up process, the internal auditor will gather data .This data should identify progress made against the recommendations, and the timeframe in which it has been done, therefore allowing the auditor to confirm the current status of the recommendation.

Similar processes to those used in audit engagements are carried out at the follow-up stage such as data collection, interviewing, document review and so on. Similarly, the same importance is attached to building positive relationships and taking a co-operative approach during follow-ups as during audit engagements.

When carrying out follow-up activities, the internal auditor should:

- Determine whether each recommendation has been implemented, either fully or in part, or if no progress has been made against the recommendation
- Fully document any progress made against recommendations
- Assess whether the risk addressed by the recommendation is now sufficiently managed to prevent the identified problems occurring again in the future
- Identify any benefits to the area, or the whole organisation, arising from the implementation of the recommendation
- Determine whether the benefits/savings are in line with expectations.

3.1 Non-implementation

During the follow-up process, the auditor may find recommendations where no progress has been taken against that recommendation. The internal auditor must establish why this is and document those reasons.

There are a number of reasons why progress may not have been taken, including

- Management does not intend to implement the recommendation
- It has proved too difficult to implement in practice
- A change in other factors mean that the risk is now managed elsewhere and the recommendation has become redundant
- Time pressures have led to a delay in implementation of the recommendation
- The recommendation was unsuitable

If it is found that the recommendation is considered unsuitable, the underlying problems must be fully identified to prevent it happening again. If the correct procedures were followed in relation to communication and the recommendation was agreed properly with management at the time, the chances of this happening are greatly reduced.

The internal auditor should engage in discussions with management and personnel in the area concerned to determine how the recommendation can best be taken forward. This may simply mean changing the time frame, or revisiting the original problem together with the aim of developing alternative approaches for addressing the problem and implementing the recommendation.

The follow-up and monitoring processes should continue for recommendations where progress is not being made. Additional follow-ups should occur until the auditor is satisfied that sufficient progress has been made.

3.1.1 Escalating issues

The auditor may need to make a decision as to whether an issue should be escalated. This decision will be based on a number of factors.

FACTOR	Explanation	Example
The issue should only be escalated if the recommendation is still valid	There may have been a change in conditions which has removed or reduced the risk, or significantly changed the solution requirements.	A new IT system may have been introduced which has built in controls where the old one did not. This may mean that the additional manual controls originally

		recommended are no longer needed.
If the objectives of the recommendation were met by an alternative approach there is no need to escalate	Management may have decided to make a change different to the one laid down in the recommendation which has achieved the same effect.	A recommendation to have two Members of staff opening post in a fulfilment house (to prevent theft) may have instead been addressed through the installation and monitoring of CCTV cameras.
If nothing be done to convince management to implement the recommendation, then escalation may be necessary	Before escalating an issue, the recommendation and the underlying problem must be fully discussed with management, and all possibilities of agreement exhausted.	Management may be more likely to give the desired approach if they have been helped to fully understand • the costs of the risk • the benefits of addressing the risk including the ancillary benefits of the recommendation • the financial costs of not implementing the recommendation
Should implementation be delayed? If so, escalation of the matter may not be appropriate	There could be a planned change pending which may make it more beneficial to implement the recommendation once that change is complete.	If a number of recommendations relating to payroll and HR have been made, and at the same time there are plans to install a new integrated IT system (to replace the two separate systems currently in place), it may be better to delay implementation until after the new system has become operational.
If the recommendation is key to resolving issues of	If it is not key, the HIA may decide to sacrifice that one recommendation in	If a department is facing staff Shortages, there may not be sufficient resource to implement all

control in this area, then escalation may be appropriate	favour of securing management agreement to implement a more critical recommendation.	the recommendations. In such cases, the most significant recommendations should be prioritised.
If the recommendations can be revised in any way to make them more achievable, then this should be done, rather than escalating the matter	If a recommendation is perceived to be more achievable, it will be viewed more favourably by management and it is more likely that it will be accepted.	If the department is taking short-cuts due to staff shortages, it may not be able to implement your recommendation to carry out the processes in full. However, suggesting the use of contractors, or outsourcing certain processes, may be much easier for the managers to implement.

These six questions highlight the importance of communication between internal audit, the HIA and management. A strong level of communication is necessary throughout the entire audit process, including planning and carrying out monitoring and follow-up activities.

3.2 Stopping monitoring

As mentioned above, additional monitoring and follow-up activities will be scheduled if the recommendation has not been fully implemented.

Monitoring of a recommendation may stop when:

- Recommendation is fully implemented (or the objectives of the recommendation are met in an alternative way)
- The problem no longer exists. This may occur for ex ample if a new system is purchased which does not have the inherent control issues in the old system over which additional controls were recommended.

