A Structured Technique for applying Risk Based Internal Auditing in Information Technology environments (With specific reference to IIA RBIA, King Report and CobiT)

Sonya Wheeler

University of Stellenbosch

Faculty of Economic and Management Sciences

Assignment presented in partial fulfilment of the requirements for the degree Master of Accountancy (Computer Auditing)

Supervisor: Prof WH Boshoff

April 2005

DECLARATION

I, the undersigned, hereby declare that the work contained in this assignment is my own original work and that I have not previously in its entirety or in part submitted it at any university for a degree.

Signature: ……

Date: ……..

SUMMARY

A technique that may be used to incorporate Risk Based Internal Auditing (RBIA) in the IT environment is to follow annual audit planning methodology steps. The IT infrastructure elements are linked to the business processes which they support. Their ranking are based on the risks assessments of the business process, the business process priority, the dependency of the business process on IT and the IT infrastructure element's own risk assessment. CobiT is used as a auditing method, i.e. best practice guidance to audit against.

OPSOMMING

‘n Moontlike tegniek wat gebruik kan work om Risiko-gebaseerde Interne Audit (RBIA) in die Informasie Tegnologie (IT) omgewing the inkorporeer, is deur die stappe in die jaarlikse audit beplanning metodiek te volg. Die IT infrastruktuur elemente word gekoppel aan die besigheidsprosesse wat hulle ondersteun. Hulle orde word gebaseer op die risiko bepaling van die besigheidsproses, die besigheidsproses prioriteit, die afhanklikheid van die besigheidsproses op IT en die IT infrastruktuur element se eie risiko bepaling. CobiT kan gebruik word as ‘n oudit metode, dit wil sê as beste praktyk om teen te oudit.

TABLE OF CONTENTS

Chapter 1

The Requirement: Perform Risk Based Internal Auditing (RBIA)

Introduction

'The focus of internal audit work has shifted over the last decade. There has been a move from systems based auditing to process based auditing and the current emphasis is on Risk Based Internal Auditing (RBIA).'[1] The International Internal Audit Standards, Combined Code and the King Committee, as per the following, also place emphasis on RBIA:

- The International Standards for the Professional Practice of Internal Auditing and the associated Practice advisories emphasise adopting a risk-based approach to internal auditing. As stated in the Institute of Internal Auditors (IIA) Position Statement on Risk Based Internal Auditing (RBIA), Internal Audit (IA) need to adopt a risk-based approach compatible with that adopted by their organisation. 'The key distinction with RBIA is that the focus should be to understand and analyse management's assessment of risk and to base audit efforts around that process.' [1]
- 'This approach is also consistent with the Turnbull guidance Internal Control: Guidance for Directors on the Combined Code, which requires directors to *adopt a* "risk-based approach to establishing sound system of internal control and reviewing its effectiveness" and to embed risk management and internal control into the culture of the organisation.' [1]
- King Committee on Corporate Governance recommends that 'the internal audit plan should be based on risk assessment as well as on issues highlighted by the audit committee and senior management. The risk assessment process should be of a continuous nature so as to identify not only residual or existing risks, but emerging risks, and should be conducted formally at least annually, but more often in complex organisations. This risk assessment should be co-ordinated with the board's own assessment of risk.' [2]

‘Information Technology (IT) is now seen as being an integral part of the enterprise strategy rather than a mere enabler within organisations. While technology developments can improve governance, they have also brought increased risks and challenges that need to be addressed so that management can discharge its governance responsibilities.’

Many organisations recognise the potential benefits that technology can yield. Successful organisations, however, understand and manage the risks associated with implementing new technologies**.**[3]

‘Auditing around the computer is no longer an option for the auditors, the controls and processes incorporated in modern systems have to be evaluated and tested. In many instances, internal control systems are altered to bring them in line with best practices included with the basic functionality of many of these systems.’

The Problem:

RBIA is no longer an option, but a requirement. IT is a major contributor to risks for organisations. Therefore IT needs to be included in the risk-based audit plan. Even though there are lots of articles and guidance on what you should do, there is less guidance in terms of how to practically apply RBIA. When one asks the question: ‘Where does IT fit into RBIA?’ the answers are even less forthcoming.

This assignment will attempt to provide a structured technique for applying RBIA in IT environments.

Research Methodology:

1. Use the IIA's Position Statement on RBIA as a basis
2. Link RBIA and IT with business processes as IT enables and supports them. 'Information is data that has been processed and is meaningful to a user. A system is a set of components that operate together to achieve a common purpose. With these two basic definitions, we can easily proceed to a definition of organisational information systems. Since information is data that has been processed, it follows that some data has to be collected, transmitted, then processed and stored. To be meaningful to users, the information must be retrieved and distributed to them. The users belong to a system called "organisation". One of the components of an organisation is the "information system". The components of this system are people, hardware, software, data and procedures. The organisational information system thus collects, transmits, processes and stores data, and retrieves and distributes information to various users in the organisation. To reiterate, information systems produce information that supports the operation and management functions (business processes) of the organisation.' [4]
3. Use CobiT as a framework for IT, as it is:
    a. Generally accepted
    b. Complete coverage of IT
4. Devise a schema for mapping RBIA objectives and CobiT.

Chapter 2

Available Frameworks, Definitions and Interpretations

Available Frameworks

The first thing that needs to be considered in developing a structured technique for RBIA in IT is available guidance or frameworks. For this assignment the following were considered:

The CobiT Framework (Governance, Control and Audit for Information and Related Technology)

'Control Objectives for Information and related Technology (CobiT) helps meet the multiple needs of management by bridging the gaps between business risks, control needs and technical issues. It provides good practices across a domain and process framework and presents activities in a manageable and logical structure. CobiT's "good practices" means consensus of the experts - they will help optimise information investments and will provide a measure to be judged against when things do go wrong.'

IIA Position Statement on RBIA

According to the Position Statement, 'RBIA is a much used and much misunderstood term. This paper aims to set out the Institute's position with regard to RBIA and to offer some high level guidance on how to approach it.' [1]

Internal Auditing – a risky biz: The practical application of risk-based auditing by David M Griffiths PhD FCA

'The aim in this report is to simplify some of the principles in internal auditing and make them consistent, based on risk. This report builds on these principles to consider why internal auditing can be of benefit to an organisation and then details how, using risk-based methods, it can deliver this benefit.' [5]

Definitions

The following definitions need to be understood:

Definition of IT Governance

'A structure of relationships and processes to direct and control the enterprise in order to achieve the enterprise's goals by adding value while balancing risk versus return over IT and its processes.'

Definition of Risk

'Risk is a concept used to express uncertainty about events and/or their outcomes that could have a material effect on the goals of the organisation. This incorporates the managerial and strategic elements of risk and opportunity in achieving goals. Risk is a central element of corporate governance.'[6] Or more simply put: 'A risk is a set of circumstances that prevent the achievement of objectives'.

'It is the expression of likelihood and impact of an event with the potential to influence the achievement of an organisation's objectives. Impact refers to the extent of the consequences or implications if the risk does occur. Likelihood refers to the probability that the risk may occur given the current context of the organisation.'[7]

Definition of Inherent (gross) Risk

'The status of risk (measured through impact and likelihood) without taking account of any risk management activities that the organisation may already have in place.'

Definition of Residual (net) Risk

Also known as post-control risk. 'The status of risk (measured through impact and likelihood) after taking account of any risk management activities that the organisation may have in place.'[1]

Definition of Risk Appetite

'The level of risk that the board or management is prepared to live with.'

Interpretations and concepts

For the purpose of this assignment the following words and concepts need to be discussed to ensure a common understanding:

Corporate Objectives

For the purpose of this assignment, Corporate Objectives can be described as an ideal or goal, which an organisation is aspiring towards in an attempt to meet certain pre-established needs.

Business Process

For the purpose of this assignment, a business process can be interpreted as a unit of work executed within the business to meet a business/corporate need or objective. To give an example - if we look at a horse farm, a business process might be 'feed the horses'.

These business processes also mitigate organisation risks in achievement of corporate objectives.

RBIA

According to the IIA position statement on RBIA, 'the objective of RBIA is to provide independent assurance to the board that:

- The risk management processes which management has put in place within the organisation (covering all risk management processes at corporate, divisional, business unit, business process level, etc.) are operating as intended
- These risk management processes are of sound design
- The responses which management has made to risks which they wish to treat are both adequate and effective in reducing those risks to a level acceptable to the board
- And a sound framework of controls is in place to sufficiently mitigate those risks which management wishes to treat.'

