Configuration management data base in an information and communication technology environment

by

TJ MEDUPE

20745094

Mini-dissertation submitted in partial fulfilment of the requirements for the degree *Masters of Business Administration* at the North-West University

Study leader: Mr. JC Coetzee

POTCHEFSTROOM

November 2009

ABSTRACT

There are more requirements for business to be able to run its operations successfully in terms of legal compliance and revenue streams optimisations. Businesses are placing high demands on Information and Communication Technology (ICT) to adapt to changing conditions. However, ICT organisations tasked with providing increased service levels at lower costs do not have the resources to reinvent itself with every technological or regulatory change. Without frameworks in place to leverage automation and best practices, these ICT, organisations are consumed with the day-to-day operations of ICT with little time and few resources left to develop new services that add value to the business. There is, therefore, a definite requirement for a central repository system in order to enhance ICT service delivery and strategy for continuing to improve service, lowering per-service delivery costs and enabling ICT organisations to bring new services that support competitive advantages.

The company of choice in the study is Sentech, which has recently adopted some of the Information Technology Infrastructure Library (ITIL) processes; these are service desk, incident management, and change management. The company is still in the middle of deciding on whether to implement the configuration management process which will eventually lead to Configuration Management Database (CMDB).

This study attempted to indicate the role and the importance of running the CMDB together with the rest of other ITIL processes. The study also indicated how the other processes cannot function effectively without a proper CMDB platform. The primary objective of the study was to identify the importance and the role of CMDB in an ICT environment.

The organisation implemented a number of processes such as configuration and change management. To be successful with using the ITIL change management process, it is important that the people, processes, and technologies work together in a coordinated manner to overcome the political roadblocks that usually inhibit cooperation between groups in the same organisation. The study has indicated that the current ITIL processes, such as change management are not achieving the required results due to a lack of proper CMDB.

General recommendations on the implementation of the CMDB based on the study were:

- Get executive and Board of Directors' support on the implementation of CMDB.
- The organisation needs to redefine the role of the General Manager - ICT to a more appropriate role of Chief Information Officer reporting directly to the board.
- The organisation must define detailed business processes and procedures.
- The organisation must set a clear scope of the CMDB.
- The relevant stakeholders on the CMDB must be identified.
- A full state of the current ICT processes must be determined.
- The business case on the CMDB must be formulated and documented.
- Set goals on what the CMDB will have to achieve.
- The organisation must create a plan on the implementation of the CMDB.
- Identify responsibilities on maintaining the CMDB.
- Create awareness within the organisation around CMDB.
- Training on CMDB must be offered to the personnel.
- The organisation must baseline all ICT assets.
- Plan for ongoing management of the CMDB.

It is believed that the objective of the study has been met. From the investigation, it has been clear that there is a dire need for an implementation of a central repository system like the CMDB to support other service delivery and support processes. If the recommendations are implemented within Sentech, the company will secure a more effective and efficient service delivery on the ICT platform. Furthermore, Sentech can become an ICT leader and gain a competitive advantage over its fellow competitors.

Key terms: Information technology infrastructure library; service desk; incident management; change management; configuration management database; information and communication technology; Sentech.

TABLE OF CONTENTS

TABLE OF CONTENTS (continued)

TABLE OF CONTENTS (continued)

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

BIA	Business Impact Analysis
BSM	Business Service Management
CIO	Chief Information Officer
CMDB	Configuration Management Database
CMS	Configuration Management System
COBIT	Control Objectives for Information and related Technology
ERP	enterprise resource planning
ICT	Information and Communication Technology
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITSCM	Information Technology Service Continuity Manager
ITSM	Information Technology Service Management
KPIs	Key Performance Indicators
MTN	Mobile Telephony Networks
RFC's	Requests For Change
ROI	Return on investment
SLAs	Service Level Agreements
SMART	Self-Monitoring, Analysis and Reporting Technology
SOX	Sarbanes-Oxley-Act

CHAPTER 1

NATURE AND SCOPE OF THE STUDY

1.1 INTRODUCTION

Organisations recognise a need of depending on Information and Communication Technology (ICT) in order to satisfy their strategic aim and meet business needs. This increasing dependency leads to growing requirements for high quality ICT services which are matched to business needs and user requirements. Increased competitive pressure upon business is continuing to escalate, generating the need for greater efficiency and productivity. Breakthroughs in technology-based services and solutions are driving frequent, rapid, and serendipitous changes in business strategies subsequently placing demand upon information technology for supporting services and solutions required to achieve sustained competitive advantage (Ness, 2005:1).

The main point of discussion will be revolving around Configuration Management Database (CMDB) in an ICT environment concentrating on Information Technology Infrastructure Library (ITIL) as best practice. CMDB represents the best thinking of thousand people about how ICT should be run, what impact can ICT has on the business it supports, and how to get the most value from the investment made on ICT infrastructure (Klosterboer, 2008:32). One of the stated goals of ITIL is to help decision makers make better decisions by ensuring that adequate ICT information is available to support those decisions. Configuration management is the discipline of identifying, tracking, and controlling the various components of the ICT environment, and it is this information that enables decision making. Configuration management covers the identification, recording and reporting of the ICT components, including its versions, constituent components and relationships (Dettmer & Watson, 2006:4).

Configuration management is tasked with capturing, keeping and providing up-to-date information about the ICT infrastructure. It aims to provide reliable detail about the ICT infrastructure, and also detail of the specific items in the infrastructure, that which configuration management refers to as *configuration items* (Lee, 2006:2). One of the

most important characteristics of configuration management is how it relates these configurations Items to one another. If ICT organisations are to improve services significantly, a well-run CMDB is critical.

1.2 FACTORS WHICH LED TO THE STUDY

The factors which prompted this particular study come from the experience that I have acquired working within the ICT environment.

The following are the factors:

- Lack of standardisation call categorisation and prioritisation schemes in most cases resulted in limited meaningful management information that can be extracted from the CMDB platform.
- Incomplete definition of the service level users expected.
- Users experienced inconsistent service, attributed largely around roles and responsibilities on whom to contact within departments.
- Formal service catalogue and identification of staff responsibilities have not been undertaken.
- Incorrect priorities on the service impact are assigned on changed request due to a lack of understanding of the network topology.
- High level support consultants regularly attend to front-line enquiries and resolve minor incidents which could have been resolved by the first line support; hence there is an improper appropriation of resources and junior staff members do not get developed and empowered.
- Problems are escalated to second level or higher staff members without proper fault description and logging.
- Lack of CMDB, with no relationships identified between components.
- Lack of Systematic means of identifying the staff training requirements.
- Inadequate documentation of major changes.

1.3 PROBLEM STATEMENT

Businesses are placing high demands on ICT to adapt to changing conditions. However, ICT organisations tasked with providing increased service levels at lower costs do not have the resources available to reinvent themselves with every technological or regulatory change. Without frameworks in place to leverage automation and best practices, ICT organisations are consumed with the day-to-day operations of ICT with little time and few resources left to develop new services that add value to the business. Thus CMDB needs to be considered as a central part of a strategy for continuing to improve service, lowering per-service delivery costs and enabling ICT organisations to bring new services that support competitive advantages.

Some of the main causes of the organisations not being able to provide improved service levels are the following:

- Lack of CMDB, with no relationship indentified between components.
- Formal service catalogue and identification of staff responsibilities have not been undertaken.
- Lack of standardised call categorisation and prioritisation schemes result in limited meaningful management information that can be extracted from the CMDB.
- Poor coordination of changes to services which impact directly on the wider company's operations.
- Lack of trend analysis to be able to quickly resolve recurring system faults
- Lack and poor events correlations which would assist in finding common causes of problems.

1.4 OBJECTIVES OF THE STUDY

The research objectives are divided into general and specific objectives.

1.4.1 Primary objective

The main objective of the study is to identify the importance and the role of CMDB in an ICT environment.

1.4.2 Secondary objectives

The above-mentioned main objectives can be actualised through the following subsequent sub objectives:

- To clearly define what Configuration Management and CMDB are all about.
- To address the question of how the rest of the ITIL processes are linked to CMDB and how these processes cannot be effectively implemented and executed without a proper CMDB in place.
- Highlight the business value of having a complete and comprehensive CMDB.
- To indicate how the correct CMDB will enable management to make good decisions.
- Show the CMDB as a basis for cost savings and process optimisation.

1.5 SCOPE OF THE STUDY

The focus of this study is on the role and importance of CMDB looking into Sentech Limited as a platform. Sentech is a service provider concentrating on ICT offering and Signal Distribution as its core business area. The main clients of Sentech are South African Broadcasting Television (SABC) and free to air channel e-TV. The other clients are Vodacom, Cell C and Mobile Telephony Networks (MTN).

This company of choice has recently adopted some of the processes outlined on ITIL and these are Service Desk, Incident Management, Change Management and Service Management. The company is still in the middle of deciding on whether to implement the Configuration Management processes which will eventually lead into CMDB.

