The process of control self-assessment and its use in risk management

L du Plessis
Department of Accounting
University of Pretoria

GP Grobler
Department of Accounting
University of Pretoria

Abstract

Organisations are exposed to various forms of risks. Business risk is the threat that the objectives of an organisation will not be achieved. Management is responsible to address the risks facing the organisation. Management should identify the risks that threaten the organisation and ensure that the total level of risk is reduced. Management makes use of the internal audit function to assist them in the risk management process. The methods used to identify and evaluate risks will differ. One method frequently used, is control self-assessment. This is an approach used to actively take responsibility and ownership for developing, assessing, maintaining and monitoring controls to address business risk.

This article will show that it is the responsibility of the management of an organisation to control and manage risks and that the internal audit function can assist management with this process through the use of control self-assessment. The process, various methods and tools used for control self-assessment, will also be discussed.

Key words

Risk management
Self-assessment

1 Introduction

In today's competitive world it is becoming increasingly difficult for an organisation to produce good results. The reason is the growing global market in which organisations do business. This larger market presents more opportunities, but it is also more complex. Furthermore, it has a larger potential for matters to go wrong. It is in this changing environment that an organisation must be able to survive. Each organisation should accept a degree of risk to ensure its survival. However, to really flourish, opportunities should be utilised (Sparrow 1998).

According to Schneier and Miccolis (1998), most business decisions are taken by comparing risk and return. Shareholders expect companies to produce a return on the investments that they have made. Risk can, however, cause the performance of an organisation to be less than desired and result in the failure of the organisation. On the other hand there is no return without risk!

Current and potential risks should be managed proactively. This can be done in the following ways: by controlling it, accepting it, insuring it and avoiding it (Anonymous 1997). Recent reports on corporate governance, such as the Cadbury Report (1992) in the United Kingdom and the King Report (1994) in South Africa, put the responsibility for the management of risk squarely on the shoulders of senior management and the board of directors. If senior managers fail to manage risk properly, they are failing to fulfil their fiduciary responsibility. To manage risk effectively, a structured approach is required.

The purpose of an internal audit function in an organisation is to assist management in the discharging of their responsibilities. The definition of internal auditing of the Institute of Internal Auditors (The institute of Internal Auditors, 1999) is as follows:

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.

Although management is responsible for the management of risk in the organisation, they do not always dispose of the necessary tools to accomplish this responsibility. As seen in the definition of internal auditing, it is the internal audit department's task to improve the effectiveness of risk management. Internal auditors use a number of tools to identify risks and improve controls to reduce these risks. A new technique was developed by the internal audit profession to assist them with this task, namely control self-assessment (The Institute of Internal Auditors, 1996).

Control self-assessment is a process whereby various role-players in an organisation is brought together to identify and address risks relevant to their environment. Internal auditors facilitate this process.

The purpose of this article is to emphasise the importance of risk for an organisation and the management of risk. It illustrates how control self-assessment can be applied in the risk management process and emphasises that it is a very effective risk management tool. It will also illustrate the involvement of the internal auditing function in this process.

2 Risk

2.1 Introduction

To manage risk, the organisation must have an understanding of the concept of risk in general, the specific risks that threaten the organisation and the risk management process.

2.2 Definitions of risk

Some dictionaries describe risk as the possibility of an accident or loss occurring, or as a potential threat. To take a risk, means to act despite the danger or loss that could possibly accompany it. Risk is also the presence of uncertainty, i.e. uncertainty about an event occurring that could cause a loss, as well as uncertainty about the result of such an event.

For purposes of this article, attention will be focused on **business risk**. The following are examples of definitions of business risk:

- The threat that an event or action (as well as the lack of action) will have a negative effect on the ability of the organisation to achieve its business objectives and to execute its strategies effectively (Arthur Andersen 1998).
- Any threat to the success of the organisation that will have unavoidable financial consequences (Colbert 1995).
- Risk is the probability that an event or action may adversely affect the organisation or activity under audit. (The Institute of Internal Auditors 1995).
- The possibility that something will go wrong to prevent (directly or indirectly) the achievement of specific business objectives (Schneier and Miccolis 1998).

Although these definitions of risk differ, most have one element in common, namely that risk holds a threat for the achievement of the objectives of the organisation. Management should identify the risks that threaten the organisation and ensure that the total level of risk is reduced.

2.3 Types of risks

One method of classifying risks is to categorise them as external and internal risks. **External risks** are usually difficult or impossible to control. They include risks such as economic factors (for example inflation rate and petrol price), the financial markets (for example exchange rates and share prices), regulatory factors for example legislation, import restrictions and regulations) and the

actions of competitors. **Internal risks** arise as a consequence of an organisation's own activities, processes, products, contractual obligations or relations with employees, clients, providers and the environment. Examples of these are the use of technology, information and employee satisfaction.

There is a very large variety of risks to which an organisation can be exposed. One of the most comprehensive lists of risks is contained in Arthur Andersen's business risk model (Arthur Andersen 1995). In terms of this model, risks are divided into three main categories, namely environmental risks, process risks and risks that are related to the information that is used in decision making.