IT Infrastructure Elements

For the purpose of this assignment, the IT infrastructure consists of applications, data management systems, operating systems, network and physical machines / servers (or otherwise location, e.g. data centre). These IT infrastructure elements support business processes. The IT dependency is determined by the extent to which IT supports the business processes.

Chapter 3

Linking the Frameworks

Introduction

An essential part of a structured technique of applying RBIA in IT is industry-accepted frameworks. Examples of these frameworks are referenced in the previous chapter.

To establish where IT fits in, it is necessary to link these frameworks. The following methods were considered:

1. Analysis of each component within each framework to determine their linkages.

   This method may be too complex and it will be difficult to have a structured approach as outcome. There is also no assurance that the results will show which IT elements carry the higher risk and thereby complying with the RBIA requirement.

2. Following an audit process to establish the linkages or fit. This leads to a more logical approach and therefore this method is preferred.

Which Audit Process?

Activities within the Internal Audit department are mostly based on auditable units / areas for review, as indicated in their annual audit plan. An audit process is followed to prepare this annual audit plan. For this reason, to apply RBIA in IT, we will attempt to establish where IT should fit into this risk-based annual audit plan process.

Linking the framework to the Audit process

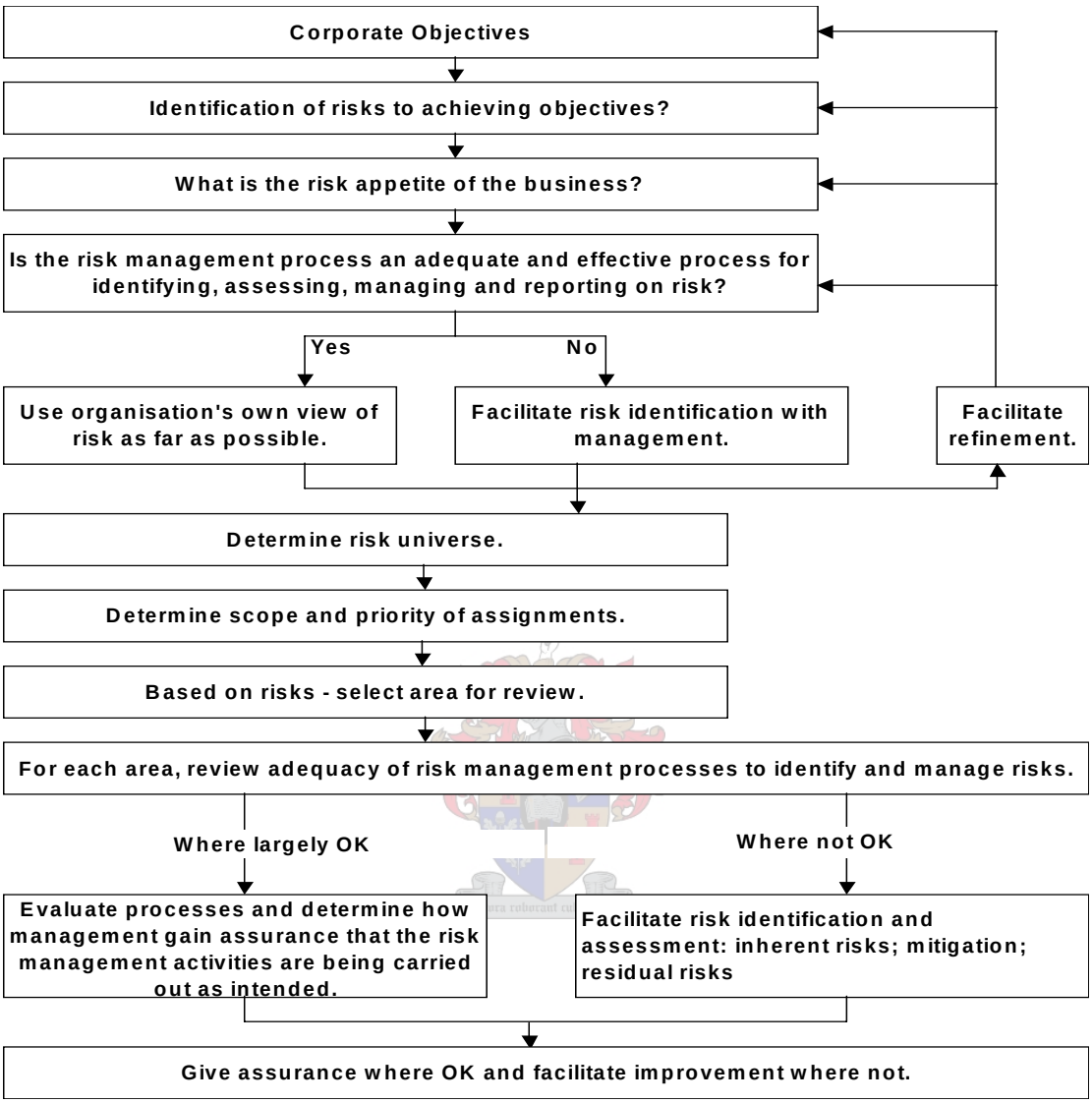
According to the King Report, 'the annual audit plan should be based on risk assessment as well as on issues highlighted by the audit committee and senior management. The risk assessment process should be of a continuous nature so as to identify not only residual or existing but emerging risks, and should be conducted formally at least annually, but more often in complex organisations. This risk assessment should be co-ordinated with the board's own assessment of risk.' [2]

CobiT is a well-known framework in the IT auditing industry. It is useful to assist in determining what type of controls should be implemented to govern an IT environment. It is also linked to process objectives. These processes support organisation risks. It is, however, more specific to controls than risks. Therefore, CobiT, if used in isolation, lacks context in terms of the organisation risks and is not an easy fit to the annual audit plan process.

The IIA's Position statement on RBIA is more suited as a starting framework as it adds context to the organisation as a whole and is not isolated to one environment. This document defines the steps to follow in RBIA and is business orientated. It contains reference to risk assessments, which is required by the King Report and is an easier fit to the annual audit plan process and therefore our starting framework.

IIA's RBIA

IIA's Position Statement on RBIA describes RBIA schematically, as follows:



Extract from IIA Practice Advisory on RBIA

RBIA starts with the corporate objectives and then focuses on those risks that prevent their achievement, as identified by management. The scope of RBIA includes strategic and business-as-usual risks.

RBIA Priorities Toolset

The Treasury Board of Canada Secretariat (2003) has developed a toolset that may be used by Internal Audit to prepare an internal audit plan that is based on areas of risk and materiality. They have broken down the process into 5 phases:

- *Phase 1: Project Preparation* – 'Objective: The implementation of the Toolset should be treated as a distinct project, with the completed template being the deliverable, and the identification of the internal audit priorities and internal audit plan being the outcome of the project. As with any project, effective planning is critical.'
- *Phase 2: Identify and Categorise Risks* – 'Objective: To identify and categorise risks to the organisation and provide examples of risks.'
- *Phase 3: Conduct Risk Assessment* – 'Objective: To assess key risks applicable to the organisation.'
- *Phase 4: Identify Internal Audit Priorities and Plan Details* – 'Objective: To determine if the risks should be examined independently, and if so, the priority, the objective of the project, the type of project, the year in which the project should be conducted, and an estimate of resources required.'
- *Phase 5: Finalise and Approve Internal Audit Plan* – 'Objective: Finalise and obtain Internal Audit Committee approval for the internal audit plan.' [7]

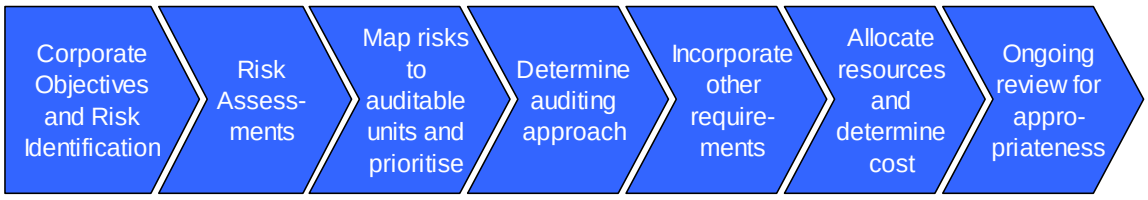
Audit process steps

Using the IIA's RBIA framework, annual audit plan steps can be established. The steps below are in a logical order to ensure that RBIA principles are complied with. It incorporates the King Report's requirements and is also substantially similar to other RBIA steps, including the IIA's illustration as set out on page 13. The steps below are broken down or enhanced to facilitate an annual audit plan as outcome.