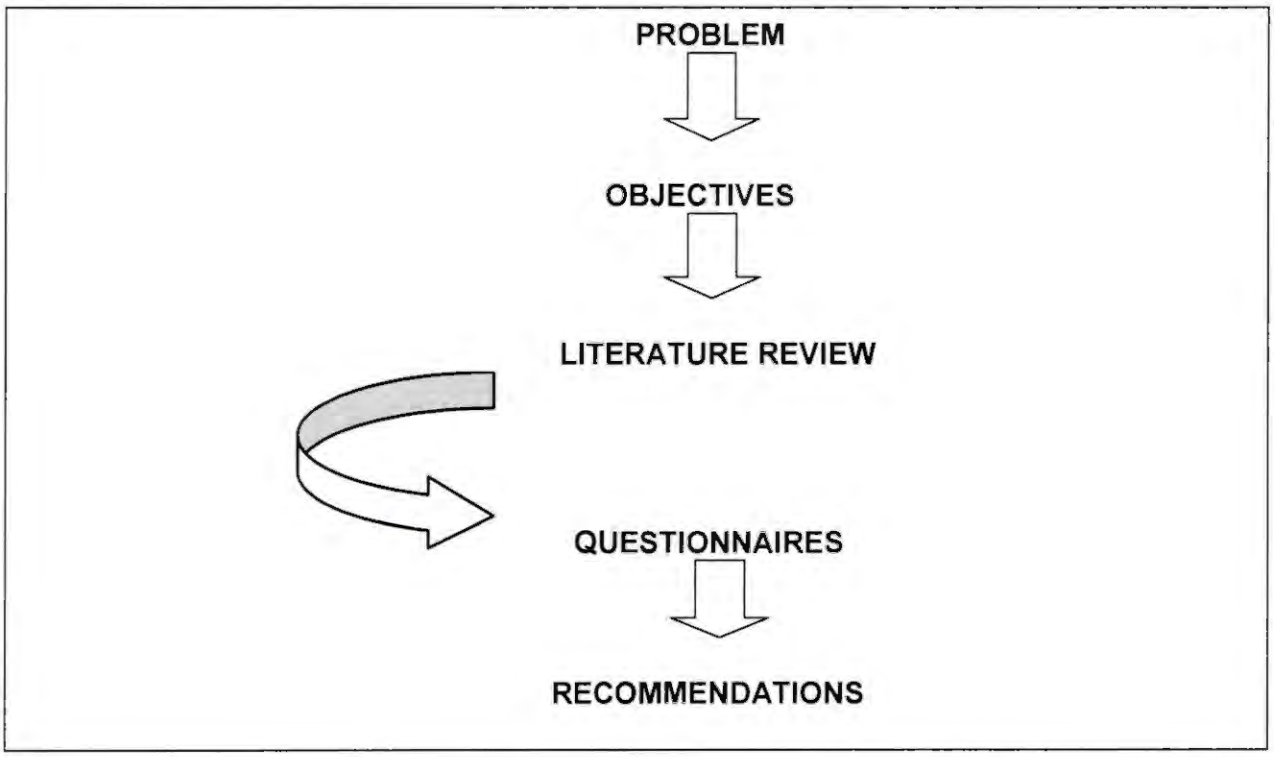
This research will seek to indicate the role and the importance of running the CMDB together with the rest of other ITIL processes. The study also seeks to indicate how the other processes cannot function effectively without a proper CMDB platform.

This research, pertaining to the specific objectives, consists of two phases, namely a literature review and an empirical study.

1.6 RESEARCH METHODOLOGY

The basic research process followed in this study is summarised below in Figure 1.1.

Figure 1.1: Summary of the structure of the study



As illustrated in figure 1.1 the study starts with a problem statement that must be solved. The objectives flow from the problem statement of the study. The empirical research is conducted through the handing out of a set of structured questionnaires. The recommendations will be made towards the adoption of A CMDB system.

The research methodology consists of the execution of the literature review restricted to ITIL and other best practises concentrating specifically on Configuration Management and CMDB.

Revisit the current ITIL processes implemented within Sentech and the success achieved. The empirical study was undertaken by means of questionnaires compiled with the assistance of the head of department of the process office within Sentech. Questionnaires were disseminated to staff members, ranging from junior management, middle management and top management level to complete.

Data collected from the questionnaires were statistically analysed by the Statistical Consultation Services of the North-West University. Recommendations are made about the future plans, as well as aspects included in the primary and secondary objectives of the study.

1.7 LIMITATIONS OF THE STUDY

This study is limited to the borders of South Africa. The literature review concentrated on articles, journals and books found within South Africa and also material found on the public domain of the internet. The study was confined to one ICT service provider. Therefore generalising the results reported in this study to other service providers around South Africa should be done cautiously.

Since the results presented in this study were based on a small number of participants, the reader should treat findings with caution. This limitation may affect the validity and reliability of the study. This study largely explores an attempt to build a foundation on which to base investigations that are more comprehensive with larger samples.

The study covered the period starting from August 2006 until November 2009 and will concentrated on the service offered by the department that directly contribute to customer service and support.

1.8 DEFINITIONS

Activity: A set of actions designed to achieve a particular result. Activities are usually defined as part of Processes or Plans, and are documented in Procedures.

Architecture: The structure of a System or IT Service, including the Relationships of Components to each other and to the environment they are in. Architecture also includes the Standards and Guidelines that guide the design and evolution of the System.

Asset: Any resource or capability. Assets of a service provider including anything that could contribute to the delivery of a service. Assets can be one of the following types: Management, Organisation, Process, Knowledge, People, Information, Applications, Infrastructure, and Financial Capital.

Attribute: A piece of information about a Configuration Item. Examples are: name, location, Version number and cost. Attributes of Configuration Items are recorded in the CMDB (CMDB).

Audit: Formal inspection and verification to check whether a standard or set of guidelines is being followed, that records are accurate, or that efficiency and effectiveness targets are being met. An Audit may be carried out by internal or external groups.

Availability: Ability of a Configuration Item or ICT service to perform its agreed function when required. Availability is determined by Reliability, Maintainability, Serviceability, Performance and Security. Availability is usually calculated as a percentage. This calculation is often based on agreed service time and downtime. It is best practice to calculate Availability using measurements of the business output of the ICT service.

Availability Management: The process is responsible for defining, analysing, planning, measuring and improving all aspects of the Availability of ICT services. Availability Management is responsible for ensuring that all ICT Infrastructure, Processes, Tools, Roles, and more are appropriate for the agreed Service level targets for availability

Best Practice: Proven activities or processes that have been successfully used by multiple organisations. ITIL is an example of a best practice.

Business Capacity Management: In the context of ITSM, Business Capacity Management is the activity responsible for understanding future business requirements for use in the Capacity Plan.

Business Case: Justification for a significant item of expenditure. Include information about costs, benefits, options, issues, risks, and possible problems.

Business Continuity Management: The business process responsible for managing risks that could seriously affect the business. BCM safeguards the interests of key stakeholders, reputation, brand and value-creating activities. The BCM process involves reducing risks to an acceptable level and planning for the recovery of business processes should a disruption to the business occur. BCM sets the objectives, scope and requirements for ICT Service Continuity Management.

Business Continuity Plan: Such a plan defines the steps required to restore business processes following a disruption. The plan will also identify the triggers for Invocation, people to be involved, communications, and more ICT service continuity plans form a significant part of business continuity plans.

Capacity Management: The process responsible for ensuring that the capacity of ICT services and the ICT infrastructure is able to deliver agreed service level targets in a cost effective and timely manner. Capacity Management considers all resources required delivering the ICT service, and plans for short-, medium- and long-term business requirements.

COBIT: Control Objectives for Information and related Technology (COBIT) provides guidance and best practices for the management of ICT processes. COBIT is published by the ICT governance institute.

Configuration: A generic term, used to describe a group of configuration items that work together to deliver an ICT service, or a recognisable part of an ICT service.

Configuration is also used to describe the parameter settings for one or more configuration items.

Configuration Identification: The activity responsible for collecting information about configuration items and their relationships, and loading this information into the CMDB. Configuration Identification is also responsible for labelling the Configuration Items themselves, so that the corresponding configuration records can be found.

Configuration Items: This is any component that needs to be managed in order to deliver an ICT service. Information about each Configuration Item is recorded in a configuration record within the configuration management system and is maintained throughout its lifecycle by configuration management. Configuration Items are under the control of change management. Configuration items typically include IT services, hardware, software, buildings, people, and formal documentation such as Process documentation and SLAs.

Configuration Management: The process responsible for maintaining information about configuration items required delivering an ICT service, including their relationships. This information is managed throughout the lifecycle of the Configuration Item. Configuration Management is part of an overall service asset and Configuration Management Process.

Continuity Service Improvement: A stage in the lifecycle of an ICT service and the title of one of the core ITIL publications. Continual service improvement is responsible for managing improvements to ICT service management processes and ICT services. The performance of the ICT service provider is continually measured and improvements are made to processes, ICT services and ICT infrastructure in order to increase efficiency, effectiveness, and cost effectiveness.

Control: A means of managing a risk, ensuring that a business objective is achieved, or ensuring that a process is followed. Example controls include policies, procedures, roles, RAID, door locks, and more. A control is sometimes called a countermeasure or safeguard. Control also means to manage the utilisation or behaviour of a Configuration Item, system or ICT service.

Fault Tolerance: The ability of an ICT service or Configuration Item to continue to operate correctly after failure of a component part.

High Availability: An approach or design that minimises or hides the effects of Configuration Item failure on the users of an ICT service. High Availability solutions are designed to achieve an agreed level of availability and make use of techniques such as fault tolerance, resilience and fast recovery to reduce the number of Incidents, and the Impact of Incidents.

Impact: A measure of the effect of an Incident, problem or change on business processes. Impact is often based on how service levels will be affected. Impact and urgency are used to assign priority.

Incident: An unplanned interruption to an ICT service or reduction in the quality of an ICT service. Failure of a Configuration Item that has not yet affected service is also an Incident.

Incident Management: The process responsible for managing the lifecycle of all Incidents. The primary objective of Incident Management is to return the ICT service to customers as quickly as possible.