This model is very comprehensive and most risks that can be envisaged can be classified in terms of it. The model appears in annexure 1.
Another framework that can be used to identify various types of risk is change (Puccinelli 1998). Any type of change within or outside the organisation always brings about a variety of risks, because it presents something new. Consider, for example, the following:

- A change in the regulatory environment;
- political change that affects the organisation;
- new staff that are appointed, or a change in management;
- new information systems or other technology;
- new products and activities;
- extensions, such as branches abroad or decentralisation of activities.

There are also a number of **other risks** that can have a detrimental effect on the achievement of an organisation's objectives. The first risk involves people (Update 1998). Many organisations consider the appointment of the right people to be a critical factor in the achievement of objectives, but on the other hand they do not consider the loss of members of staff to be a risk. A lack of expertise is a worldwide problem. In Germany there are 100 000 vacancies in the field of information technology, while the figure in America is about 346 000 (Leithhead 1998).

Other risks that also involve staff concern their health and safety (Waterman 1995), the risk of inappropriate sexual behaviour (Update 1997) and risks that are associated with new labour legislation.

According to Grobler and Du Plessis (1998), fraud and other forms of crime are increasingly becoming a social problem. It is economic crime in particular that is increasing daily.

One of the risks that is possibly addressed very seldom in an organisation is the risk that is related to poor management (Sawyer 1998). Poor management and poor management decisions can give rise to many other risks in the

organisation.

According to Dimartini and Mcanally (1997), the risk of natural disasters or *Acts of God* should also be borne in mind, especially if the products of the organisation are exposed to such risks or if the location of the organisation increases the risk.

The risk that the organisation can have a negative impact on the natural environment (De Villiers and Vorster 1995), as well as the consequences thereof, is of great importance. The increasing awareness of environmental issues and the impact that organisations have on the environment has had the effect that organisations are expected to act with greater social responsibility (Teets, Kuhnke and others 1994).

Another important risk is the risk that emanates from the use of information technology (The Institute of Internal Auditors 1991). Information technology is a critical part of all business activities. In the present era, an organisation can not ignore the risk that results from the use of information technology. Other business risks can also arise as a consequence thereof. Consider in this regard the risk that computer systems can be damaged, data lost or processing of data interrupted.

2.4 The risk management process

To manage all the diverse risks facing the organisation, a structured approach is required. The methods that are used to identify and evaluate risk differ from one organisation to the next. An organisation should investigate all systems and processes to ensure that all risks and potential risks are identified. The following model of the management of risk was compiled from various literature sources (Arthur Andersen 1999, ABSA 1999, PricewaterhouseCoopers 1999, The Institute of Internal Auditors 1996):

Identification of risks that threatens the success of the organisation
▼
Analysis and classification of the identified risks
▼
Determination of the source of the risks
▼
Evaluation of the impact and extent of the risks
▼
Addressing the risks by means of control procedures In operation
▼
Ongoing monitoring

2.4.1 Identification of risks

The term *risk identification* is self-explanatory. It is the basic process of indicating risks and potential risks (Technikon Pretoria 1999). Because changes in the internal and external environment of each organisation occur constantly, management should continuously identify risks.

Risk identification is a systematic and logical process, but it also requires insight and imagination on the part of the participants. The following techniques can be used to identify risk areas:

1 Previous internal and external audits that have been executed;
2 internal auditor's knowledge (experience and training);
3 problems in similar organisations and industries;
4 industry, market and financial trends;
5 discussions with the external auditors;
6 applicable rules, legislation and regulations;
7 analysis of financial and operating data;
8 interaction between management, directors and employees.

2.4.2 Analysis and classification of identified risk

It should be determined which areas of the organisation are affected by the various risks. The similar risks are then grouped together.

2.4.3 Determination of the source of the risk

The origin of risks can be internal or external. Normally management has more control over risks that originate internally than risks that originate externally. To address risks effectively, it is therefore necessary to determine the source of each identified risk.

2.4.4 Evaluation of the impact and extent of the risk

The evaluation or measurement of risk comprises the determination of the extent (how regularly it occurs or can occur) and impact (placing of a value on the damage that is caused or can be caused). It is not cost effective or possible to eliminate risk completely. The assessment of risk offers management the opportunity to reduce risk to an acceptable level.

Risks that are identified can be represented on a graph. See annexure 2 for an example.

2.4.5 Addressing risk by means of internal control procedures

The designing and implementation of internal control procedures to reduce risk will be determined by the allowable limits of risk that are laid down by management. These limits are determined by among other things:

1 The number of errors that management will accept;
2 the extent of the losses that are permissible;
3 the organisation's objectives;
4 the extent to which management accepts risk;
5 the ability to assess the risk; and
6 the cost versus the advantage of controlling risk.

Less critical risks can be addressed with the aid of detective control procedures, because they are usually cheaper to implement.

Low risk is normally not addressed, because it is not cost effective to implement proper internal control measures for them.