Thus, the steps in the annual audit plan process that will be used forthwith in this assignment are:

1. Determine/obtain the corporate objectives
2. Obtain/facilitate the identification of risks that prevent the achievement of the identified objectives or missed opportunities
3. Obtain/facilitate the assessment of inherent and residual values for the identified risks
4. Obtain/facilitate the assessment of the organisation's risk appetite for the identified risks
5. Map these risks to auditable units / areas for review. For example, a risk on its own, risks that fall into a certain category or combined risks within a specific business processes can each be an auditable unit
6. Rank/prioritise the auditable units, based on the risk assessments and their importance weighting within the organisation
7. Determine the auditing approach for the identified auditable units. This should be based on the combination of inherent and residual risk assessments, as well as the organisation's risk appetite
8. Incorporate other requirements, such as specific requirements from the audit committee or previously reported concerns to be followed up on
9. Allocate resources and determine costs to complete the audit plan
10. Periodically, review the appropriateness of the audit plan in relation to organisational changes and needs.

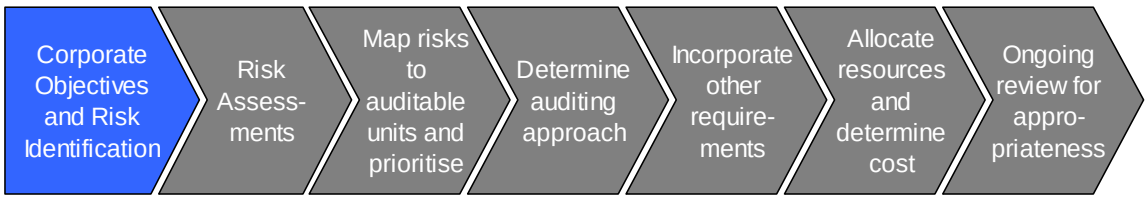
The above audit process steps can schematically be summarised as follows:



How do we apply RBIA in IT?

The questions still remains - How do we apply RBIA in IT? Where does CobiT fit in? Let us talk through the annual audit planning steps in an attempt to answer these questions:

Corporate objectives and Risk Identification (Step 1 and 2 in determining the annual audit plan as described above)



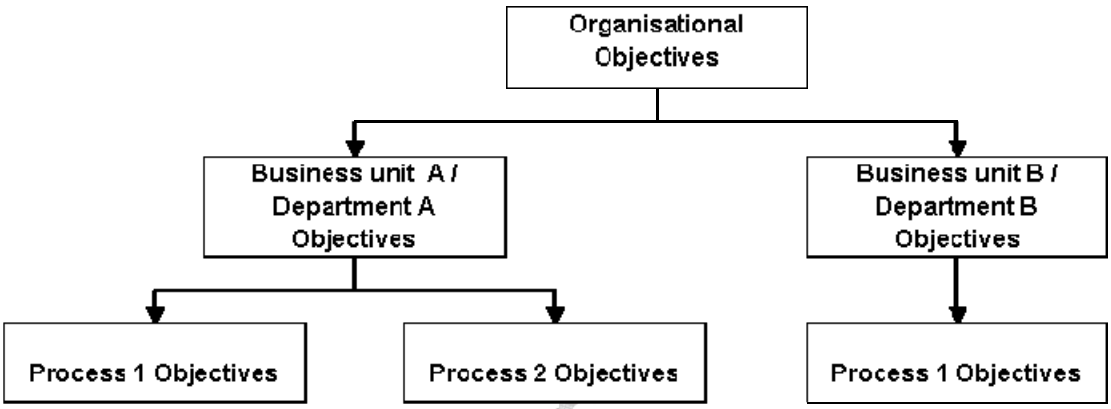
According to the IIA's Position statement and our annual audit plan process steps, the first step is to determine that appropriate objectives have been set by the organisation and then to determine whether or not the business has an adequate process in place for identifying, assessing and managing the risks that impact on the achievement of these objectives. This includes the strategic and business-as-usual objectives.

There can be various layers of corporate objectives. For simplicity three layers are categorised for the purpose of this assignment:

- **Organisational** objectives. These are the top-level objectives and are most often strategic in nature, but should include business-as-usual objectives at its highest level.
- **Business unit or departmental** objectives. These are the slightly more detailed objectives. For an organisation to be successful, business unit or departmental objectives should ideally be aligned to the organisational objectives. These objectives include both business-as-usual and strategic objectives. It is also important to note that IT can be a department on its own, with it's own departmental objectives. This too should be linked to the organisational objectives.

- **Process** objectives. These objectives are at the detailed level and are activity specific. These, in turn should be aligned to the business unit / departmental objectives. Again, IT process objectives can be included here, provided that there is a linkage all the way back to the organisational objectives.

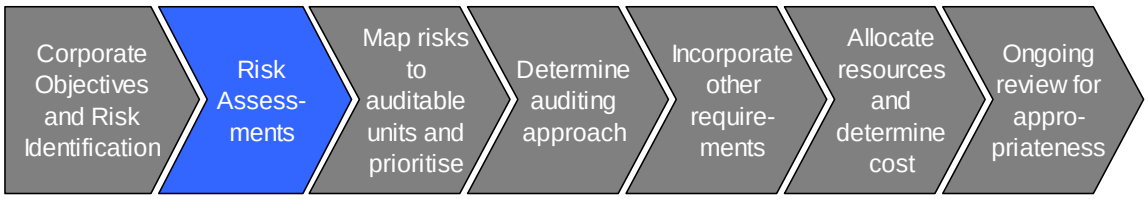
Schematically, the corporate objective layers can be illustrated as follows:



For the annual audit plan, the risks that prevent the achievement of at least the organisational and business unit / departmental objectives need to be identified. Risks can be uncertainties, opportunities or threats such as stumbling blocks, hazards, lost opportunities and circumstances that could lead to an impact on information integrity, ownership, delivery, outputs, etc.

The corporate objectives and risks should, of course, be obtained from management responsible for setting the strategic direction and managing ongoing business. If these objectives cannot be obtained from them, the process to identify these objectives and risks should be facilitated with them. According to the King Report, 'a comprehensive system of control should be established by the board, to ensure that risks are mitigated and that the company's objectives are attained. The control environment should also set the tone of the company and cover ethical values, management's philosophy and the competence of employees.'

Risk assessments (Step 3 and 4 in determining the annual audit plan as described above)



After the risks that may prevent the achievement of the objectives are identified, they should be assessed. This risk assessment includes inherent risk, residual risk and the risk appetite as determined by the organisation.

According to the King Report, 'a systematic, documented assessment of the processes and outcomes surrounding key risks should be undertaken at least annually. This risk assessment should, where possible, include an estimate of the likelihood of occurrence, the quantification of the probable impact, and comparison with available benchmarks. Recommendations should also be made as to how each risk should be managed.'

'To assess impact, people need to ask themselves "How much of an impact will the risk have if it does occur?"

- A minor impact suggests that the risk would not have important implications on the organisation.
- A moderate impact suggests that the risk could have implications for the organisation's ability to succeed.
- A significant impact suggests that the risk would have important implications on the organisation.

To assess likelihood, people need to ask themselves "How likely is the risk to occur in the future, given what we currently do about it?"

- A low likelihood suggests that the risk is unlikely to occur, given its nature and current risk management practices in place.
- A medium likelihood of occurrence suggests that the risk has a moderate probability of occurrence.

- A high likelihood of occurrence suggests that the risk is likely to occur, despite current risk management practices in place.'

This risk assessment should be performed based on pre-determined criteria for impact and likelihood of the occurrence to ensure consistency throughout the organisation.

The following, much simplified table, is an example that can be used by organisations to add its own criteria by defining significant, moderate, probable, etc. It is important to remember that these criteria should include quantities, as well as qualitative factors.