Information and Communication Technology: The use of technology for the storage, communication or processing of information. The technology typically includes computers, telecommunications, applications and other software. The information may include Business data, voice, images, video, etc. Information Technology is often used to support Business Processes through IT Services.

Information Technology Infrastructure Library (ITIL): A set of best practice guidance for ICT service management. ITIL is owned by the OGC and consists of a series of publications giving guidance on the provision of quality ICT services, and on the processes and facilities needed to support them.

Key Performance Indicator: A metric that is used to help manage a process, ICT service or activity. Many metrics may be measured, but only the most important of these are defined as KPIs and used to actively manage and report on the process, ICT

service or activity. KPIs should be selected to ensure that efficiency, effectiveness, and cost effectiveness are all managed.

Mean Time To Repair: The average time taken to repair a Configuration Item or ICT service after a failure. MTTR is measured from when the Configuration Item or ICT service fails until it is repaired. MTTR does not include the time required to recover or restore. MTTR is sometimes incorrectly used to mean Mean Time to restore service.

Operational Level Agreement: An agreement between an ICT service provider and another part of the same organisation. An OLA supports the ICT service provider's delivery of ICT services to customers. The OLA defines the goods or services to be provided and the responsibilities of both parties.

Planned Downtime: Agreed time when an ICT service will not be available. Planned Downtime is often used for maintenance, upgrades and testing.

Release Management: The ability of a product, service, or process to provide the intended value. For example, a hardware component can be considered to be of high quality if it performs as expected and delivers the required reliability. Process quality also requires an ability to monitor effectiveness and efficiency, and to improve it if necessary.

Reliability: A measure of how long a Configuration Item or ICT service can perform its agreed function without interruption. Usually measured as MTBF or MTBSI. The term reliability can also be used to state how likely it is that a process, function, and so on. will deliver its required outputs.

Root Cause: The underlying or original cause of an Incident or Problem.

Service Level Agreement: An agreement between an ICT service provider and a customer. The SLA describes the ICT service, documents service level targets, and specifies the responsibilities of the ICT service provider and the customer. A single SLA may cover multiple ICT services or multiple customers.

Service Level Management: The process responsible for negotiating Service Level Agreements, and ensuring that these are met. SLM is responsible for ensuring that all

ICT Service Management processes, Operational Level Agreements, and Underpinning Contracts, are appropriate for the agreed service level targets. SLM monitors and reports on service levels, and holds regular customer reviews.

Service targets: A commitment that is documented in a Service Level Agreement. Service level targets are based on service level requirements, and are needed to ensure that the ICT Service Design is Fit for Purpose. Service level targets should be SMART, and are usually based on KPIs.

Total Cost of Ownership: A methodology used to help make investment decisions. TCO assesses the full lifecycle cost of owning a Configuration Item, not just the initial cost or purchase price.

Workaround: Reducing or eliminating the Impact of an Incident or Problem for which a full resolution is not yet available. For example, by restarting a failed Configuration Item. Workarounds for problems are documented in Known Error Records. Workarounds for Incidents that do not have associated Problem Records are documented in the Incident Record.

1.9 LAYOUT OF THE STUDY

Chapter 1

This chapter outlines the general introduction of the topic to be covered during the research. The chapter also outlines the overall structure of the dissertation throughout the report on chapter per chapter basis.

Chapter 2

This chapter covers the literature review, dealing mainly with the ICT environment and where does the CMDB feature in the environment. The chapter also covers broader ITIL best practices.

Chapter 3

Chapter 3 begins with an investigation into the organisation. The chapter also covers the methodology of the empirical study. The design of the questionnaire, the sample design, the sample size and the processing, analysis and evaluation of the data are outlined.

Chapter 4

Chapter 4 presents a summary of the most important findings of the study, a discussion of the conclusions reached and recommendations to the company.

1.10 SUMMARY

From the initial discussion on the Configuration Database Management we can therefore conclude that there is indeed a need for this discussion to be undertaken and the role of CMDB on the ICT environment be thoroughly researched and its importance be clarified. This will be the main point of the discussion on the subsequent chapters which will eventually come up with recommendations at the end of the study.

The chapter has mainly outlined the scope and the nature of the study which mainly concentrated on the factors that have led to the study and the problem which the research will address. The chapter further outlined and explained the objectives of the study and what the study will seek to achieve. The research methodology on how these objectives are going to be achieved was clearly explained in the chapter. Finally the

limitations of the study are stipulated and mentioned in the chapter and the layout of the rest of the study on the chapter by chapter basis was explained.

The next chapter provides a literature review of the the ICT environment and where the CMDB features in the environment

CHAPTER 2

LITERATURE REVIEW

2.1 INTRODUCTION

Businesses require quality ICT services to be provided effectively and economically. In order to be efficient and effective, all organisations has to ensure that they control their ICT infrastructure and services (Berkhout *et al.*, 2003:74).

ICT, as a support department, is expected to support the needs of revenue producing, customer-facing business operations. It is also expected of ICT to enable other business support activities such as human resources, financial management, legal affairs, facilities and operations departments. Determining the expectations and tradeoffs of these support responsibilities are often not done systematically, thus the overall consumption of ICT resources is generally poorly governed. Overpromising and underdeliviring are cornmon complaints because the business demands exceed the ICT supply and explicit governance and prioritasing mechanisms are lacking (Betz, 2006:5).

ICT has taken a prominent role within business as a means to achieve not only operational efficiencies, but increased firm productivity and sustained competitive advantage in the face of dynamic change and uncertainty. However, ICT organisations tasked with providing increased service levels do not have the resources available to reinvent themselves with every technological or regulatory change (Ness, 2005:1).

In order to achieve operational efficiencies and increased service levels, ITIL framework is critical in addressing the external and internal pressures of the organisation. One of the vehicles to achieve this is a comprehensive CMDB. The CMDB plays a critical role within the ITIL framework by providing data support and enhances the ITIL processes (Oldfield *et al.*, 2005:1).

One of the main objectives of ITIL is to ensure support for enterprises, by means of CMDB, to improve ICT efficiency and effectiveness while improving the overall quality of service to the business within imposed cost constraints (Moeller, 2008:206).

Historically the CMDB is a creation of the ITIL and its best practice recommendations. ITIL's notion of the CMDB reflects its definition of configuration management as touching virtually all aspects of the infrastructure as it maps to service delivery. This includes hardware and software, topological and configuration detail as well as operational and business impacts, service mappings, assets-related implications and even incidents impacting critical services. In short, the CMDB is a dynamic common ground for providing consistent perspectives across virtually all management disciplines (Dubie, 2006:1).

Finally, beyond the operational processes there is a significant value to having complete accurate configuration management data. Having timely and accurate data at the point of resolving an incident or considering a change will result in huge savings. Having information is critical to making good decisions, and this is certainly the case with configuration information. Hence a comprehensive CMDB and configuration management enhances all the ITIL processes with a particular emphasis on the configuration management (Klosterboer, 2008:31).

2.2 THE CONFIGURATION MANAGEMENT AND CMDB

No matter its relative size, virtually all ICT operations functions are complex with multiple types and versions of systems of components that must work together in an orderly, well managed manner. This is certainly true for a major corporation with classic mainframe systems, server farms, and multitude of storage devices and communications gear, but smaller server-based operations systems can be complex as well. A formal configuration management function is an important service delivery process supporting the identification, recording and reporting of ICT components, its versions, constituent components, and relationships (Moeller, 2008:208).

Furthermore, configuration management ensures that selected components of a complete service, system or product are identified, baselined and maintained, and that changes to them are controlled. It also ensures that releases into controlled environments and operational use are done on the basis of formal approvals. It provides a configuration model of the services, assets and infrastructure by recording the

relationships between service assets and configuration items (Lacy & Macfarlane, 2006:113).

Lacy and Macfarlane (2006:113) further remarks that configuration management provides visibility of accurate representations of a service or environment that enables:

- Better forecasting and planning of changes in ICT systems;
- Changes on the ICT systems to be assessed planned and delivered successfully;
- Incidents and Problems to be resolved within the service level targets;
- Service levels and warranties to be successfully delivered;
- Better adherence and conformance to standards, legal and regulatory obligations;
- More business opportunities as being able to demonstrate control of assets and services;
- Changes on ICT systems to be traceable from requirements; and
- Creation of the ability to indentify costs for a service.

The basic activity of the configuration management process is to identify the various individual components in ICT operations, called configuration items, and then to identify key supporting data for these Configuration Items, including its owners, identifying data, version numbers and systems interrelationships. This data is captured, organised, and recorded on what is called CMDB (Moeller, 2008:228).

The CMDB is simply defined as a repository of Configuration Items, which are elements within the ICT infrastructure including hardware, software, business applications and services, and relationship between them (Oldfield *et al.*, 2005:1).

According to Oldfield *et al.* (2007:4), a fully deployed CMDB managed by the Change and configuration management processes offers important benefits including:

- Reduced mean time to repair (MTTR) through service outage root cause analysis;
- Increased mean time between failures (MTBF) through better change planning and more accurate impact analysis;

- Adherence to contractual obligations;
- Minimised operational risk through improved change impact analysis;
- Service provider accountability to the user community;
- Heightened security by controlling Configuration Items in use;
- Improved contingency planning due to a thorough understanding of the Configuration Items underlying critical business services;
- Improved Infrastructure integrity by identifying, controlling and correcting Configuration Items exceptions (instances where the discovered Configuration Items differ from previously known Configuration Items);
- Control of assets through verification of Configuration Item records against the discovered infrastructure;
- Gain in ICT process efficiency and cost-effectiveness through sharing of a consistent, single and accurate set of Configuration Items across the entire infrastructure;
- Improved planning as the status of the entire infrastructure is kept current. No unplanned changes are made and all changes to Configuration Items (i.e. new incidents, software deliveries and patch updates) will be recorded in the CMDB;
- More accurate risk assessments as the relationships and dependencies between Configuration Items are known; and
- Improved root-cause diagnosis and resolution through a graphical view that provides visibility to identify upstream and downstream Configuration Items impacted and related to the problem.