When a recommendation reaches this stage and no longer requires follow-up, it is vital to ensure it is removed from the list/database of ongoing re commendations when appropriate.

4. Communicating the results

ISQIA 8000 Reporting and communication

The conclusion reached by internal auditor from internal auditor activity must be communicated to appropriate authority.

Just as the results of the initial audit engagement have to be communicated, so too do the results of the follow-up process.

The HIA is responsible for reporting the outcome of follow-up activities to senior management and the board.

In practice, the HIA often meets the reporting requirement by doing so in person at audit committee and senior management meetings. At such meetings the HIA will usually report:

- Planned audit engagements
- Any ad-hoc work undertaken and its results
- Audit engagements in progress
- Audit engagements completed and their outcome
- The results of follow-up activities carried out

The follow-up report should specifically document the results of the monitoring plan and highlight the benefits achieved for the organisation as a result. These results should link directly back to the criteria in the original recommendations.

The report should be a one-page summary of objectives, monitoring activity and results with supporting information and evidence listed in appendices.

Any other issues that impacted on the implementation of the recommendation, caused changes to be made to the recommendations, or highlighted new or related risk or control issues, should also be fully disclosed in the report.

4.1 Inadequate management response

Where the internal auditor feels that the management response has not been adequate (for example management disagree on the need for, or the urgency of, the recommendation), the HIA should first discuss with management the reasons for the recommendation. This will involve highlighting the underlying risk and problems, and encouraging management to respond to the

recommendation. The HIA may need to move higher up the layers of management to achieve this.

If the recommendation relates to a significant risk to the organisation then the HIA is obliged to escalate the matter. This could go right up to senior management, and eventually the board if a suitable response is not achieved.

Achieving an adequate response from management will be more likely if care is taken at the time of the original engagement to ensure that recommendations are addressed to individuals with sufficient authority and ability to make the changes.

APPENDIX: International Standards for Qualified Internal Auditor (ISQIA)

This publication was prepared by the IQN. Its mission is to serve those adopting *International Standards for Qualified Internal Auditor (ISQIA)* for organisational governance, strengthen the worldwide internal auditing profession and contribute to the development of strong international economies by establishing and promoting adherence to high quality internal audit standards. This publication may be downloaded free-of-charge from the IQN website http://www.iqnuk.com. The approved text is published in English language. IQN welcomes any comments you may have regarding internal auditing standards. Comments may be emailed to admin@iqnuk.com.

International Standards for Qualified Internal Auditor (ISQIA)

TABLE OF CONTENTS

1000. Principles and responsibilities

1100 Objective of International Standards for Qualified Internal Auditor (ISQIA)

- To outline the scope and functional requirements of internal auditing activities
- To interpret the terms and definitions used in the statement of standards

1110 Concepts and definitions

Internal Auditing

Internal auditing is an independent scrutinisation, analysis and monitoring of activities related to an organisation's operation internally.

Internal Auditor

Internal Auditor is a person who performs the activities of internal auditing.

1200 Code of professional conduct for Internal Auditor

Fundamental principles of professional ethics applicable for an internal auditor are:

1) Integrity;
2) Objectivity;
3) Due Professional Care; and
4) Confidentiality

2000 Supervision

Effective management of internal audit activity should contribute organisation's functional enhancement. Administration and monitoring of such activities is the responsibility of the head of internal auditor.

Organisation's functional enhancement is ensured when internal audit assurance is objectively rendered, establishment of good governance, effective and efficient risk management processes, control procedures with internal audit personnel complying with the Code of Ethics and the Standards (ISQIA).

2100 Monitoring Engagement

Head internal auditors must ensure appropriate monitoring of internal audit engagement so as to ensure:

(i) Achievement of objectives

(ii) Quality assurance

(iii) Human resource development

(iv) Minimisation of risk exposure

The proficiency and experience of internal auditor and the nature of internal audit activity will determine the level and degree of monitoring activities that should be performed by head of internal auditor. It is head of internal auditor's discretion whether to delegate the review performance to an experienced internal audit staff. All evidence during monitoring must be appropriately documented and retained.

2200 Administering resources

In order to achieve set plan and objective of internal audit activity, sufficient level of knowledge, skills and competencies are required in order to be able to utilise available quantity of resources effectively**.** The head of internal auditor should ascertain that availability of resources is adequate and effective.

3000 Planning Engagement

Internal auditor should prepare and document each engagement plan. In particular, the objectives of engagement, scope of engagement, timing and allocation of resources.

Several engagement plans must be separately developed and documented. These should include engagement's objectives, its scope, timing, and allocation of resources.