Table to determine risk assessment based on impact and likelihood, i.e risk assessed as high, medium or low				
IMPACT	Significant	Medium	High	High
	Moderate	Low	Medium	High
	Minor	Low	Low	Medium
		Unlikely	Probable	Almost Certain
		LIKELIHOOD		

A point to consider when identifying and assessing risks, is that 'while the IS (Information Systems) auditor has no explicit responsibility to detect or prevent illegal acts or irregularities, the IT auditor should design procedures to detect illegal acts or irregularities based on the assessed level of risk that irregularities or illegal acts could occur. As part of the planning process and performance of risk assessment, the IS auditor should make inquiries to management with regard to such issues as:

- Their understanding of the level of risk of irregularities and illegal acts in the organisation.
- Whether they have knowledge of irregularities and illegal acts that have occurred or could have occurred against or within the organisation.
- How the risk of irregularities or illegal acts is monitored, managed and controlled.

The IS auditor should design procedures that take into account the identified level of risk for irregularities and illegal acts. In practice, this means that when a high risk of irregularities or illegal acts is identified, procedures designed to identify whether irregularities or illegal acts exist should be performed.' [8]

Map risks to auditable units and prioritise (Step 5 and 6 in determining the annual audit plan as described above)

From the previous step it is clear that what we have at the moment is a huge list of risks that are linked to the corporate objectives, i.e. risk universe.

The question now is how can these risks be audited? Will each risk be a separate auditable unit? Yes, that is an alternative, but it may not be the most efficient way to approach the risk universe. Another option one can consider is to find the best or most logical way of grouping these risks together.

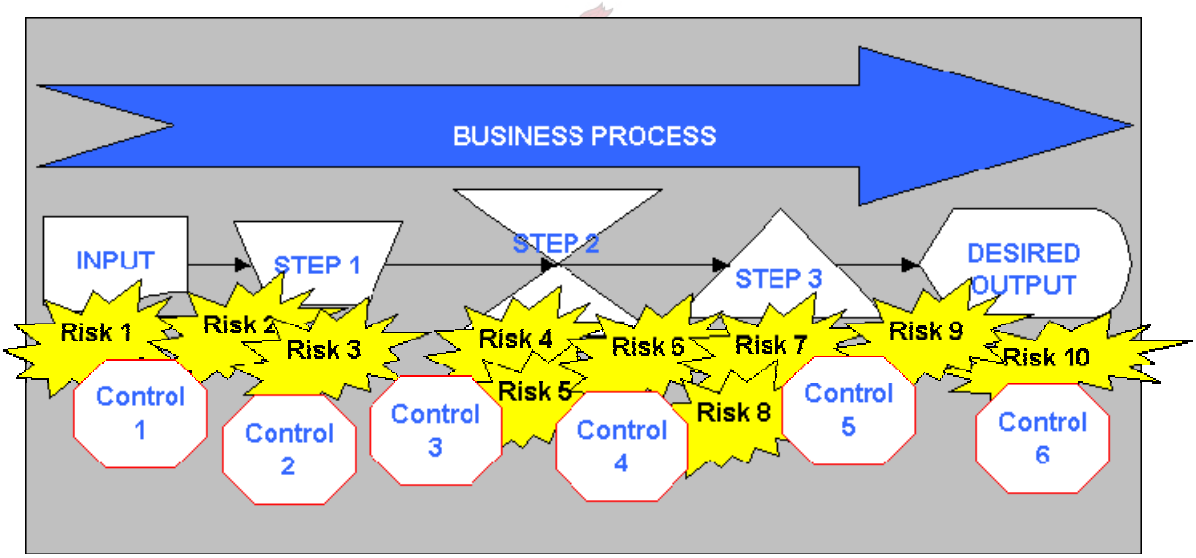
Groupings that can be considered include:

- The corporate objectives the risks are linked to
- Pre-defined risk categories, e.g. strategic risk, financial risk, information risk, etc
- Business processes
- Or even combinations of the above.

Some risks might still be significant enough to be audited on it's own and therefore, while grouping risks together, one can decide to exclude this risk from one of the categories. These groupings and excluded risks each become an auditable unit in the annual audit plan.

Following this grouping, these auditable units should be ranked/prioritised based on the risk assessments and their importance weighting within the organisation. This will assist in understanding what auditable unit deserves attention first. The more important and risky the risks or grouping of risks, the higher the audit focus.

As explained in chapter 2, a business process is the unit of work executed to meet a business need or objective. This business process comprises controls, which, in their design, mitigate risk. Schematically it can be described as follows:



The benefit of mapping the risks to business processes is that it assists managers and auditors alike to understand the business environment and risks better. With this understanding the control environment can be designed optimally.

The following table illustrates the information we have thus far:

Illustrative table for the linkage from organisational objective to business process:						
Organisational Objective (OO)	**Business Unit objective (BUO)**	**Risk**	**Risk assessment**			**Business process (BP)**
			Inherent Risk (IR)	**Risk Appetite (RA)**	**Risidual Risk (RR)**	
Examples:						
OO 1	BUO 1	Risk 1	High	Low	High	BP 1
OO 1	BUO 2	Risk 2	Medium	Low	Medium	BP 1
OO 1	BUO 3	Risk 2	Medium	Low	Medium	BP 2
OO 1	BUO 3	Risk 3	High	High	High	BP 3
OO 2	BUO 4	Risk 3	High	High	High	BP 4
OO 2	BUO 5	Risk 5	Low	Low	Low	BP 4
OO 3	BUO 6	Risk 6	High	Medium	Low	BP 5
OO 3	BUO 7	Risk 6	High	Medium	Low	BP 6
OO 3	BUO 8	Risk 7	Medium	Low	Low	BP 6

We've linked corporate/organisational objective to business processes and used this information to identify the auditable units. The auditable unit are:

- Specific risks within a business process,
- All risks relating to a specific business unit,
- A group of risk that fall into a certain category or
- A specific risk as a stand-alone.

This is dependant on the internal auditors' judgement of most logical or efficient grouping of risks in the annual audit plan.

When we focus our attention back to the IT infrastructure elements we realise that we still have a gap. The IT related risks in the risk universe are specific to processes that exist within the IT Department that support the corporate objectives directly, for example the effective management of third party services. There is still uncertainty of what the risky IT infrastructure elements are that should be audited.

Mapping IT infrastructure elements to business processes

As explained under the heading 'Corporate objectives (Step 1 and 2 in determining the annual audit plan as described above)', IT departments also link their business unit objectives back to the organisational objectives. The same goes for IT process objectives. This, however, is only one aspect of IT that needs to be included in the annual audit plan. The other aspect is the linkage between the business process and the IT infrastructure elements or phrased differently, the access path to the business process.

Once the risks are mapped to these business processes and their related IT infrastructure elements, the IT dependency of such processes needs to be determined. The business process priority is determined by assessing the importance of that business process is to the organisation. The IT dependency is the reliance the business process places on IT to function. The highest IT priority is therefore based on the high priority business processes with a high reliance on IT.

To explain further – a business process is performed either:

- Manually (by a human without IT assistance),
- Automated (entirely dependant on IT, with little or no human intervention) or
- Partially automated (both human intervention and IT is required).

For IT audit plan the IT dependency of the business processes need to be assessed. For example, automated processes might be assessed as highly dependant on IT, partially automated processes as medium dependency and manual business processes as low or no dependency on IT.

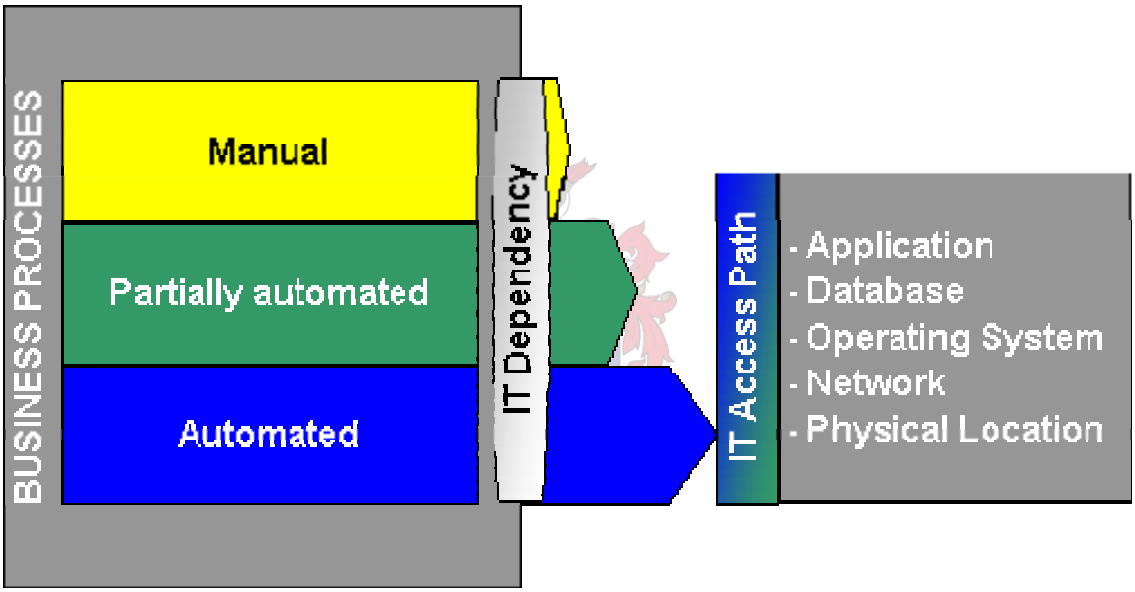
These business processes are, in turn, mapped to the underlying infrastructure elements and are used to determine the IT auditable unit/area.