It can be concluded that the deployment of comprehensive CMDB can help organisations improve its Change and Configuration Management processes. The upside to a well-planned CMDB that fully exploits the principles of federation, reconciliation, synchronisation and relationship mapping is considerable. Enhanced root-cause and impact analysis leads to improved service levels and increased user and customer satisfaction. As change and configuration processes evolve and mature, change itself becomes more controlled and predictable, resulting in fewer outages caused by unauthorised or poorly planned changes. Improved traceability meets compliance objectives (Oldfield *et al.*, 2007:10).

Overall, the CMDB has broad ramifications in delivering a new approach to ICT system management. It allows an organisation to shift from completely reactive ICT problem resolution to proactive efforts for system improvements, to break down ICT silos for greater synergies and economies in serving the business, and to improve enterprise-wide ICT services aligned with the business. These in turn facilitate process improvements, efficiency and profitability (Anon., 2007:5).

2.3 ICT IN AN ORGANISATION

In recent years it has become increasingly recognised that information is the most important strategic resource that any organisation has to manage. Key to the collection, analysis, production and distribution of information within an organisation is the quality of the Information Communication Technology (ICT) systems and ICT services provided to the business. It is essential to make mention of the fact that ICT systems are crucial, strategic, organisational assets and therefore organisations must invest appropriate levels of resources into support, delivery and management of these critical ICT services (Rudd, 2004:4).

Ward and Peppard (2004:18) state that, ICT have become inextricably intertwined with business. In industries such as telecommunications, media, entertainment and financial services, where the product is already, or is being increasingly digitised, the existence of an organisation crucially depends on the effective application of information and communication technology. With the emergence of e-commerce, the use of technology is becoming just an accepted, indeed expected, way of conducting business. Consequently, organisations are increasingly looking toward the application of technology not only to underpin existing business operations but also to create new opportunities that provide them with a source of competitive advantage. This competitive advantage is not just realized without challenges normally faced by the ICT departments.

The challenges for most ICT departments are to coordinate and work in partnership with the business to deliver high quality ICT services. This has to be achieved while trying to reduce the overall Total Cost of Ownership (TCO) and often increasing the frequency, complexity and the volume of change. The main method of realising this goal is the

operation of effective processes and provision of appropriate, value for money services. This can be enhanced by the implementation of ITIL best practices (Rudd, 2004:5).

ITIL best practices are based on the widely recognised concept that information is the most important strategic resource that any enterprise must manage. The quality of the enterprise's ICT systems and services is key to the collection, analysis, production and information on strategic and organisational levels. It is therefore important that the enterprise invests sufficient levels of resources into its support and delivery, but the emphasis is normally on the more tangible resources such as hardware, communication facilities, or applications (Moeller, 2008:204).

The reason enterprises do not invest a sufficient level of resources in ICT is because ICT budgets are often prepared as if every ICT initiative were being developed in a vacuum. This type of budgeting presumes that ICT initiative goes through a development period and then is magically implemented without any extra costs to overall system maintenance. In reality, linking any ICT initiative into the total existing ICT environment involves a cost. The amount of that cost depends not only on the size and the complexity of the initiative being undertaken but on the state of the current environment (Betz, 2006:7).

In order for the ICT infrastructure to be allocated resources, the ICT will need to be aligned to business. Analysing and documenting the alignment of ICT capabilities with the company business model can be an excellent focus area for an enterprise architecture organisation. If the architecture model is understood to include nontechnical matters and this business model is then linked systematically to the underlying supporting ICT services, the organisation is far ahead than most (Betz, 2006:17).

During the last 30 years, ICT has become an increasingly integral part of business operations. When companies originally began utilising ICT, the ICT development and support organisations resided within the business departments that they supported. This was primarily because use of Information Communication Technology was relatively limited and was directed toward the specialised needs of a particular department, and the need for integration of technology resources across the organisation was limited (Cline & Guynes, 2004:15).

As the use of ICT increased and spread throughout the business, organisations modified their organisational structures. Companies began to realise that there was a large duplication of effort across different departments. New technologies, such as client-server, the internet, data warehousing, and enterprise resource planning (ERP) systems emphasized the need for centralisation of the organisation's technical and information infrastructure (Aldridge & Harris, 2005:54).

Developing, building, and maintaining these technologies required a centralised ICT department, driven by the needs of the organisation as a whole, not the specialised needs of different departments, divisions, or subsidiaries (Anderson & Reid, 2003:44).

The response of many organisations to these issues has been to create a separate ICT department, responsible for developing and supporting ICT resources across the enterprise. This organisational structure provided significant benefits to organisations: simplifying the network infrastructure, minimizing maintenance cost, maximizing ICT operational efficiency, and enabling enterprise-wide deployment of ICT resources. However, this organisational structure can also result in a communication gap between the ICT department and the rest of the organisation (Benamati, Lederer, & Singh, 2005:9).

The fact is effective and dependable ICT services deliver value to the enterprise customers and help business units to achieve their goals, without requiring each of the business units to address the specific management risks and costs for each of the ICT services. Automating ICT services can increase business value by making ICT services more reliable and consistent and shortening service delivery times. ICT has become a utility within most businesses today. Unfortunately, ICT is often implemented and managed in such a way that it is not reliable, is uncoordinated throughout the enterprise, and often seems to do more harm than good to the business in the opinions of the enterprise network users, who are ICT's customers (Herold, 2008:1).

2.4 CONFIGURATION MANAGEMENT AND CMDB DEFINED

It does not matter its relative size, virtually all ICT operations functions are complex with multiple types and versions of systems components that must work together in an

orderly manner. The configuration management function is an important service delivery process supporting the identification, recording, and reporting of ICT components, its version, constituents' components, and relationships (Moeller, 2008:228). In other words, anything that makes up the ICT environment should be recorded as part of configuration management. Most importantly, the physical relationships and logical dependencies between components, subcomponents, applications, servers, networks, documentation, and the myriad of parts of the ICT environment, must be tracked (Klosterboer, 2007:29).

According to Addy (2007:269), there are five basic activities of configuration management:

- **PLANNING:** The configuration management plan covers the first three to six months in detail, and the following twelve months are outlined. The plan is reviewed at least twice a year and will include the strategy, policy, scope, objectives, roles and responsibilities, the configuration management processes, activities and procedures, the change management database, relationships with other processes and third parties, as well as tools and other resource requirements.

- **IDENTIFICATION:** This covers the recording of information about configuration items, including ownership, relationships, versions, and unique identifiers. Configuration Items should be recorded at all level of detail justified by the business need, typically to the levels of independent change.

- **CONTROL:** This gives the assurance that only authorised and identifiable Configuration Items are accepted and recorded from receipt to disposal. It ensures that no configuration Item is added, modified, replaced or removed without the appropriate controlling documentation. All configuration Items will be under change management control.

- **STATUS ACCOUNTING:** This is the reporting of all current and historical data concerned with each Configuration Item throughout its life-cycle. It enables changes to Configuration Items and tracking of its records through various

statuses; for example, ordered, received, under test, live, under repair, withdrawn, or for disposal.

- **VERIFICATION AND AUDIT:** This is a series of reviews and audits that verifies the physical existence of configuration items, and checks that these are correctly recorded in the CMDB. It includes the process of verifying configuration documentation before changes are made to the live environment.

CMDB is very appealing in concept: it has a process that gathers together information about all the objects managed by ICT and its inter-relationships. It provides views into the data so that staff can determine the relationships to understand the impacts (ideally the business service impacts) of changes or outages. The repository of all this data is the CMDB (England, 2009:78).

The CMDB plays a critical role within the ITIL framework by providing critical data to support and enhance service support and service delivery processes. The CMDB is a repository of configuration items, which are elements within the ICT infrastructure including hardware, software, business applications and services, and its relationships to each other.

Figure 2.1 indicates a typical CMDB with a number of configuration items loaded. This particular CMDB provides an example of a centralised enterprise repository of information that contains all the details related to the ICT architecture. This allows for a unified view of every ICT component within the enterprise. This centralised, unified capability will allow all the business leaders to make better business decisions, as well as technical decisions.

One of the configuration items populated in the CMDB, in Figure 2.1, is change request. The CMDB — or more specifically, the information it contains — is important to change management. A change review board might be reviewing tens or even hundreds of potential changes in a meeting. On the surface it might look like approving two changes for two separate business applications would be unrelated tasks, and both might get approved. By looking at an accurate CMDB, however, the change board can quickly see that both applications depend on the same database server, and one

change record has asked to have the server backed up while the other change record has asked to have the same database server taken out of service. Clearly both changes cannot be implemented at the same time but without configuration management data, these conflicts can be all too common. In the security domain, when vulnerability is uncovered, it becomes vital to understand exactly what applications and infrastructure components are exposed. If the IT manager needs to go through an inventory exercise to find the affected components, the company is left vulnerable far too long, and even then some significant relationships might be missed. Accurate configuration data allows everyone to understand exactly how serious the vulnerability is and quickly plan the level of effort required to secure the environment.