3100 Planning Considerations

The principal considerations for internal auditors with regards to engagement planning must include objective activities under review, evaluation of control procedures. Internal auditor's engagement planning considerations should also span areas of significant risks associated with engagement activity, its objectives, resources, and operations including ways to keep risks under a satisfactory level; the sufficiency and effectuality of the governance, risk management, control processes equated to an applicable framework or model and the opportunities for improvement.

Third party engagement planning: Internal audit objectives, scope, responsibilities, ranges of expectations, distribution of internal audit engagement outputs and accessibility to records should all be planned, agreement with clients and must appropriately be documented by internal auditors.

Consultation engagements: Internal audit objectives, scope, responsibilities, ranges of expectations, distribution of internal audit engagement outputs and accessibility to records

should all be planned, agreement with clients and must appropriately be documented by internal auditors.

4000 Performing Activities

4100 Corporate Governance

The management and the board should have set standards for organisation's corporate governance, management of risks and controls. This is to ensure the achievement of objectives and goals. In absence of such standards, internal auditors must collaborate with the management and the board to establish suitable standards.

4200 Risk Assessment

The internal auditors and internal audit team must not take part in the management processes of risk mitigation. Management responsibilities should be avoided during risk assessment engagements.

Internal auditors should establish engagement objectives that must reflect output from initial risk assessment process for internal audit activity.

4300 Control Activities

The internal audit activity should execute feed-forward control system to identify and appraise possible existence or occurrence of fraudulent activities. The activity should also cover the appraisal of organisation's own process of identifying fraudulent activities.

Controls within organisation must be evaluated in terms of effectiveness and efficiency and appropriate recommendations for scope of improvement must be identified and communicated on timely basis to senior management and the board.

Internal auditors must clarify the facts of the existence of risk associated with engagement objectives and any other considerable risks identified, during consultation engagements. Organisation's risk management procedures should then be identified and appraised.

The internal auditors and internal audit team must not take part in the management processes of risk mitigation. Management responsibilities should be avoided during risk assessment engagements.

5000 Gathering and analysing data

To ensure successful achievement of engagement's objectives, it is required for internal auditors to identify, analyse, evaluate, and document sufficient, reliable, relevant and useful engagement information.

Internal auditors must obtain good quality engagement information. Good information refers to its relevance, completeness, accuracy, and clarity to internal audit engagement. The information must be reliable and should be manageable and appropriately communicated in a timely fashion that meets the internal audit engagement objectives. The benefits of obtaining such information should exceed its expenses.

Internal auditors must engage in analysis and evaluation to establish a form of base for supporting audit opinions and conclusions.

Methodical documentation of appropriate engagement information should be the basis of conclusions and engagement results reached by internal auditor. Engagement information should therefore be restricted in terms of accessibility and controlled by head of internal auditors. Head of internal auditor must formulate information retention, custody, and requirements policy.

Internal audit activity should be set on priority basis which is responsibility of the head of internal auditor. Audit programmes are based on types and levels of risk associated with internal audit engagements, types of organisation and objectives of organisational goals.

The responsibility of developing a risk-based assessment plan is the sole responsibility of the head of internal auditor. Risk-based engagement plan are to be developed on the basis of organisation's risk management framework, levels of management's risk acceptability for every different functional and operational activities. In situation where there is no risk management framework exists, head of internal auditor must exercise own judgement supported with information from senior management and the board. The head of internal auditor must review and correct, as necessary, in response to changes in the organisation's business, risks, operations, programmes, systems, and controls.

There must be detailed methodologies for the guidance of the internal audit activity. The set methodologies are to be established by the head of internal auditor giving appropriate considerations about the size, extent and structure of the internal audit activity and the complexity of the assurance engagement.

The head of internal auditor is obligated to convey or communicate the internal audit engagement plan, appropriate resources availability and its impact if unavailable. Any significant changes during the period of engagement must be communicated with the senior management and the board. Management and the board in turn should thoroughly review, approve and allocate resources accordingly.

6000 Risk and governance

The internal audit activity must review existing practices of governance procedures and be able to recommend ways of improvement. Organisational governance procedures aims in establishment of appropriate promulgation of organisation specific ethical stances and the extent of values placed in. Effective governance procedures should also ensure reliability in performance measurement, accountability, risks identifications and timely flows of information between senior management, boards, internal auditor and external auditor.

Internal audit activity must consider evaluating the organisational risk management policies and procedures in order to recommend suitable improvement.

Sufficient information relating to risk exposures should be obtained and analysed through number of internal audit engagements within the organisation. The analytical output should provide an overall understanding of the organisations risk management procedures. In order to assess efficacy of the risk management process, internal audit activity should ascertain:

- Whether organisation's strategic objectives and mission are adjuvant
- Whether material risks elements are sufficiently identified and evaluated
- Whether safeguards against risks are identified that are suitable to organisation's risk appetite
- Whether relevant risk information are identified and communicated in timely manner to the personnel associated with it. This would aid in carrying out appropriate responsibilities to minimise risks.