For each business process with a high IT dependency (and medium, dependant on the requirement from the Audit Committee and business sector), the IT Infrastructure elements are included in the IT audit plan. These

will include the applications supporting the business process, the data management systems that these applications run on, the underlying operating system, the network and the physical location of the machines where the technology resides.

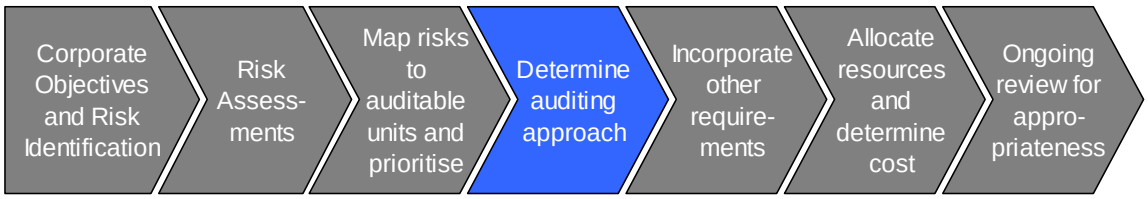
Once the linking is complete it is easier to see which application, databases, operating systems, network or data centres should be audited. The priority for auditing the IT infrastructure elements is determined by considering the priorities of the business processes, which it supports, the number of business processes that it impacts as well its IT dependency.

Schematically it can be described as follows:



A risk assessment can also be performed for each IT infrastructure element and the approach to auditing will be the same as tabled under risk assessment above. This level of detail is excluded from the scope for this assignment and examples will therefore not be given.

Determine the auditing approach for the identified auditable units (Step 7 in determining the annual audit plan as described above)



For auditing purposes these risks and their combinations can be used to determine the area and depth of audit work. This can be based on the combination of inherent and residual risk assessments, as well as the organisation's risk appetite.

The table following can be used as a guideline in determining the audit strategy/approach. Normative measures, i.e. descriptions of high, medium and low risk, are used to simplify risk assessment. Inherent risk (IR), Risk appetite (RA) and Residual risk (RR) are used in combination to determine this approach.

To explain the functioning of the table: Where IR, RR and RA, for example are all high, no audit testing is required. IR and RA are the same and imply that management accepts that level of risk. However, the level of risk acceptance need to be assessed by Internal Audit (IA) and reported to the respective Chief Executive Officer (CEO) and Audit Committee (AC).

Where RA is lower than the IR, it implies that management desire key controls to be in place to mitigate the risk. Where the RR is lower than the RA, it implies that there are more controls in place to mitigate the risk than what management is prepared to live with, i.e. over-controlled resulting in over-expenditure. Here the level of risk acceptance needs to be assessed by IA and reported to the respective CEO and AC. IA also needs to determine if the key controls are in fact in place to address the risk as the RR indicates.

These and other combinations are illustrated in the following table:

Linking Risk Assessments to Audit approach

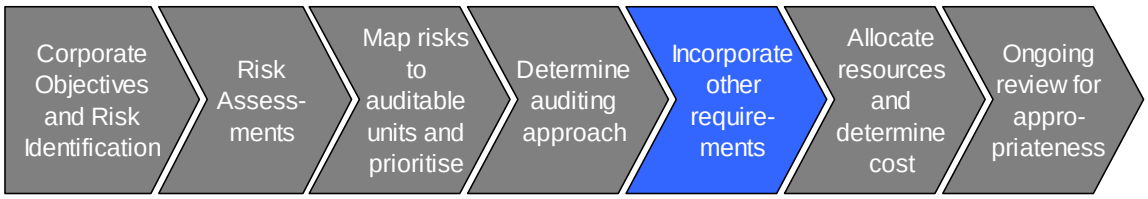
IR	RA	RR	Management appetite based on IR and RA	Audit depth / approach based on combination of IR, RA & RR	
H	H	H	Accepts risk, require no additional controls	Communication	Confirm risk acceptance with CEO and ACC, highlight potential impact, apply auditor's judgement, and voice any concerns.
H	H	M	Accepts risk, require no additional controls	Communication	Confirm risk acceptance with CEO and ACC. Highlight potential impact and possible over control ito RA. Apply auditor's judgement and voice any concerns.
H	H	L	Accepts risk, require no additional controls	Communication	Confirm risk acceptance with CEO and ACC. Highlight potential impact and possible over control ito RA. Apply auditor's judgement and voice any concerns.
H	M	H	Accepts some risk, require key controls	Assess Action	Assess management actions plans to reach desired risk appetite
H	M	M	Accepts some risk, require key controls	Communication and limited audit	Confirm risk acceptance with CEO and ACC and highlight potential impact. Perform audit on key controls implemented.
H	M	L	Accepts some risk, require key controls	Communication and limited audit	Confirm risk acceptance with CEO and ACC. Highlight potential impact and possible over control ito RA. Perform audit on implemented key controls
H	L	H	Require good control environment	Assess Action	Assess management actions plans to reach desired risk appetite
H	L	M	Require good control environment	Assess Action and limited audit	Assess management actions plans to reach desired risk appetite and perform audit on implemented controls
H	L	L	Require good control environment	Confirm good control environment	Perform audit on implemented controls to confirm existing good control environment.
M	M	M	Accepts risk, require no additional controls	Communication	Confirm risk acceptance with CEO and ACC and highlight potential impact OR request management to perform CSA.
M	M	L	Accepts risk, require no additional controls	Communication	Confirm risk acceptance with CEO and ACC. Highlight potential impact and possible over control ito RA OR request management to perform CSA.
M	L	M	Require good control environment	Assess Action	Assess management actions plans to reach desired risk appetite OR request management to perform CSA.
M	L	L	Require good control environment	Confirm good control environment	Perform audit on implemented controls to confirm existing good control environment OR request management to perform CSA.
L	L	L	Require control environment	Confirm good control environment	Detailed review of controls in place to manage the risk OR request management to perform CSA.

Abbreviations

H	High risk assessment
M	Medium risk assessment
L	Low risk assessment
CEO	Chief Executive Officer
ACC	Audit Committee Chair
CSA	Control Self Assessment

This approach will also be applicable to the IT infrastructure elements once their risk assessment has been performed.

Incorporate other requirements (Step 8 in determining the annual audit plan as described above)