Figure 2.1: Typical content of CMDB

Source: Adapted from Herald (2007:28)

Herold (2007:29) outlines configuration management activities that relate to the CMDB as:

- Creating a list of key attributes to collect and maintain for each Configuration Item.

- Defining the relationships between individual configuration items, the relationships between configuration items and ICT services and the relationships between ICT services and business services;
- Tracking the current status and history of each configuration item;
- Verifying and ensuring that the configuration item attributes are complete and accurate; and
- Maintaining an authorised state for comparison to actual state.

Effective CMDB must have four critical capabilities: federation, reconciliation, mapping and visualisation, and synchronous (Herold, 2008:33-38).

- **FEDERATION:** Generally, "federation" means taking data from multiple configuration and management sources and repositories and effectively putting these into one logical, virtual Configuration Management System (CMS) in such a way that the most up-to-date values are used, all the information is integrated so that there are no repeats or gaps, and the information is comprehensive. Federation directly brings multiple data sources by linking it to different sources.

- **RECONCILIATION:** Reconciliation will ensure data is coalesced to avoid having duplicates as well as to enable matching configuration items from different sources. The CMDB is the repository that provides a single source of configuration item data for enterprise ICT services and processes to use.

- **MAPPING AND VISUALISATION:** Most ICT enterprise networks of all sizes can benefit from a mapping and visuliasation tool to see how all the types of data found within a CMDB relate. Even in the otherwise seemingly simple enterprise networks, there is inherent complexity that, if not visually represented, makes it very difficult for ICT leaders to keep track of all the business-critical network components and applications.

  Mapping relationships and dependencies from ICT services down to the configuration items that enable those services and populate that data in the CMDB. Relationship and dependency mapping tools should recognise the

logical relationships between mapped configuration items as well as any changes to those relationships.

- **SYNCHRONISATION:** Synchronisation, through the use of reconciliation, will ensure accuracy across integrated systems. The automated detection of actual state compared with desired state is of the value propositions for good discovery. Being able to associate unplanned infrastructure changes with the services, the infrastructure support is critical for driving stable and resilient services. Change controls will have to be in place to synchronise or to ensure any changes to the monitored configuration items are approved and updated within the CMDB.

The overall benefits of the CMDB is that, based on the configuration and change statistics it stores, a management system can correlate configuration changes with performance changes and usage patterns, thereby determining which configuration changes had an adverse impact on the service performance. After all, what customers care about is service quality, not whether the ICT infrastructure is optimally configured or not (Herold, 2007:31).

2.5 BUSINESS VALUE OF HAVING A COMPREHENSIVE CMDB

Determining Return on Investment (ROI) around CMDBs and ITIL is hard, because we're talking about productivity gains. One of the big benefits of CMDBs is return on avoided outages, but that is tough to calculate because there is no empirical evidence available (England, 2009:30).

England (2009:30) further states that ICT companies which have deployed CMDBs, stand to enjoy the following savings:

- Reducing or eliminating unnecessary servers and other hardware;
- Better license and maintenance contract management;
- Tighter management of outsourcing agreements; and
- Labour savings.

The real value of CMDBs comes from service excellence, and fostering a service-oriented culture. Service resolution time, business alignment, customer satisfaction that is what matters most at the end of the day. But the biggest payoff from CMDBs comes when organisations use it to gain visibility into configuration information to make better decisions about change management processes. One of the best ways to frame the ROI argument is to look at repair times. The dominant metric for financial types is reducing the mean-time-to-repair (England, 2009:31).

The most frequent driver for organisations to use CMDBs is to have a better, more comprehensive understanding of how the enterprise infrastructure components relate to each other, and use this information to make better decisions during change impact assessment problem isolation to ultimately improve the business. A valuable CMDB will be one that is business service-centric. It will maintain a comprehensive and current record of all configuration items and the relationships from multiple sources, in addition to providing services to make the CMDB information as valuable as possible to the business. This value is increased through using automated CMDB tools (Scott, 2005:3).

To put it another way, a CMDB is a view of all the ICT services and the associated enterprise infrastructure interdependencies. This includes configuration information within the network devices as well as the systems and applications. It also includes information for the logical associations for ICT services and infrastructure components, including such things as customers, operational owners, suppliers, outsourced services, and so on (Herold, 2008:38).

BMC Software (2006:2) point out number of benefits that a comprehensive CMDB offer to the business:

- **ENSURING CONSISTENCY:** For the organisation to realise the benefit of CMDB, a framework need to be created to help ensure consistency across the enterprise. Without a framework there can be a temptation to try to confederate existing systems, which tends to fuel a resistance to change. But without the discipline of a formal, centralised CMDB with precise configuration item definitions, you can not gain the consistency required to operate across the enterprise.

- **SPOTTING TRENDS:** One other benefit of CMDB to business is that CMDB can give an insight into the enterprise operations, including trends that might otherwise be missed. This will ensure that the recurring faults on the system are quickly resolved and the mean time to repair will be drastically reduced and in the process services to the customer will be improved.

- **CORRELATING EVENTS:** The CMDB has the ability to filter database searches for a number of different characteristics, which can be extremely helpful in getting a precise picture of what is happening with the enterprise infrastructure.

- **ENHANCING SERVICE LEVEL AGREEMENT DELIVERY:** As the Service Level Agreements (SLAs) become more ubiquitous and more demanding, the CMDB provides data to help organisations meet SLA commitments. The CMDB assists with the allocation of the correct resources, including human resources, whenever there is a system outage. This ensures that faults are resolved as quickly as possible and the SLA times are met.

Return on investment (ROI) for the use of ITIL can be determined in cost savings. In fact, an organisation can gain ROI by reducing the cost of the way that it supports its services. Correct implementation of ITIL ensures that processes are standardized; hence, the business gets streamlined and sustainable. ITIL allows everyone to understand the goals, objectives, and paths to success (Dettmer & Watson, 2006:5).

Overall, business value and ROI for the CMDB can be calculated in a variety of ways. Enhanced operational effectiveness and control, better service and reduced downtime all provide payback in savings of time and money. Better utilisation of ICT staff, the ability to "do more with less," is also a critical point of return, while the ability to know all of an ICT system's components and inter-relationships provides a huge step in improving its overall management (Anon., 2007:5).

2.6 THE EFFECT OF CMDB ON CORPORATE GOVERNANCE

2.6.1 ICT governance aligned to King III

Corporate governance is the system by which organisations are directed and controlled and involves the establishment of organisational structures, process and governance mechanisms (Liell-Cock, Graham & Hill, 2009:3)

King III (2009:1) asserts that, ICT is a big ticket item for most companies and can consume considerable resources with little real value being created. Few organisations have not experienced the disappointment of failed ICT projects or dissatisfaction from poorly delivered services and support. Many organisations are all too familiar with the ever increasing cost of ICT not being matched with ever more effective ICT solutions.

King III states that "the board should be responsible for ICT governance". It is expected that through effective and responsible leadership ICT will be used to sustain and extend the company's business strategy and corporate objectives (Liell-Cook *et al.*, 2009:1).

The first step toward governance is to establish accountability. This requires an examination of the roles and responsibilities within the process used for decision – making that can impact on the achievement of strategic goals (Liell-Cook *et al.*, 2009:2)

The board provides leadership and delegates responsibility to the Chief Information Officer (CIO) to implement the organisational structures and processes to leverage ICT resources and drive alignment, deliver value, manage risk, optimise resources and manage performance. People who are accountable for good governance are responsible for making the changes, when necessary, to deliver the performance expected by the business (Liell-Cook *et al.*, 2009:2).

The board needs to ensure that an ICT control framework is adopted and implemented, and that the board receives independent assurance of its effectiveness.

The role of an internal control is to be preventative, detective or corrective regarding a particular risk. Controls are made sustainable through incorporation in the operational process. The condition of controls depends on the organisational structure, written

policies, systemisation, evidence of controls operating and the competence and integrity of the people involved (Liell-Cook *et al.*, 2009:12).

Committee of Sponsoring Organisations of the Treadway Commission (COSO) is one of the suggested internal control frameworks to be used for compliance to Sarbanes-Oxley (Liell-Cook *et al.*, 2009:12).

Increasingly stringent regulations such as the Sarbanes-Oxley act (SOX) and higher penalties associated with licensing infringements are some of the factors that make it more critical than ever before to maintain accurate and in-depth information on configuration items. SOX and others at first glance appear to focus on accounting and auditing. But data management in general and financial reporting in particular are almost completely reliant on the performance of the ICT infrastructure such as networks, software, servers, and desktops (Dettmer & Watson, 2006:12).

SOX and other regulations require documented controls and processes for the ICT hardware and software used in the financial reporting system, and where configuration items are material to financial statements, for those configuration items themselves. Most of the companies have a huge number of configuration items involved in financial reporting, ranging all the way from computers used to track inventory in a plant to the ones used to prepare the income statement. Knowing where all those are, what safeguards are in place to prevent unauthorized access, and ensuring that one will be able to detect any change, is key. To manage authorisation processes and provide an audit trail to track changes with the help of the CMDB and change management is of utmost importance for SOX and other legal requirements to be successful (Dettmer & Watson, 2006:12).

One other challenge is that the integration trend with business processing centres introduces several complexities to the assurance of internal controls. The concerns result from the sharing of services, staff, and systems with other companies and potential competitors. At risk is the level of safeguards placed on the shared assets which might not adhere to the company's internal practices. The absence of legislative and judicial laws that protect the business ICT resources is a serious risk to organisation that outsource (DeLuccia, 2008:15).