2.4.6 Ongoing monitoring

The ongoing monitoring of systems, activities, processes, etc is also important, because circumstances (can) change regularly and (can) also cause risks to change. The internal auditor can fulfil a very important role in this regard. Comparison with the best practices or *benchmarking* can be applied to facilitate this task. The latest trend is, however, to assign this responsibility to the manager(s) of processes (usually line management), i.e. the person who knows the process best should monitor the risk controls.

A schematic representation of the risk management process appears in annexure 3.

2.5 Various approaches to risk management

The risk management process can be approached in different ways. A number of models have been developed and documented by various organisations' internal audit functions. In the following paragraphs a number of models for the management of risk are briefly discussed.

2.5.1 The Arthur Andersen model

Arthur Andersen (1999) developed a specific methodology for identifying and addressing risk. The process comprises the following steps:

1 Define objectives;
2 identify important risks;
3 assess the extent and impact of these risks;

4 determine the extent to which these risks are currently controlled as well as the possibility of improvement;

5 determine how urgently improvement is required;

6 design and implement management and control processes; and

7 continuously evaluate and monitor the processes and compare them with the best practices.

The model is based on business processes. Most organisations are divided into various functions, for example purchases, marketing and production. The final product, namely products and/or services, are usually the sum of various combinations of two or more of the activities of these functions (functional groups). A process therefore comprises various activities that occur in various functions.

2.5.2 The PricewaterhouseCoopers model

This model (PricewaterhouseCoopers 1999) is similar to the above model, except for a few differences in respect of the method of risk identification and assessment. The following table contains a summary of the method, objective of the activity and the outputs obtained.

Method	Objective	Output
Workshop in which the knowledge of the group (usually decision makers) is used	Identification and systematisation of risks by means of voting	Systematised list of risks (from important to unimportant risks)
Questionnaire or investigation to revise management and business processes	Identification of controls to reduce risk	List of key controls linked to syste-matised list of risks
Workshop or questionnaire	Identification of processes being used	List of activities in various processes
Questionnaire	Testing of controls in operation and assessment of effectiveness	List of controls in operation and shortcomings
Workshop or questionnaire	Confirmation of effectiveness of controls in operation	List of risks that are not controlled

2.5.3 Model for the determination of risk in the execution of internal audits

Because the internal audit division usually has too few members of staff and they are overworked, it is not always possible to audit all the activities of an organisation meaningfully and regularly. Some organisations do not have access to the latest technology for the identification and assessment of risks. According to Reding and DiGirolamo (1994), the following steps can be applied to determine which activities should be audited urgently, and which should receive attention at a later stage.

1 Recognition of audit opportunities. This knowledge can be gathered in several ways, for example enquiries made with managers of business processes and the study of management's formal policy and procedures.

2 Specification of the audit design. A specific audit is designed that accords with the business processes of the organisation and is understood by both the auditor and management.

3 Definition of the statement that is to be tested. It is the auditor's interpretation of processes, expressed in quantitative and verifiable terms. Criteria in terms of which statements are assessed, include particular organisational standards, industry standards, previous assessments and assessment of similar regions.

4 Determination of the consequences if the statement proves to be false. The auditor should now identify the risks for the organisation (impact of the risk). Aspects such as costs, client service, time factor and legal aspects should be considered. If possible, these consequences should be expressed in measurable terms.

5 Determination of the possibility that the statement is false. The auditor should also consider the extent to which the statement is indeed a risk (extent of the risk). Factors that increase and decrease the possibility should be considered, for example the environment, control procedures and policy.

6 Deciding whether the statement can be audited. Taking resources, other priorities, knowledge of the audit staff, use of specialists etc into account, a decision should be taken on whether or not the statement should be audited. The cost related to the audit is a very important factor. Questions such as the availability of audit evidence and where the audit should be executed should be answered.

2.5.4 Model for risk assessment in the public sector

The Auditor-general in Texas, USA, designed a model for risk assessment in the public sector (Arnold 1997). However, this risk model is designed in such a way that it is possible to focus simultaneously on the planning and fieldwork phases of the investigation, thereby saving time. The steps briefly comprises the following:

1 Definition of risk and controls in respect of auditable environments (divisions, departments etc). Determination of what should occur or not occur to ensure the continued existence of the audit environment. Also determination of the controls in operation to ensure the outcome.

2 Identification of risks in terms of measurable criteria. The activities, actions etc that should occur or not occur to ensure the continued existence should be expressed in terms of measurable criteria at this stage. The risks related to each criterion are specified.

3 Incorporation of previous knowledge of the auditable environment. All available information is used to identify and analyse the risks. For example, information gathered in the course of previous audits and events that occurred in the past year(s).

4 Designing a risk profile of the environment. All the previous steps are used to create a risk profile of each auditable environment.