The Head of Internal Auditor should understand that key exposures to risks within organisation are:

- Governance: Risks those are detrimental in the achievement of organisation's strategic objectives, risks of not complying with laws, regulations, policies, procedures, and contracts.
- Operations: Risks of not relevant measures for safeguarding of assets

- Information systems: Reliability and integrity of financial and operational information may not be steadfast

Operations and programmes may not be effective and efficient to serve the purpose of achieving organisational strategic objectives

7000 Working with others

7100 External assessments

External assessments must be conveyed at least once every 3 years by a professionally qualified, independent, assessor or assessment team from an external professional assessment provider. The head of internal auditor and the board must develop policy for the pattern and frequency of external assessment, qualifications and level of independence of the external assessor or assessment team and identify any probable conflict of interest.

External assessments can be either in the form of 'complete external assessment' and/or externally verified self-assessments.

The head of internal auditor must use his professional judgement to assess whether an external assessor is satisfactorily qualified in terms of academic knowledge and possesses relevant, appropriate practical knowledge. The head of internal auditor should focus on the external assessor's experience in terms of knowledge of business, similar size business, functional and operational complexity, sector or industry, and technical issues. Assessment team are expected to have such knowledge and experience as a whole not merely all members are required to possess the required level of expertise.

7200 Interaction with other departments

Head of internal must formulate a policy to be followed by the internal auditor teams when interactions with other departments are necessary for information collection, facts verifications, etc. Head of Internal auditor must then train-up and provide appropriate guidance in a feed-forwarding approach.

7300 Outsourced Internal Audit service

It is the responsibility of the organisation to maintain appropriately sufficient and effective internal audit activity when such activity has been outsourced to an external audit firm or service provider.

8000 Reporting and communication

The conclusion reached by internal auditor from internal auditor activity must be communicated to appropriate authority.

The followings aspects must be taken into account during the issuance of overall opinion and should include:

- Expectations of senior management
- The management board
- Key stakeholders and users of the information
- The possible prospects of senior management, the governing board and relevant stakeholders should be considered by the internal auditors when providing opinions and conclusions.

Communication benchmarks must include such contents as:

Engagement's objectives, scope of engagement, conclusions, recommendations, and appropriate action plans.

Internal auditors must provide his opinions and conclusions during final communication of engagement results. The possible prospects of senior management, the governing board and relevant stakeholders should be considered by the internal auditors when providing opinions and conclusions. Opinions may be provided through ratings, conclusions and any form of descriptions of the outcome from internal audit engagement.

Internal auditors are expected to disseminate engagement communications successfully.

Internal auditors must state the presence of limitations on distribution and usage of the results in time of communicating engagement results to third parties outside the organisation.

Developments and outcomes of consulting engagements may be communicated in a manner most suitable for the nature of engagement and requirements of the users.

The quality of communications must possess attributes so that it is accurate, objective, clear, concise, constructive, complete, and timely.

Communications are accurately made if it does not incorporate errors, misstatement, or distortions and based on relevant facts. Objective communications takes into account all relevant facts and conditions and are assessed on the basis of fairness and impartiality and are free from bias and prejudice.

Communications are clear when significant, relevant information is understood easily with logical approach; any technical jargons should be avoided. Concise communications avoids irrelevant wordiness, excess detail, repetition; only 'to the point' information are used for communications. Constructive communications assists engagement clients and the organisation by identifying areas of development and improvements. Communications are complete when it includes only information that are significant and appropriate; it should be a reference to all recommendations and conclusions reached and are meant for appropriate audiences and users. Timely communications are practical and advantageous for consulting engagement, risk assessment, or other engagement issues that allows management to take suitable remedial and corrective actions.

9000 Observation and control

Senior management and the board must be kept informed with current progresses and required changes as following internal audit activity. Therefore, the head of internal auditor should prepare timely report focusing on the purpose of internal audit activity, the level of authority, responsibilities of internal audit staffs and evaluation of performance. It is important to highlight any divergences from the initial internal audit engagement plan. The report should also include identified risk factors, possible fraudulent activities, governance issues and any particular requirements of senior management and the board.

The head of internal auditor must design and execute a monitoring system when results are being communicated to organisation's management.

If significant errors and / or omissions are discovered in the end results and conclusions, the head of internal auditor must amend, if required, and communicate the adjusted or actual information to all affected parties possessing the original communication.

Internal auditors may report that their engagements are "Conducted in conformance with the International Internal Auditing Standards for the Professional Practice", should the results and conclusions of the quality assurance and enhancement programme are in agreement with the report statement.