The ICT risks form part of the company's risk management profile. ICT management should regularly demonstrate to the board that the company has adequate "business resilience" arrangements in place to recover from any eventualities (Liell-Cook *et al.*, 2009:21).

The use of a risk management plan to achieve risk management objectives is encouraged by King III. It states that the board is to adopt a risk management plan. The plan should outline the resources, tasks and responsibilities for introducing and developing the risk management processes and activities into the company (Liell-Cook *et al.*, 2009:23).

King III has identified information security as an important aspect of ICT governance. Weaknesses in ICT solutions continue to exist and be exploited by growing number of criminals. To the extent the threats are real, companies need to invest in ever increasing levels of information security (Liell-Cook *et al.*, 2009:25).

A common statement within the ICT security profession is that if the organization is secure it might be compliant; if it is only compliant it certainly is not secure. This statement is both true and false. Any organisation that does just enough as detailed by a regulatory checklist or an internationally accepted ICT control standard, such as COBIT, will be secure if it is done without the perspective of the organisation's systems, business, and risks. In fact, it is likely that such an organisation can even mitigate or address the threat that the regulation had intended (DeLuccia, 2008:30).

From a business perspective, compliance regulations continue to pressure ICT organisations in having the ability to generate reports that show change impact on financial reporting, security, and ICT service delivery. There has never been more of a need for ICT organisations to gain control over changes that take place in the ICT infrastructure, as shareholder value, customer security, reputation, and legal ramifications are real risks. The ability of ICT to adjust to business demands, deliver new revenue-generating innovation, and impact business processes are dependent on managing change. But technology itself does not solve these problems. CMDB and server-provisioning projects enable ICT organisations to deliver successful results that integrate people, processes and technology to meet business demands (Broussard & Elliot, 2007:1).

ITIL should be considered as something more than procedures within a traditional computer room; it is a set of very important service management best practices that will help an enterprise to meet and even exceed these compliance requirements in a cost effective manner. These compliance requirements can be met by ensuring that a comprehensive CMDB exists and contains credible information that is regularly updated. The CMDB includes classifications from security management for trustworthiness, integrity and availability, and provides information for risk management (Moeller, 2008:367).

2.7 CMDB AS A BASIS OF COST SAVINGS AND PROCESS OPTIMISATION

About 70% of the costs associated with the Year 2000 (Y2K) - changes were spent on indentifying the ICT infrastructure and its components as well as on locating the configuration items (Dettmer & Watson, 2006:4).

The majority of these costs could have been saved if more accurate information had been available at the time. Today, legal requirements such as the SOX, Base 11 or software audits again demand a detailed knowledge of the ICT infrastructure, which can only be gained with a well maintained CMDB. In addition, organisations can assess potential risks of changes in advance and thus minimise negative effects on the business operations with the help of CMDB. This will ensure huge cost savings from the organisation side on possible penalties which would have been otherwise enforced in case the SLA is breached. Savings of up to 25% of total cost of ownership are possible, if 3% of the operational ICT budget can be invested in configuration management solutions (Dettmer & Watson, 2006:5).

Whether or not financial improvements, as mentioned above, can be realised depend on the initial situation and the objectives of the individual organisation. Independent of ROI and cost savings, the CMDB can lead to improvements in virtually all ICT processes and can support organisations in their compliance efforts with regard to legal requirements. For instance, SOX states, the CMDB can help meet these legal requirements as installed software instances are also maintained as configuration items in the CMDB (Dettmer & Watson, 2006:5).

CMDB will ensure financial gains through better asset management and reduced manual labour because of automated processes. It ensures increased operational efficiencies derived from management data correlation across multiple systems (Dubie, 2006:1).

2.8 ITIL PROCESSES AND HOW THEY RELATE TO CMDB

2.8.1 ITIL processes

Unless having lived under a rock for the past couple of years one will know that ITIL is a documented set of processes designed to define how a company's ICT functions can operate. It contains a series of statements defining the procedures, controls and resources that should be applied to a variety of ICT related processes (Addy, 2007:35).

Hill and Turbitt (2006:7) outline the following important ITIL processes:

- **INCIDENT MANAGEMENT:** Incident management is responsible for managing all incidents from detection and recording through resolution and closure. Incident management is reactive. The objectives of incident management are to reduce or eliminate the business impacts and effects of actual or likely disturbances within ICT services to ensure personnel can get back to work and business can resume to normal as soon as possible.

- **PROBLEM MANAGEMENT:** Generally, a problem is an unwanted or undesirable situation that, if not addressed soon enough, can become the root cause of an incident. Problem management takes the entire ICT infrastructure into account, using all available information to identify existing and potential failures in the delivery of ICT services. Problem management supports incident management by providing alternative workarounds and temporary fixes during an incident, but does not hold responsibility for actually resolving incidents. Problem management also involves the analysis of incidents and problems to identify trends and then subsequently takes

proactive actions to prevent the further occurrence of similar incidents and problems.

- **CHANGE MANAGEMENT:** Changes arise as a result of problems, but many Changes can come from proactively seeking business benefits such as reducing costs or improving services. The goal of the change management process is to ensure that standardised methods and procedures are used for efficient and prompt handling of all changes, in order to minimise the impact of change-related incidents upon service quality, and consequently to improve the day-to-day operations of the organisation.

- **CONFIGURATION MANAGEMENT:** Businesses require quality ICT services provided economically. To be efficient and effective, all organisations need to control its ICT infrastructure and services. Configuration management provides a logical model of the infrastructure or a service by identifying, controlling, maintaining and verifying the versions of configuration items in existence.

- **RELEASE MANAGEMENT:** Many service providers and suppliers may be involved in the Release of hardware and software in a distributed environment. Good resource planning and management are essential to package and distribute a Release successfully to the Customer. Release Management takes a holistic view of a Change to an IT service and should ensure that all aspects of a Release, both technical and-non-technical, are considered together.

- **SERVICE LEVEL MANAGEMENT:** Service Level Management (SLM) is essential in any organisation so that the level of IT service needed to support the business can be determined, and monitoring can be initiated to identify whether the required service levels are being achieved – and if not, why not.

  SLAs, which are managed through the SLM process, provide specific targets against which the performance of the IT organisation can be judged.

- **FINANCIAL MANAGEMENT FOR ICT SERVICES:** To understand whether an ICT organisation is doing the best that it can and to demonstrate this to its customers, it has to both understand the true cost of providing a service and manage those costs professionally. To do this, it is usual to implement ICT accounting and budgeting processes and often to implement charging processes as well.

  Financial management is the sound stewardship of the monetary resources of the organisation. It supports the organisation in planning and executing its business objectives and requires consistent application throughout the organisation to achieve maximum efficiency and minimum conflict.

- **CAPACITY MANAGEMENT:** A corporate capacity management process ensures that the entire organisation's capacity requirements are catered for. The cost of upgrading all the desktop equipment in an organisation could easily exceed the cost of a mainframe upgrade. Capacity management should have responsibility for the refresh policy, ensuring that desktop equipment has sufficient capacity to run the applications that the business requires for the foreseeable future. Capacity management is one of the forward-looking processes, which, when properly carried out, can forecast business impacts before they happen.

- **AVAILABILITY MANAGEMENT:** The goal of the availability management process is to optimise the capability of the IT infrastructure, services and supporting organisation to deliver a cost-effective and sustained level of Availability that enables the business to satisfy its business objectives.

  This is achieved by determining the availability requirements of the business and matching these to the capability of the IT infrastructure and supporting organisation. Where there is a mismatch between the requirement and capability, availability management ensures the business is provided with available alternatives and associated cost options.

  Availability management should ensure the required level of availability is provided. The measurement and monitoring of IT availability is a key activity

to ensure availability levels are being met consistently. Availability management should look continuously to optimise the availability of the IT Infrastructure, services and supporting organisation, in order to provide cost effective availability improvements that can deliver evidenced business and user benefits.

- **INFORMATION TECHNOLOGY SERVICE CONTINUITY MANAGEMENT:** Information Technology Service Continuity Manager (ITSCM) focuses on the IT services required to support the critical *business processes*. The impact of a loss of a business process, such as financial loss, damage to reputation or regulatory breach, is measured through a Business Impact Analysis (BIA), which determines the minimum critical requirements. The specific ICT technical and service requirements are supported by ITSCM. The scope of ITSCM within an organisation is determined by the organisational structure, culture and strategic direction (both business and technology) in terms of the services provided and how these develop and change over time.