5 Arrangement of the various areas from high to low. Because there are usually a large number of auditable environments in any public entity, the auditor should first audit the most critical areas. The areas should therefore be arranged from high-risk areas to low-risk areas and attention given to the high-risk areas

3 Control self-assessment

3.1 Introduction

There are various models that can be used in the risk management process. The internal auditor uses different tools to assist in this process. Control self-assessment is one of the tools used by management during the different steps of the risk management process. It is therefore important for management to have an understanding of the concept of control self-assessment in order to support the process. The techniques used for performing control self-assessment will also be discussed.

3.2 Definitions

Various definitions have been used in this regard, for example:

□ Control self-assessment is a technique used by bringing together

individuals in natural work to evaluate the effectiveness of business process groups and focusing the work group teams on the assessment of steps necessary to assure the achievement of business objectives.

(The Institute of Internal Auditors 1996)

- An approach that refers to the actions by an organisation's management within the realm of sound Corporate Governance, to evaluate for themselves the set of organisational rules and regulations (written or verbal) that establish and define the boundaries and guide people how to behave inside these boundaries in order for the entity to be successful, related to internal control and risk management systems and the achievement of objectives, with a view to implementing appropriate remedial action whenever deficiencies are identified.

(CNA Gallo Ltd 1997)

- A leading edge process which yields reliable, quantitative information regarding achievements of operational, financial reporting and legal compliance objectives.

(Deloitte & Touche 1997)

- Control self-assessment is the process whereby line management actively takes responsibility and ownership for developing, assessing, maintaining and monitoring controls to address business risk.

(PricewaterhouseCoopers 1999)

The following can be deduced from the above definitions:

1 It is a process or technique;
2 in which individuals and/or management are brought together;
3 management assumes responsibility for the process; and
4 the focus is on risk management, internal control and the objectives of the organisation.

It is important that management should support this process. If it does not, the entire process will be a waste of time and money. Management should be prepared for the process, in order to realise that they are not usually control specialists. They are the owners of control in the organisation and should therefore identify the various role players that are indeed specialists and allocate tasks to them.

The following questions should first be answered affirmatively by the organisation before control self-assessment can be implemented successfully:

1 Are we ready for control self-assessment?
2 Will the information gathered in the control self-assessment be reliable?

3.3 Process

According to Crawford (1999), the implementation of the process of control self-assessment will depend on the specific motive. It can comprise one of the following:

1 Risks (identify, control and monitor the risks that threatenthe organisation);

2 control (study of the existence of various aspects of control);

3 processes (study of business processes necessary to achieve a specific aim);

4 objectives (determination of objectives for the organisation at the micro and macro levels).

This article only focuses on the risk-based approach. The steps in the process are discussed in paragraph 2.4 above. The execution of the self-evaluation process comprises the following:

3.3.1 Planning and preparatory work

According to the Institute of Internal Auditors (1996), this is a critical part of the implementation of control self-assessment. One of the most important aspects that should be addressed in this regard is that primary and various secondary objectives for a specific risk area should be indicated in advance. It gives structure to the workshop or interview conducted or the questionnaire administered.

The following are also important matters to bear in mind:

1 Determine a time schedule and adhere to it.

2 Make the people concerned aware of management's support for the process.

3 Communicate to the participants in advance the matters that should be discussed so that they can obtain the required inputs from other employees who will not be participating in the process.

4 Ensure that all participants know what is expected of them and that they have the necessary knowledge to be actively involved, for example if technology is to be used.

5 Use the best method for the particular situation.

6 Plan in advance who should participate, when it should occur and which method is to be used.

3.3.2 Techniques for performing control self-assessment

The following are some of the techniques that can be used to gather the information needed to manage risks. For each of the techniques discussed the most important advantages and disadvantages are listed.

Interviewing:

According to Grow Consulting (1999), interviewing is the best method for obtaining information in respect of the areas in which the organisation could be exposed to risks. However, a thorough study requires more than the use of interviews and other techniques should therefore also be used. The following are the advantages and disadvantages of the use of interviews:

Advantages:

- Because the interview takes place in a face to face situation, it is possible for the interviewer to "read between the lines" and to obtain the complete message and not merely the words or sentences.
- The interviewer can verify the information obtained, ensure that he or she understands it and encourage the interviewee to provide more information.

Disadvantages:

- The time required for individual interviews can be costly.
- The success of the interview mainly depends on the capability of the interviewer.
- If the interviewer makes assumptions and does not ensure that the information is correct and that he understands it correctly, the outcome of the interview can be misleading.
- The interviewer could be prejudiced or have fixed ideas.
- The interviewer can influence the interviewee by means of his bearing, attitude, tone of voice, expressions etc.

Questionnaires:

According to ABSA (1999), questionnaires can be used to reveal important information that can then be investigated in greater detail by means of another technique. Questionnaires are used in the following situations:

- When there are many similar divisions, departments etc;
- limited resources;
- other methods are impractical;
- large quantities of data must be processed to determine risks; and
- time is an important factor.

The following types of questionnaires and methods to compile these questionnaires, can be used, namely:

- hand driven questionnaires;
- computerised questionnaires, namely internet, e-mail and disk;

- internal control questionnaires;
- questionnaires compiled in general terms; and
- questionnaires compiled with a client orientation.