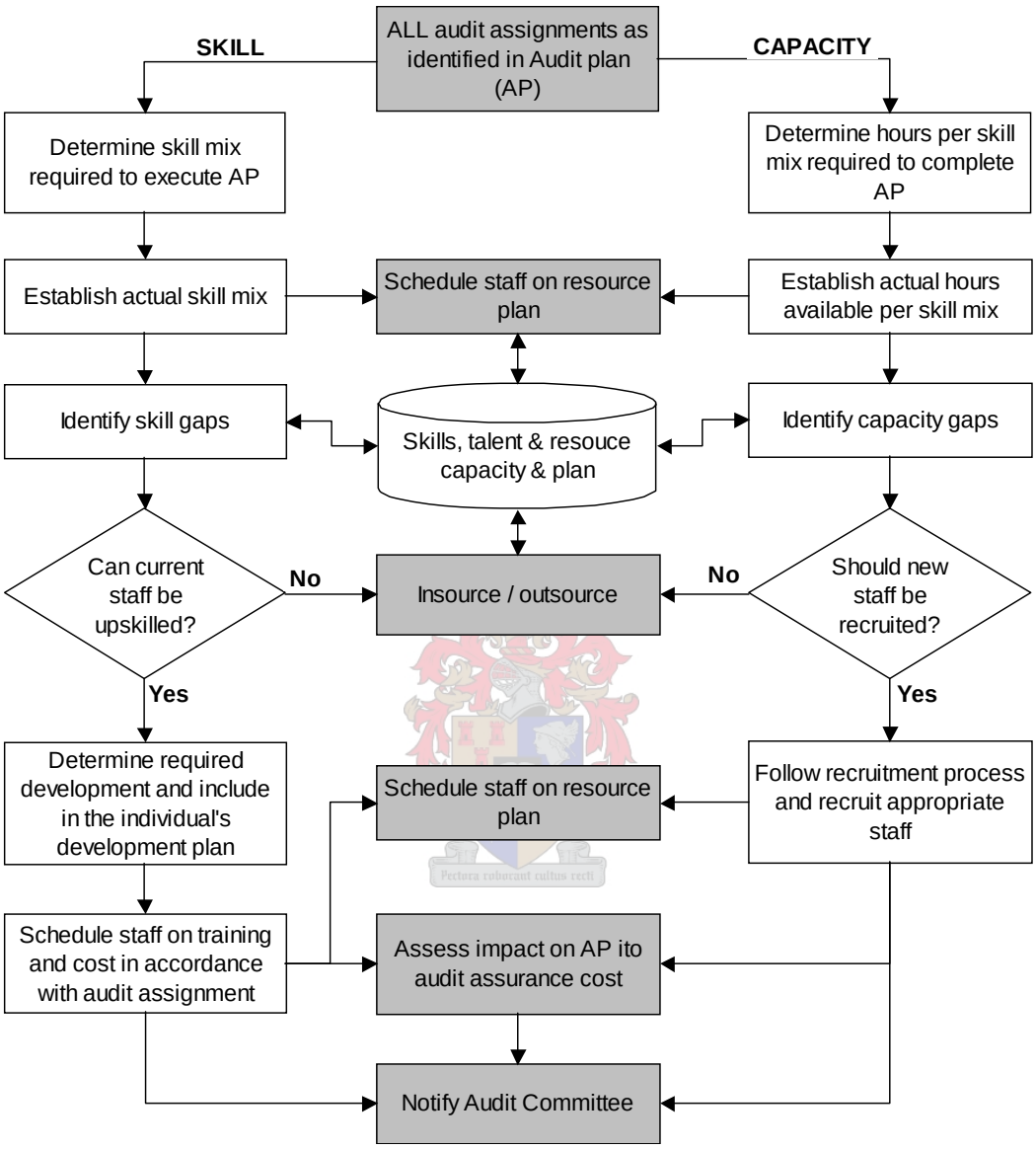
Other requirements should be considered for incorporation into the audit plan. These requirements could be specific requests from the audit committee; it could be previously reported concerns that need to be followed up on; or requirements from the management board. These requests need to be considered in conjunction with the overall audit plan, e.g. audit priorities.

Resources and Cost (Step 9 in determining the annual audit plan as described above)

Resource requirements are 'an estimated range of level of effort required to carry out the project. The effort estimate should take into consideration the following factors:

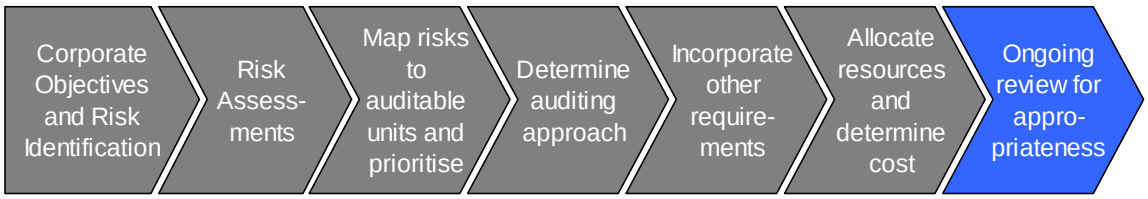
- The type and level of audit engagement (assurance, consulting).
- The scope of the engagement (including consideration for audit period, business process, business objectives to be assessed).
- The complexity of the audit subject, business processes and systems in scope.
- The availability of internal audit and subject matter expertise.
- The quality and quantity of existing documentation in the subject area.
- The audit approach and techniques to be used (e.g. interviews, transaction sampling, workshops, computer aided tools, etc.).'

The following decision tree may be used to assist developing the resource plan:



Once resource requirements and availability is determined, the cost of the audit plan can be calculated based on the applicable charge-out rates. If applicable, the Audit plan can be presented to the Audit Committee for approval.

Ongoing review (Step 10 in determining the annual audit plan as described above)



It is important to remember that the risk profile might change and that the audit plan should be adjusted accordingly. Therefore, it is recommended to review the appropriateness of the audit plan in relation to organisational changes and needs, at least every six months.

The audit plan will also be subject to an approval process specific to the organisation, which needs to be obtained before execution of the audit assignments.

Where does CobiT fit in?

Understanding CobiT

We now understand where IT fits into RBIA – what part of IT and how IT could be included in the audit plan. What we don't understand is where the CobiT framework fits into it. 'The CobiT Framework provides a tool for the business process owner that facilitates the discharge of this responsibility. The Framework starts from a simple and pragmatic premise: In order to provide the information that the organisation needs to achieve its objectives, IT resources need to be managed by a set of naturally grouped processes.

The Framework continues with a set of 34 high-level Control Objectives, one for each of the IT processes, grouped into four domains:

- Planning and organisation (with 11 high level control objectives)
- Acquisition and implementation (with 6 high level control objectives)
- Delivery and support (with 13 high level control objectives)
- Monitoring (with 4 high level control objectives).

This structure covers all aspects of information technology that supports a business. By addressing these 34 high-level control objectives, the business process owner can ensure that an adequate control system is provided for the IT environment.' [3]

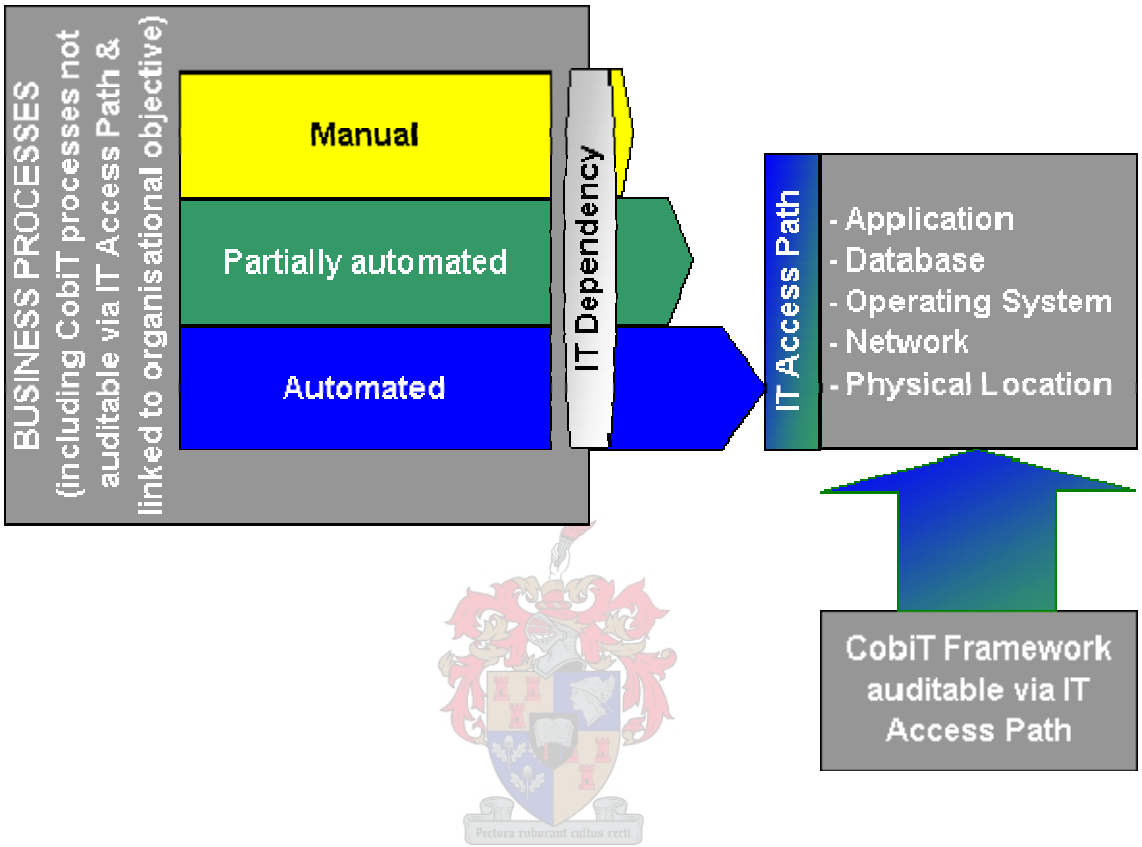
Therefore, when executing the audit for an infrastructure element, the IT processes as defined by CobiT can be used as benchmark (best practice) to assess how well that specific element is managed.