2.8.2 How ITIL processes relate to the CMDB

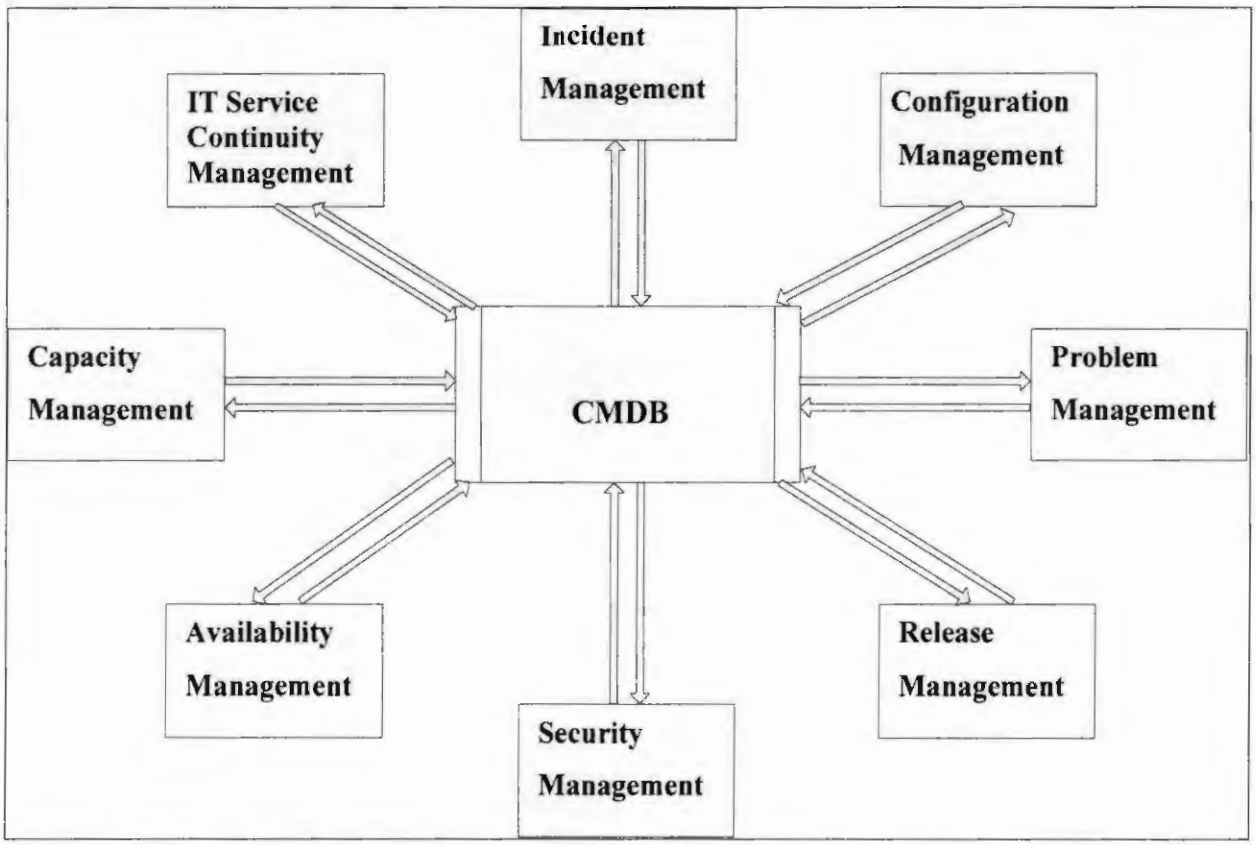
To be successful with using the ITIL change management process, it is important that the people, processes, and technologies are working together in a coordinated manner to overcome the political roadblocks that usually inhibit cooperation between groups in the same organisation. The primary goal of the CMDB is to house the configuration items that exist throughout the enterprise and the relationships between them, revealing the status for each configuration at any time (Herold, 2007:34).

Used effectively, the CMDB improves quality-of-service because all CMDB components and their relationships are clearly understood. It provides an accurate view of current ICT capability, enabling the organisation to quickly discern the status of its entire ICT infrastructure and how one interaction impacts another. This ability helps to manage changes more effectively. The knowledge gained through a CMDB, combined with ITIL best practices, provides greater flexibility for the business through an improved understanding of ICT service support delivery and infrastructure management (Bishop, 2005:8).

Figure 2.2 depicts that the CMDB is central to all the ITIL processes and is centralised enterprise repository of information that contains all the details related to the ICT architecture. One of the processes which is linked to the CMDB is the incident management process. Incident management in ITIL terms is about restoring service, and the key metric is how quickly service can be restored.

The CMDB provides information to help the incident management team isolate the source of the problem more quickly. The better system administrators or application managers track some pieces of the information, or recall the last time this incident occurred, but they still don't have the complete picture that enables them to deal with new kinds of incidents. With configuration management data, the same ICT manager simply looks at a few servers and applications that are down, and quickly sees that they are all related to the same router. With an accurate CMDB, the source of the incident can be isolated quickly, and then details about the failing component, such as software and firmware levels, can be viewed. Having configuration data in place can literally cut hours off the time it takes to resolve a complex incident.

Figure 2.2: Relationship of CMDB to ITIL processes



Source: Adapted from Herold (2007:55)

According to Dettmer and Watson (2006:6), the following functions for different ICT service management processes are supported by the CMDB:

- **INCIDENT MANAGEMENT:** Incidents can be prioritsed more accurately based on the relationships between affected configuration items. Incidents can be resolved faster, because the entire CI information for each user is visible.

- **PROBLEM MANAGEMENT:** Detailed information for problem analysis will always be available. This will assist in conducting trends analysis on recurring problems and in the process common incidents will be eliminated.

- **CHANGE MANAGEMENT:** It supports the analysis of potential ramifications for the production environment after changes take place.

- **RELEASE MANAGEMENT:** It manages the availability of information for release planning and execution, so that rollouts do not have a negative effect on the business.

- **CONFIGURATION MANAGEMENT:** The CMDB is the database in which the ICT infrastructure is recorded and described, delivering a detailed model of the ICT infrastructure for all processes.

- **SERVICE LEVEL MANAGEMENT:** It manages the availability of information about the configuration Items that support an ICT service. Without this data, SLAs cannot be thoroughly created and adhered to.

- **FINANCIAL MANAGEMENT:** Configuration Items information is enhanced by financial data which are necessary for the cost and service billing.

- **AVAILABILITY MANAGEMENT:** This entails the measuring and control of the availability of the configuration items and delivery of information to identify weak points.

- **INFORMATION TECHNOLOGY SERVICE CONTINUITY MANAGEMENT:** Based on the configuration items, emergency contingency plans and baselines are created, which should be available at the alternative location.

- **CAPACITY MANAGEMENT:** The CMDB delivers information for capacity planning and tuning measures.

- **SECURITY MANAGEMENT:** The CMDB includes classifications from security management for trustworthiness, integrity and availability, and provides information for risk management.

Overall, security is one of the most aspects of the CMDB that since the introduction of, what is called Grid Computing, in the ICT environment. The grid is the computing and data management infrastructure that will provide the electronic underpinning for a global society in business, government, research, science and entertainment. Grids integrate networking, communication, computation and information to provide a virtual platform

for computation and data management in the same way that the Internet integrates resources to form a virtual platform for information (Minoli, 2005:20).

Security is therefore a much more important factor in planning and maintaining a grid than in conventional distributed computing, where data sharing comprises the bulk of the activity. In a grid, the member machines are configured to execute programs rather than just move data. This makes an unsecured grid potentially fertile ground for viruses and Trojan horse programs. For this reason, it is important to understand exactly which components of the grid must be rigorously secured to deter any kind of attack (Minoli, 2005:86). This is where the job of the CMDB comes in where classifications from security management for trustworthiness, integrity and availability, are employed to provide information for critical risk management.

Every process defined by the ITIL framework gains concrete benefits from accurate and timely configuration management data, and those other processes will never function effectively without configuration data. These key dependencies are facilitated by relating the configuration items to key concepts in other processes. Because configuration data are so vital and used for so many purposes, it is critical that it should be accurate and complete (Klosterboer, 2008:31).

2.9 THE IMPORTANCE AND THE ROLE OF CMDB IN AN ICT ENVIRONMENT

The goal of realising best practices in ICT configuration management, via the utilisation of a CMDB, is the result of some very real business drivers. These drivers include the ability of an organisation to effectively manage and deploy not only desktops and servers, but all of the ICT resources and processes across the enterprise, and to make better decisions regarding change management, especially as environments become increasingly complex. By performing relationship discovery and dependency mapping to better understand change implications, organisations can improve problem isolation and perform subsequent problem resolution more quickly. These organisations can also consolidate configuration information in a single location, to drive enhancements in such critical areas as security and asset management, improved vendor management and software license compliance (Anon., 2007:5).

When change and configuration management processes are integrated and fully functioning, ICT can truly understand and control the ICT infrastructure. Incidents can be prioritised so that resolution is focused on those with true business impact. Proposed Requests For Change (RFCs) to CI can be assessed and approved with a clearer picture of the configuration items' relationships to other devices and impact on ICT and business services. Unauthorised changes to the infrastructure can be minimised and their resulting costly business service outages avoided. ICT services can be defined, measured and ensured more precisely. The capacity of ICT resources and services can be more accurately anticipated and planned for. To achieve these benefits, configuration management maintains the current status of the dynamic ICT environment in the CMDB, with change management maintaining data integrity with updates to the CMDB.

Oldfield *et al.* (2005:4) remarks that a fully deployed CMDB managed by the change and configuration management processes offers key benefits including:

- Reduced downtime due to root-cause analysis of service outages;
- Minimised operational risk due to change impact analysis and the proper planning around the changes on the network;
- Improved contingency planning due to visibility of ICT components underlying business services;
- Improved service integrity due to monitoring of ICT components related to critical services; and
- ICT processes efficiency and cost-effectiveness as a result of sharing a consistent set of ICT service, application and infrastructure data.

The goal of realising best practices in ICT configuration management, via the utilisation of a CMDB, is the result of some very real business drivers. These drivers include the ability of an organisation to effectively manage and deploy not only desktops and servers, but all of the ICT resources and processes across the enterprise, and to make better decisions regarding change management, especially as environments become increasingly complex. By performing relationship discovery and dependency mapping to better understand change implications, organisations can improve problem isolation and perform subsequent problem resolution more quickly. They can also consolidate configuration information in a single location, to drive enhancements in such critical

areas as security and asset management, improved vendor management and software license compliance (Anon., 2007:4).