The use of questionnaires to gather information also has several advantages and disadvantages, namely:

Advantages:

- Improves the risk-identification process, because various aspects can be investigated relatively quickly.
- Increases the effective utilisation of resources (less staff can gather more information).
- Reduces the time required to complete the process.
- Critical areas can be identified relatively quickly.
- More people can be involved in the process, and not only management.
- They are easy to complete.

Disadvantages:

- Sensitive information is "exposed".
- Management does not have the required skills, for example to use the Internet.
- Respondents interpret questions in various ways.
- Management does not have the time to fill in long questionnaires.
- There is no personal interaction, for example body language can not be evaluated.
- Questionnaires are completed with bias in favour of the respondent's own environment, and the large picture is ignored.

Workshops:

Workshops can be arranged to obtain information on risk areas. They comprise the bringing together of key figures in the organisation at a central point. A facilitator is appointed and the group discusses particular topics, from which the identification of risks emanates. The workshops can be hand driven or computer driven.

In a hand system (Crawford 1999), the facilitator tables certain topics and the group discusses them. Risks are identified from the discussion. The hand system also has various advantages and disadvantages, namely:

Advantages:

- The discussion initiates new ideas.

Disadvantages:

- The facilitator can be prejudiced.
- Participants can be afraid to express their opinions in the presence of senior members of staff.
- The success of the workshop depends on the capability of the facilitator.
- It is a slow process and it is sometimes difficult to get all the role players together on one day.

In the case of a computer-driven workshop (ABSA 1999), certain aspects are highlighted in advance. The group sits in a central place with a computer in front of each member. The computer is linked to a central computer (facilitator). A period is allowed during which the participants can freely identify risks in respect of each area. After a particular period the risks are grouped by the facilitator (central computer) and returned to the participants. Each participant then has the opportunity to decide what the impact and extent of each identified risk is. Insignificant risks are therefore eliminated in this process.

Advantages:

- There is no room for prejudice.
- Participants retain the freedom to remain anonymous.

Disadvantages:

- Ideas are not exchanged.
- Participants should be computer literate.
- The system can be interrupted, for example by a power failure.

Research by PricewaterhouseCoopers (1999) has indicated that the facilitated workshop is the method used most in South Africa. Whereas approximately 50% of companies use this method, 20% use computer-driven workshops, 22% a combination of all methods, 0.4% computerised questionnaires and 6% hand-driven questionnaires.

Regarding the use of control self-assessment in South Africa, compared to Europe, the data is as follows:

	EUROPE	SOUTH AFRICA
Mostly paper driven	29%	32%
Only paper driven	40%	21%
Mostly computer driven	24%	35%
Only computer driven	6%	10%

According to the Institute of Internal Auditors (1996), the following factors among other things determine which method is selected:

1 Objective pursued with the use of control self-assessment;
2 the organisation's objectives;
3 organisational culture;
4 opportunities;
5 other projects of the organisation;
6 capability in respect of facilitating;
7 technology available.

3.3.3 Reporting

When the various workshops, questionnaires or interviews in respect of specific activities or processes have been completed, a report should be compiled as soon as possible. The team responsible for control self-assessment should evaluate, improve and summarise the results. For example, it should check the spelling, ensure that the information is clearly set out and process the data of the questionnaires (The Institute of Internal Auditors 1996).

Thereafter a preliminary report is compiled and distributed to participants. Comment is received and processed and a final report submitted to management within a certain period. The report should be user friendly. The latest trend is to use graphs to present the findings.

3.3.4 Development and implementation of action plans

The true success of control self-assessment depends on whether that which is found in the process is addressed afterwards (The Institute of Internal Auditors 1996). If participants know in advance that their recommendations do indeed have authority and that they will be addressed properly, it encourages them to participate fully in the process.

Action plans and aspects of the implementation should therefore be determined before the self-evaluation of the control process. Specific persons should be

given the responsibility. Time limitations on the implementation of action plans should be laid down and communicated to participants in advance. If possible, action plans should be stated during the self-evaluation of the control process. Management should, however, still approve the implementation of actions.

3.3.5 Feedback on the success of the process

Various actions can be taken to determine whether control self-assessment has been completed successfully. The facilitator can launch an investigation to determine whether participants' objectives and perceptions have been achieved, whether management is of the opinion that value has been added etc. A comparison of activities, processes and/or control before and after the process can provide valuable information on the success of the process.

3.4 Advantages of the implementation of control self-assessment

There are various advantages to the implementation of control self-assessment. The following are some of the most important advantages:

1 The source or causes of risks are dentified.

2 Management's responsibility for risk and control in the organisation is confirmed by their participation in the process.

3 The control environment is strengthened, because members of staff see that management is committed to the process of reducing risk and establishing proper control procedures.

4 Inputs are obtained from all levels of the organisation.

5 Participants acquire a broader perspective on the activities, processes and objectives of the organisation.

6 Horizontal and vertical communication improve.

3.5 Problems and disadvantages in the implementation of control self-assessment

Although there are not many disadvantages associated with control self-assessment, a poorly planned process can prove to be fruitless, with the result that valuable time and money is wasted. The following are some of the most important problems and disadvantages:

1 Opposition of participants and/or management to the process, with the result that erroneous information is supplied or that important information is not revealed.