While designing the controls for an organisation, management can use CobiT as a framework to link IT processes or control objectives to their identified risks (after performing a cost-benefit analysis). Auditors can use CobiT as a framework to compare the organisation's system of internal control against, considering what is best suited for the specific organisation.

It should be noted that, when using CobiT as a framework as a basis for an audit assignment that some CobiT processes should be considered as

independent processes. Other processes may be audited through the infrastructure elements. The point of departure is that the organisation's objectives remain the starting point.

We can summarise the above by means of the following diagram:



Auditing via CobiT Processes

The following table provides a guide on where CobiT fits into the audit process, i.e. auditing the CobiT Process through infrastructure or as a business process:

CobiT Process		Audit via Infrastructure?	Audit as Business Process?	Reason
Domain: Planning and Organising				
PO1	Define a Strategic IT Plan	No	Yes	A strategic planning process encompass the entire IT environment and is not limited to certain infrastructure elements. Thus this is better audited as a business process.
PO2	Define the Information Architecture	No	Yes	This process satisfies the business requirement of optimising the information systems. Thus an overview picture of the entire IT infrastructure.
PO3	Determine the Technology Direction	No	Yes	Here available and emerging technology is considered to drive and make possible the business strategy. Best audited as a business process.
PO4	Define the IT Organisation and Relationships	No	Yes	This process is focussed on delivering the right IT services through an organisation suitable in numbers and skills. Thus looking at the broader picture.
PO5	Manage the IT Investment	No	Yes	Funding and control over disbursement of financial resources relates to the entire IT investment and is best audited as a business process.
PO6	Communicate Management Aims and Direction	No	Yes	The communication of management's aims and direction is to ensure awareness and understanding of those aims at a high level and is not infrastructure specific.
PO7	Manage Human Resources	No	Yes	Sound, fair and transparent personnel management practices are for the entire IT department and therefore best audited as a business process.
PO8	Ensure Compliance with External Requirements	Yes	Yes	Legal, regulatory and contractual obligations can be at a business process as well as infrastructure layer, e.g. corporate licensing or a licence for a specific database.
PO9	Assess Risks	Yes	Yes	The business process that can be audited include the risk assessment methodology, whilst the application of this methodology can be audited via the infrastructure.

CobiT Process		Audit via Infrastructure?	Audit as Business Process?	Reason
Domain: Planning and Organising, continued				
PO10	Manage Projects	No	Yes	Projects are aimed at implementation of systems and is not live in production. Therefore this CobiT process is best audited as a business process.
PO11	Manage Quality	No	Yes	This process is aimed at the planning, implementing and maintaining of quality management standards and systems and is best audited as a business process.
Domain: Acquisition and Implementation				
AI1	Identify Automated Solutions	No	Yes	This process identifies alternative opportunities measured against user requirements. Therefore there is no infrastructure element to audit yet.
AI2	Acquire and Maintain Application Software	No	Yes	Mostly system development life cycle control objectives are included in this process. These refer to pre-production applications, which is best audited as a business process.
AI3	Acquire and Maintain Technology Infrastructure	Yes	Yes	Installations referred to in this process are pre-production and are best audited as a business process, while maintenance is best audited via the infrastructure elements.
AI4	Develop and Maintain Procedures	Yes	Yes	As a business process, structured approach to develop manuals can be audited or alternatively audited via the infrastructure to ensure these are up-to-date.
AI5	Install and Accredit Systems	No	Yes	This process is enabled by the realisation of a well-formalised installation migration, conversion and acceptance plan. Therefore it can be viewed as pre-implementation.
AI6	Manage Changes	Yes	No	The objective of the process is to minimise the likelihood of disruption, unauthorised alteration and errors. It is infrastructure specific and therefore audited as such.
Domain: Delivery and Support				
DS1	Define and Manage Service Levels	Yes	Yes	The overall measurement of service levels can be audited as a business process or alternatively the service level per infrastructure element, e.g. response times.
DS2	Manage Third-party Services	Only if directly linked	Yes	Ideally this is best audited as a business process as third party management is normally a centralised process, unless the service is directly linked to the infrastructure.

CobiT Process		Audit via Infrastructure?	Audit as Business Process?	Reason
Domain: Delivery and Support, *continued*				
DS3	Manage Performance and Capacity	Yes	Yes	The performance and capacity trends should be analysed both at a business process level as well as a infrastructure level to ensure availability and best usage.
DS4	Ensure Continuous Service	Yes	Yes	The IT continuity plan, in line with the business plan can be audited as a business process, while the implementation of this plan can be audited in relation to the infrastructure.
DS5	Ensure Systems Security	Yes	Yes	The centralised security administration is something that can be audited as a business process, while user account management, for example, can be audited via infrastructure.
DS6	Identify and Allocate Costs	No	Yes	This CobiT process is enabled by a cost accounting system to ensure an awareness of the costs attributable to IT services, which is best audited as a business process.
DS7	Educate and Train Users	No	Yes	A training and development plan should be in place to ensure effective use of IT and awareness of risks and responsibilities. This is best audited as a business process.
DS8	Assist and Advise Customers	No	Yes	The helpdesk function is best audited as a business process. Root cause analysis and problem tracking that can be traced back to the infrastructure should be identified.
DS9	Manage the Configuration	Yes	Yes	The configuration management procedure is something that can be audited as a business process, while the configuration baseline is infrastructure specific.
DS10	Manage Problems and Incidents	Yes	No	This CobiT process' objective is to ensure that problems and incidents are resolved, and the cause investigated to prevent recurrence. It is infrastructure specific.
DS11	Manage Data	Yes	No	The objective of this CobiT process is to ensure that data remains complete, accurate and valid during input, update and storage. This is infrastructure specific (databases).
DS12	Manage Facilities	Yes	Yes	This process can be used as guideline when the physical location of an IT infrastructure element is audited. It can, however, also be used as a business process to be audited.

CobiT Process		Audit via Infrastructure?	Audit as Business Process?	Reason
Domain: Delivery and Support, *continued*				
DS13	Manage Operations	Yes	Yes	This CobiT process relates to support activities which is to be recorded and cleared. This can be audited via the business processes or infrastructure.
Domain: Monitoring				
M1	Monitor the processes	Yes	Yes	This process refers to the management information system that can be utilised for and therefore audited via business processes or infrastructure.
M2	Assess Internal Control Adequacy	No	Yes	This process relates to monitoring and reporting of internal controls' effectiveness. It is thus best audited as a business process on its own.
M3	Obtain Independent Assurance	No	Yes	These relate to the internal and external audit functions, who cannot audit themselves, but certain teams can be appointed to ensure the quality of these functions.
M4	Provide for Independent Audit	No	Yes	

Chapter 4

Results

When the process as explained in the previous chapter is followed, one can typically expect the following type of output:

Organisational Objective (OO)	Business Unit Objective (BUO)	Risk	Risk			Business Process (BP)	Priority (P)	IT Dependancy (D)	IT Priority (ITP)	CobiT Processes that can be used as guideline during IT Infrastructure audits:				
			IR	RA	RR					Bought or Built Applications (APP)	Database (DB)	Operating System (OS)	Network (NW)	Physical Location
Examples:										PO8 Ensure Compliance with External Requirements PO9 Assess Risks AI4 Develop and Maintain Procedures AI6 Manage Changes DS1 Define and Maintain Procedures DS2 Manage Third-Party Services Levels DS3 Manage Performance and Capacity DS4 Ensure Continuous Service DS5 Ensure System Security DS9 Manage the Configuration DS10 Manage Problems and Incidents	PO2 Define the Information Architecture PO8 Ensure Compliance with External Requirements PO9 Assess Risks AI4 Develop and Maintain Procedures AI6 Manage Changes DS1 Define and Maintain Procedures DS2 Manage Third-Party Services Levels DS3 Manage Performance and Capacity DS4 Ensure Continuous Service DS5 Ensure System Security DS9 Manage the Configuration DS10 Manage Problems and Incidents DS11 Manage Data DS13 Manage Operations	PO8 Ensure Compliance with External Requirements PO9 Assess Risks AI3 Acquire and Maintain Technology Infrastructure AI4 Develop and Maintain Procedures AI6 Manage Changes DS1 Define and Maintain Procedures DS2 Manage Third-Party Services Levels DS3 Manage Performance and Capacity DS4 Ensure Continuous Service DS5 Ensure System Security DS9 Manage the Configuration DS10 Manage Problems and Incidents	PO8 Ensure Compliance with External Requirements PO9 Assess Risks AI6 Manage Changes AI3 Acquire and Maintain Technology Infrastructure DS1 Define and Maintain Procedures DS2 Manage Third-Party Services Levels DS3 Manage Performance and Capacity DS4 Ensure Continuous Service DS5 Ensure System Security DS9 Manage the Configuration DS10 Manage Problems and Incidents DS13 Manage Operations	PO8 Ensure Compliance with External Requirements PO9 Assess Risks AI4 Develop and Maintain Procedures DS1 Define and Maintain Procedures DS4 Ensure Continuous Service DS10 Manage Problems and Incidents DS12 Manage Facilities
OO 1	BUO 1	Risk 1	H	L	H	BP 1	P1	D_Low	ITP0	None	None	None	None	None
OO 1	BUO 2	Risk 2	M	L	M	BP 1	P6	D_High	ITP3	APP1	DB1	OS1	NW1	Offsite server room
OO 1	BUO 3	Risk 2	M	L	M	BP 2	P8	D_Medium	ITP6	APP2	DB2	OS2	NW1	Offsite server room
OO 1	BUO 3	Risk 3	H	H	H	BP 3	P2	D_High	ITP1	APP3	DB2	OS2	NW1	Offsite server room
OO 2	BUO 4	Risk 3	H	H	H	BP 4	P3	D_Medium	ITP2	APP4	DB2	OS2	NW1	Offsite server room
OO 2	BUO 5	Risk 5	L	L	L	BP 4	P9	D_Medium	ITP7	APP4	DB3	OS3	NW2	Onsite server room
OO 3	BUO 6	Risk 6	H	M	L	BP 5	P4	D_Low	ITP0	None	None	None	None	None
OO 3	BUO 7	Risk 6	H	M	L	BP 6	P5	D_Medium	ITP4	APP5	DB3	OS3	NW2	Onsite server room
OO 3	BUO 8	Risk 7	M	L	L	BP 6	P7	D_High	ITP5	APP6	DB4	OS3	NW2	Onsite server room

WHERE:
IR = Inherent Risk
RA = Risk Appetite
RR = Risidual Risk
H = Risk assessed as high
M = Risk assessed as Medium
L = Risk assessed as Low

CobiT Processes not included:

Planning and Organisation:

PO1 Define a Strategic information Technology plan

PO3 Determine the Technology Direction

PO4 Define the Information Technology Organisation and Relationship

PO5 Manage the Information Technology Investment

PO6 Communicate Management Aims and Direction

PO7 Manage Human Resources

PO10 Manage Projects

PO11 Manage Quality

Acquisition and Implementation*:*

AI1 Identify Automated Solutions

AI2 Acquire and Maintain Application Software

AI5 Install and Accredit Systems

Delivery and Support:

DS6 Identify and Allocate Costs

DS7 Educate and Train Users

DS8 Assist and Advise Customers

These CobiT processes should be included in the audit plan where it is linked to the respective organisational objectives. The CobiT processes can also be used as guidance to determine which best practice controls should be in place for these processes.

IT Infrastructure Annual Audit plan

Example of Auditable IT Infrastructure Elements:

IT Priority (ITP)	IT Infrastructure Category	IT Infrastructure Elements	IR	RA	RR	IT Ranking (ITR)	Audit Approach
ITP3	Bought Application	APP1	H	L	H	ITR7	Assess Action
ITP6	Built Application	APP2	H	L	M	ITR12	Assess Action and limited audit
ITP1	Bought Application	APP3	M	L	L	ITR13	Confirm good control environment
ITP2&7	Bought Application	APP4	H	L	L	ITR5	Confirm good control environment
ITP4	Built Application	APP5	H	L	L	ITR8	Confirm good control environment
ITP5	Built Application	APP6	H	L	L	ITR9	Confirm good control environment
ITP3	Database	DB1	L	L	L	ITR17	Request CSA
ITP1,2 & 6	Database	DB2	H	L	M	ITR3	Assess Action and limited audit
ITP4&7	Database	DB3	M	L	L	ITR14	Confirm good control environment
ITP5	Database	DB4	M	L	L	ITR15	Confirm good control environment
ITP3	Operating System	OS1	L	L	L	ITR16	Request CSA
ITP1,2 & 6	Operating System	OS2	H	L	M	ITR2	Assess Action and limited audit
ITP4,5 & 7	Operating System	OS3	M	L	M	ITR11	Assess Action
ITP1,2,3&6	Network	NW1	H	L	L	ITR1	Confirm good control environment
ITP4,5 & 7	Network	NW2	M	L	L	ITR10	Confirm good control environment
ITP1,2,3&6	Physical	Offsite server room	M	L	M	ITR4	Assess Action
ITP4,5 & 7	Physical	Onsite server room	M	L	L	ITR6	Confirm good control environment

The IT ranking (ITR) was determined by using the combination of ITP and risk assessments.

Chapter 5

Conclusion

Technique to fit IT in RBIA

We have established a technique to include IT in RBIA by following a risk-based audit approach whilst developing the annual audit plan. The following steps discussed in the previous chapters can be highlighted:

- The starting point was the organisational objectives and the risks that prevent their achievement
- The risks were assessed and these assessments were used to determine the priority and audit approach
- Business risks were linked to the processes identified
- IT Infrastructure elements that support high priority business processes were included in the audit plan
- These were ranked according to the risk assessment of the business process, the IT dependency of the business process and the risk assessments of the IT infrastructure elements.

Conclusion on CobiT result

When we look at the CobiT processes that are included to be audited through the IT infrastructure elements, it is evident that they are mostly the Delivery and Support type processes. It makes sense if one remembers that this is exactly what IT infrastructure elements do – they deliver and support business processes.

The Planning and Organisation, as well as the Acquisition and Implementation CobiT processes, are processes that should be assessed alongside other business processes. They should be linked to specific corporate objectives rather than IT infrastructure. Their specific risks should be identified and assessed. This also makes sense when one thinks that these are processes

required to run an IT department, rather than supporting other business processes.

[1] *Position Statement: Risk Based Internal Auditing* 2003, Institute of Internal Auditors – UK and Ireland, [Online], Retrieved: 27 September 2004 http://www.blindtiger.co.uk/IIA/uploads/48dc2e62-f2a7bd939a--7cee/RiskBasedInternalAuditing.pdf

[2] King Committee on Corporate Governance and the Institute of Directors 2002, *King Report on Corporate Governance for South Africa* 2002, Institute of Directors in Southern Africa, South Africa, pp 78, 80, 90, 137 & 138

[3] IT Governance Institute 2000, *Control Objectives COBIT® Governance, Control and Audit for Information and Related Technology*, 3rd Edition, Information Systems Audit and Control Foundation (ISACF), United States of America, pp 5 & 6

[4] Ahituv, Niv & Neumann, Seev 1990, *Principles of Information Systems for Management*, Third Edition, Wm. C. Brown Publishers, United States of America, pp2

[5] Griffiths, David M. 2003, 'Internal Auditing – A Risky Biz. The Practical Application of Risk-Based Auditing', v1.1.0, [Online], Retrieved: 27 September 2004 http://www.internalaudit.biz/files/web/Internalauditv1.1.0.doc

[6] McNamee, David & Selim, Georges 1998, 'Risk Management: Changing the Paradigm', *Mc2 Management Consulting Article*, Retrieved: 27 September 2004 http:// www.mc2consulting.com/riskart8.htm

[7] *Risk-Based Internal Audit Priorities Toolset for Small Departments and Agencies* 2003, Treasury Board of Canada Secretariat, [Online], Retrieved: 27 September 2004 http://www.tbs-sct.gc.ca/ia-vi/policies-politiques/priorities-priorites/priorities-priorites_e.pdf

[8] Niblett, Peter & Wechsler, Sander S. 2003, 'The IS Auditor's Consideration of Irregularities and Illegal Acts', *Information Systems Control Journal*, vol. 3, pp 57