2 The facilitator is not accepted by the participants.

3 It is not always appropriate to reveal certain risks, for example where participants are involved in fraud.

4 Other important factors in the organisation can handicap the process, for example a rationalisation programme.

5 If management does not support the process in word and deed, the remainder of the staff will be reluctant to become fully involved in the process.

6 Technology is lacking or participants are not capable of using the technology.

7 The facilitator does not have the necessary knowledge and experience to manage the process.

8 Participants only focus on their own tasks and risks, and ignore the risks for the organisation as a whole.

9 The wrong combination of participants, method or facilitator is used for a specific group.

10 Role players oversimplify the process and the planning it requires.

3.6 Critical success factors for the implementation of control self-assessment

Certain factors determine the success of control self-assessment. The following are, in brief, the factors concerned:

1 It should be determined in advance whether control self-assessment is the best method to use for the organisation's circumstances.

2 Clear objectives should be set in advance for the use of control self-assessment.

3 Expectations should be described in advance by defining the end product.

4 Top management should support the process.

5 Top management should be enthusiastic about the process.

6 Participants should accept and identify with the process.

7 The culture of the organisation should complement the process.

4. Summary

Risk is becoming more of a reality in today's competitive business world. Management is accountable towards shareholders, creditors, partners and employees and it is their responsibility to address the various risks facing an organisation.

Internal auditors assist management with this task. Control self-assessment was developed by the internal audit profession to structure the process of managing risk. This is an approach used to actively take responsibility and ownership for developing, assessing, maintaining and monitoring controls to address business risk.

The use of control self-assessment in the risk management process has various advantages of which only the most important ones are mentioned below. The first important advantage is that management accepts responsibility for the risk management process and the internal control of the organisation. It also promotes a positive attitude on the part of employees towards the internal control system. A second advantage is that a partnership is formed between management and the other role players in risk management and control self-assessment. Thirdly a communication channel is created for feedback on the operation and effectiveness of risk management.

Annexure 1

ENVIRONMENTAL RISK

Competitor
Catastrophic Loss
Sensitivity
Sovereign/Political
Shareholder Relations
Legal/Regulatory
Industry
Capital Availability
Financial Markets

PROCESS RISK

OPERATIONAL RISK
Customer Satisfaction
Human Resources
Product Development
Efficiency
Capacity
Performance Gap
Cycle Time
Sourcing
Commodity Pricing
Obsolescence/Shrinkage
Compliance
Business Interruption
Product/Service Failure
Environmental
Health and Safety
Trademark/Brand Name Erosion

EMPOWERMENT RISK
Leadership
Authority
Limit
Performance Incentives
Communications

INTEGRITY RISK
Business Fraud
Employee Fraud
Illegal Acts
Unauthorised Use
Reputation

FINANCIAL RISK
Currency
Interest Rate
Liquidity
Cash Transfer/Velocity
Derivative
Settlement
Reinvestment/Rollover
Credit
Collateral/Security
Counterparts

INFORMATION PROCESSING/ TECHNOLOGY RISK
Access
Integrity
Relevance
Availability

INFORMATION FOR DECISION-MAKING RISK

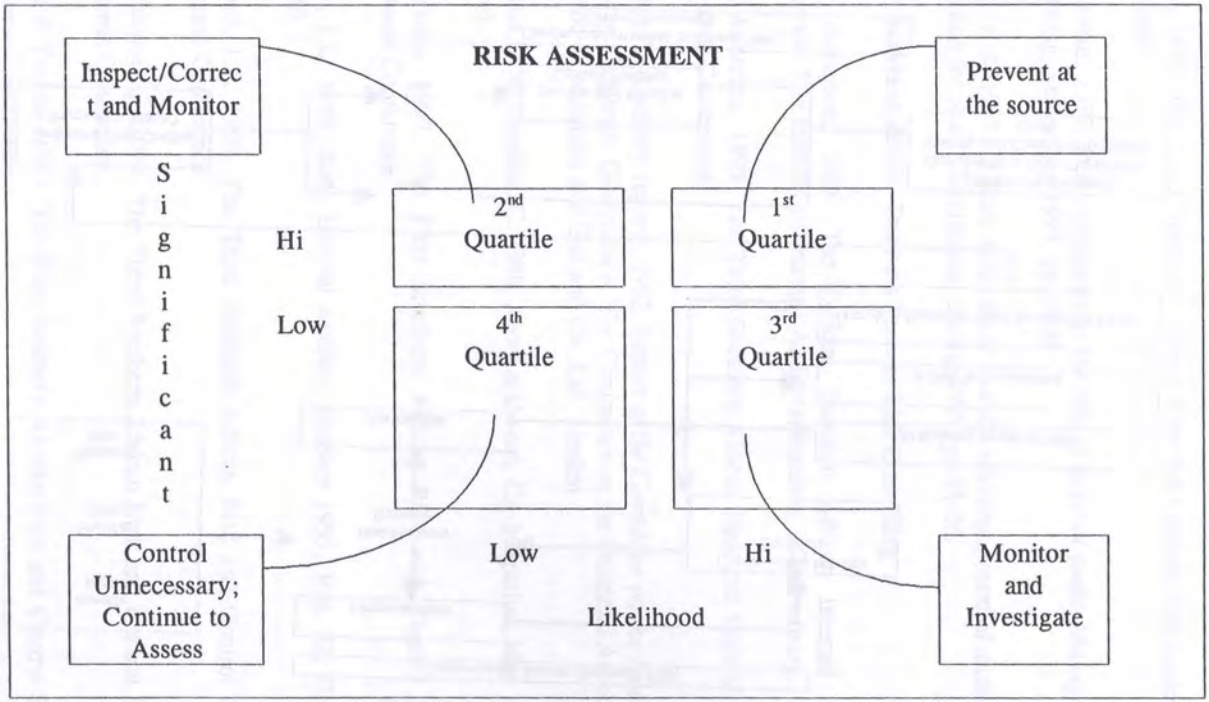
OPERATIONAL
Pricing
Contract Commitment
Measurement
Alignment
Completeness and Accuracy
Regulatory Reporting

FINANCIAL
Budget and Planning
Completeness and Accuracy
Accounting Information
Evaluation of Financial Reporting
Taxation
Pension Fund
Evaluation of investment
Regulatory Reporting

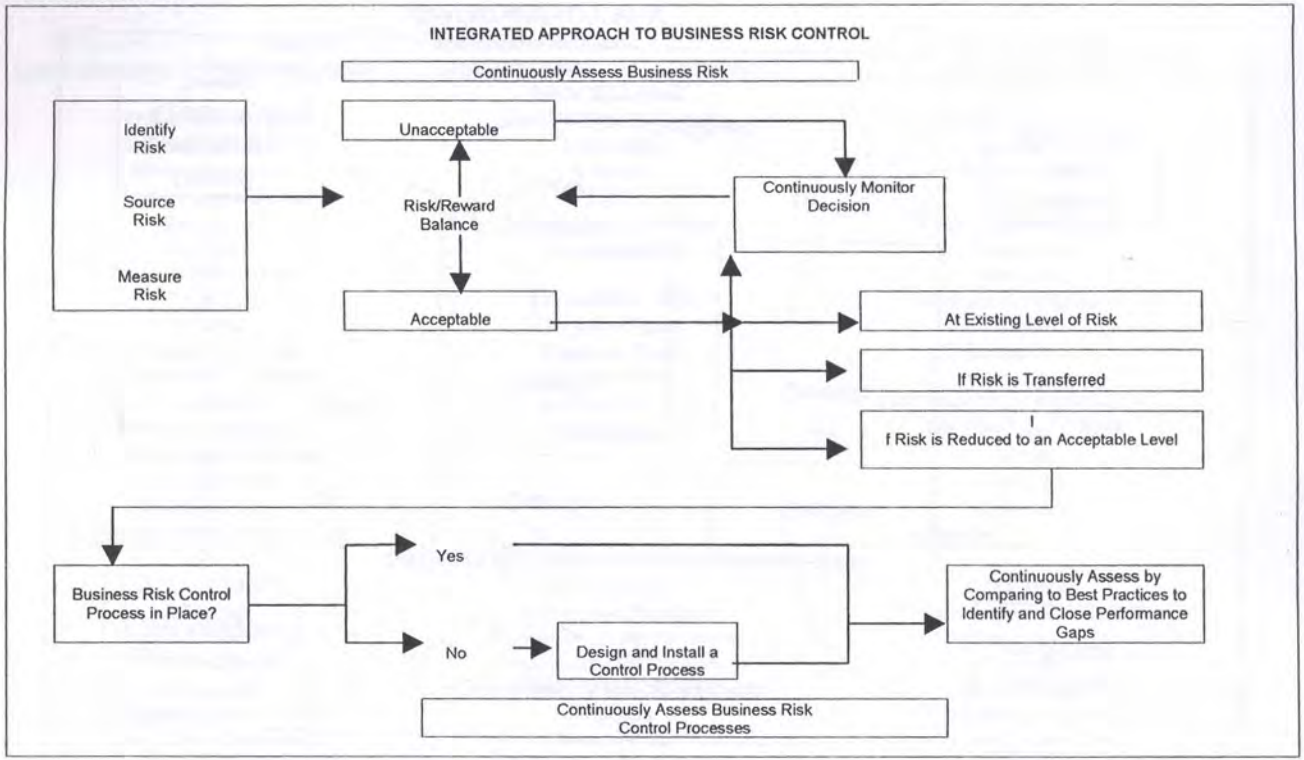
STRATEGIC
Environmental Scan
Business Portfolio
Valuation
Measurement
Organisation Structure
Resource Allocation
Planning
Life Cycle

Annexure 2

Identified risks can be presented on a graph as follows:



Annexure 3


INTEGRATED APPROACH TO BUSINESS RISK CONTROL
Continuously Assess Business Risk
Identify Risk
Source Risk
Measure Risk
Unacceptable
Risk/Reward Balance
Acceptable
Continuously Monitor Decision
At Existing Level of Risk
If Risk is Transferred
If Risk is Reduced to an Acceptable Level
Business Risk Control Process in Place?
Yes
No
Design and Install a Control Process
Continuously Assess by Comparing to Best Practices to Identify and Close Performance Gaps
Continuously Assess Business Risk Control Processes

Bibliography

ABSA, 1999. The Third Southern African Risk and Control Self-Assessment Conference.

Anonymous, 1997. *Risk management: the role of internal audit*, Management Accounting, September 1997, pp.42-43.

Arnold, E.S. 1997. *A Risk Assessment tool for selecting potential audits: An application for State Government*, Spring 1997, pp.21-26.

Arthur Andersen, 1995. Business Process Risk Consulting.

Arthur Andersen, 1998. The Official Southern African Internal Audit Conference: The Institute of Internal Auditors, Sandton, Johannesburg.

Arthur Andersen, 1999. The Third Southern African Risk and Control Self-Assessment Conference.

Cadbury, A. (Cadbury report), 1992. *Report of the Committee on the Financial Aspects of Corporate Governance*, The Committee on the Financial Aspects of Corporate Governance and Gee and Co. Ltd. London.

Cleveland, P. & Rossiter, C. 1998. *Room at the top*, CA Magazine, May 1998, pp.39-40.

CNA Gallo, 1997. The First Southern African Risk and Control Self-Assessment Conference.

Colbert, J.L. 1995. *Risk*, Internal Auditor, October 1995, Vol. 52, No. 5, pp.36-40.

Crawford, J.A. 1999. The Third Southern African Risk and Control Self-Assessment Conference.

Crow Consulting, 1999. The Third Southern African Risk and Control Self-Assessment Conference.

Deloitte & Touche, 1997. The First Southern African Risk and Control Self-Assessment Conference.

De Villiers, C.J., Vorster, Q. 1995. *Green Reporting in South Africa*, Third Edition, Department of Accounting, University of Pretoria, Pretoria.

Dimartini, W., Mcanally, P. 1997. *Regulating Disaster Recovery*, Internal Auditor, December 1997, Vol. 54, No. 6, pp.42-52.

Grobler, G.P. & Du Plessis, L. 1998. *Die effek van die beheeromgewing op werknemersbedrog*, Meditari Accountancy Research, UP, 1998, Vol. 6, pp.121.

Leithhead, B.S. *Managing "People" Risks*, Internal Auditor, December 1998, Vol. 55, No. 6, pp.66-67.

PricewaterhouseCoopers, 1999. The Third Southern African Risk and Control Self-Assessment Conference.

Puccinelli, B. 1998. *Overcoming resistance to change*, Inform, September 1998, Vol. 12, No. 8, pp.40-41.

Reding, K.F. DiGirolamo, K.K. 1994. *Allstate's Risk Assessment Approach to Selecting Operational Audit Topics*, Internal Auditor, April 1994, Vol. 51, No.2, pp.48-52.

Sawyer, L.B. 1998. *When the problem is management*, Internal Auditor, August. 1998, Vol. 55, No. 4, pp.33-38.

Schneier, R., Miccolis, J, 1998. *Enterprise Management*, Strategy & Leadership, March/April 1998, pp.10-16.

Sparrow, A. 1998. *Business Risk Management*, Chartered Accountant's Journal, April 1998, pp.11-13.

Technikon Pretoria, 1999. *Internal Auditing*, The Impact of Risk on Internal Audit, Chapter 2.

Teets, R.W., Kuhnke, D.B., Bradley, P., Bridegan, G. *et al.* 1994. *Applying the risk management process to environmental management*, Risk Management, February 1994, Vol. 41, No. 2, pp.18-24.

The Institute of Directors in Southern Africa, 1994. *The King Report on Corporate Governance*, Parklands.

The Institute of Internal Auditors, 1996. *Control self-assessment: experience, current thinking and best practices*, IIA Research Foundation, VSA.

The Institute of Internal Auditors, 1999. *The new definition of internal auditing and a professional practices framework,* IA Advisor., August/September 1999, p.6.

The Institute of Internal Auditors, 1995. *Standards for the Professional Practice of Internal Auditing.*

The Institute of Internal Auditors, 1991. *Systems Auditability and Control Report.* IIA Research Foundation, VSA.

Update, 1997. *Inappropriate Sexual Conduct Named Top Risk of the 90s*, Internal Auditor, December 1997, Vol. 54, No.6, p.14.

Update, 1998. *Risk Management Activities Found Lacking*, Internal Auditor, June 1998, Vol. 55, No. 3, p.14.

Waterman, L. 1995. *Health and safety risk assessments in the health sector*, Facilities, March 1995, Vol. 13, No. 2, pp.22-25.