Overall, the CMDB has broad ramifications in delivering a new approach to ICT system management. It allows an organisation to shift from completely reactive ICT problem resolution to proactive efforts for system improvements, to break down ICT silos for greater synergies and economies in serving the business, and to improve enterprise-wide ICT services aligned with the business. These, in turn, facilitate process improvements, efficiency and profitability (Anon., 2007:5).

2.10 THE COMPARISON BETWEEN ITIL AND COBIT BEST PRACTICES

Control Objectives for Information and related Technology (COBIT) is a framework and supporting toolset that allows managers to bridge the gap with respect to control requirements, technical issues and business risks, and communicates that level of control to stakeholders. COBIT enables the development of clear policy and good practice for ICT control throughout enterprises. COBIT is continuously kept up to date and harmonised with other standards. Hence, COBIT has become the integrator for ICT best practices and the umbrella framework for ICT governance that helps in understanding and managing the risks and benefits associated with ICT. The process structure of COBIT and its high-level business-oriented approach provide an end-to-end view of ICT and the decisions to be made about ICT (Anon., 2005:9).

The benefits of implementing COBIT as a governance framework over ICT include:

- Better alignment, based on a business focus;
- A view understandable to management, of what ICT does;
- Clear ownership and responsibilities, based on process orientation;
- General acceptability with third parties and regulators;
- Shared understanding amongst all stakeholders, based on a common language; and
- Fulfilment of the COSO requirements for the ICT control environment.

A major thrust of ITIL is to promote the alignment of ICT with the business. ITIL defines service quality as the level of alignment between the actual services delivered and the actual needs of the business. Although ITIL covers a number of areas, its main focus is on Information Technology Service Management (ITSM). ITIL provides a comprehensive, consistent, and coherent framework of best practices for ITSM and related processes, which promotes a quality approach for achieving business effectiveness and efficiency in the use of information and communication systems (Anon., 2005:10).

2.10.1 Leveraging the combination of ITIL and COBIT

Organisations wanting to adopt ITIL need an effective ICT governance and control framework for successful ITIL implementation. COBIT provides a broad-based governance framework that includes guidelines to help the organisation drive toward the business requirements. COBIT also provides a mechanism for measuring the capability of the organisation (people, processes, and technology) to achieve a successful outcome in meeting the business requirements, and for measuring performance (Hill & Turbitt, 2006:3).

Although COBIT is oriented to ICT processes, it does not include processes, steps and tasks. It focuses on what an enterprise needs rather than how to do it. COBIT processes are focused on the business requirements, and provide guidance in determining what is sufficient to meet these requirements.

ITIL, on the other hand, defines best practice processes for ITSM and shows how to get there. It focuses on method and defines a more comprehensive set of processes than COBIT, providing a roadmap for building processes.

COBIT and ITIL provide a valuable combination for helping an organisation manage ICT from a business perspective, an approach known as a Business Service Management (BSM). ITIL provides guidelines in best practice ITSM processes geared towards aligning ICT with the business. COBIT helps the organisation mould the ITIL processes to the business needs and goals of the organisation. It helps the organisation to establish a start and end point; that is, determining where the organisation wants to be. Knowing the goals, ICT can then activate business objectives (Hill & Turbitt, 2006:4).

COBIT also provides an effective mechanism for managing and measuring progress in implementing ITIL processes by helping the organisation understand its goals and measure progress in achieving them. In addition, COBIT provides a mechanism for measuring improvement, and continual improvement is a major thrust of ITIL (Hill & Turbitt, 2006:4).

Specifically, COBIT provides management directions for getting the enterprise's information and related processes under control, monitoring achievement of organisational goals, monitoring performance within each ICT process, and benchmarking organisational achievement.

2.11 CONCLUSION

The conclusion that can be derived from the literature study is that many organisations consider the ability to manage assets as the primary step for getting the business to have a competitive edge. It can further be deduced from the study that using a CMDB (CMDB) for asset management can significantly reduce the business' operational costs. Without a CMDB, organisations run the risk of over-provisioning because they cannot track which assets are used for which purposes, or which availability and service problems relate to certain types of assets. It has also been discovered that in the past, ICT budgets were fairly generous and organisations would routinely over-provide to be on the safe side. One of the ways that ICT organisations can survive and prosper in today's budget-crunching climate is to get the maximum advantage out of its ICT assets and software. The literature study has also revealed that CMDB provides an accurate picture of available assets and its use. This capability ensures assets are used most effectively and promotes cost savings for the enterprise.

It has further been established in the study that CMDB developed with a consistent, logical model provides the common infrastructure for identifying, controlling, maintaining, and verifying the various components — the configuration items that exist in an ICT environment. It is therefore essential to have a consistent and logical way to maintain information about those items. That is why the CMDB is critical to increasing information sharing and maintaining accuracy of information across the ICT organisation. The emphasis on sharing data and maintaining accuracy to support

business services helps enable BSM, the strategy of managing ICT from a business perspective. Linking individual configuration items back to business processes, it is found to be problematic for many ICT organisations. It is therefore important when problems occur, and when configuration items are changed, to understand the impact of the change. When things break, it is also essential to link the problem back to changes in the configuration. Without a CMDB, it is impossible to deliver on the basic premise that when a change is made in configuration, the organisation must have some idea of what business processes have been affected.

The literature review also emphasised that the ITIL notion of CMDB has gained traction in the industry as a centralized source for ICT system information that can assist with a variety of processes including change and configuration control, asset management, patch management, software provisioning and compliance. Within the ITIL framework the CMDB exists not as a tool or specific piece of software but as an enabling concept. Regardless of definition, organisations are realising that there are compelling business drivers that are validating CMDB deployments, critical areas for ICT improvements that include enhanced service, informed change management, improved asset and vendor management, software licence compliance and overall alignment of ICT with business needs.

The area of compliance and corporate governance is non-negotiable when it comes to the maintaining of data integrity and security around ICT. The organisation will, therefore, need to ensure that the relevant support structures and resources are in place in order to meet the requirements stipulated in the King111 report the ICT governance. In order to be effective, business strategy and goals have to be cascaded down into the ICT organisation and used as the basis of measuring performance. Each layer of the governance contributes to the fulfilment of the business strategy achievement of corporate goals.

It has also been established that no organisation can be fully efficient and effective unless it manages its configuration items, particularly those assets that are vital to the running of the customer's business. The goal of optimising the performance of service configuration items will improve the overall service performance and optimises the costs and risks caused by poorly managed configuration items.

It can also be said that CMDB can help ensure consistency in identifying and defining configuration items. It unifies change management, configuration management, and incident management, while enforcing adherence to the CI-driven framework created with the help of the stakeholders. CMDB helps to correlate events to find a common cause, and provides the data needed to better ensure the ability to meet SLAs.

Deploying the CMDB will help organisations improve its change and configuration management processes. The upside to a well-planned CMDB that fully exploits the principles of federation, reconciliation, synchronisation and relationship mapping is considerable. Enhanced root-cause and impact analysis lead to improved service levels and increased user and customer satisfaction. It is therefore inconceivable that any ICT service provider will be able to render services without a proper CMDB platform in place.

Used effectively, the CMDB will help improve quality-of-service, because all CMDB components and its relationships will be clearly understood. It will provide an accurate view of current ICT capability, enabling the organisation to quickly discern the status of the entire ICT infrastructure and how one interaction impacts another. This ability will help the organisation manage changes more effectively. The knowledge gained through a CMDB, combined with ITIL best practices, can provide greater flexibility for the business through an improved understanding of ICT service support delivery and infrastructure management. The more information the organisation has, the more flexible it can become and better prepared to meet service management objectives.

2.12 SUMMARY

The chapter covers largely ICT as a basis for any enterprise that needs its business to be run efficiently and successfully. It outlines the importance of why businesses must ensure that a proper CMDB exist for proper service quality to be offered.

The relationship between configuration management and CMDB is clearly outlined and there is an elaboration of how the two are intertwined and cannot function exclusively from each other.

Different ITIL processes were discussed and how each of them relates to service management. Furthermore, the relationship between the CMDB and the rest of the ITIL processes was thoroughly explained and broadly discussed. Furthermore, the benefit of the CMDB in a business was broadly discussed and how cost can be saved on running a business with a proper CMDB platform.

The strategic role of ICT in an organisation was discussed in the literature review and the need to realign the ICT services to the business strategy was also emphasized. The realignment will ensure that ICT departments work as a support base in order to advance the goals and targets of the enterprise. This will then ensure that appropriate budget allocation for the maintenance and refresh of the ICT systems occur on a regular basis.

The value of CMDB in the ICT environment was discussed and found that the value cannot be quantified but can be achieved by means of ensuring that the service level agreed on is achieved. This will ensure that the organisation is not penalised by customers due to lack of meeting the service level targets agreed on. The literature review confirmed that the real savings come from service excellence, and fostering a service oriented culture. Service resolution time, business alignment and customer satisfaction; that is what matters most at the end of the day.

The literature review also covered the effect of CMDB on corporate governance and the need for compliance to regulations. It indicates that organisations must be in a position to generate authentic reports on financial reporting, security, and ICT security delivery. These compliance requirements can only be met by ensuring that a comprehensive CMDB exists and contains credible information that is regularly updated. The King III requirements on what is needed by organisations to be compliant to ICT corporate governance was also covered extensively.

The cost savings from implementation of CMDB was subsequently discussed. It is made mention that the financial gains can be ensured by better asset management and reduced manual labour because of automated processes. CMDB will ensure increased operational efficiencies derived from management data correlation across multiple systems.

The literature review also discussed extensively the importance of CMDB in an ICT environment. One of the important aspects of CMDB is linked to an effective incident management process. The study mentions that the time spent on resolution of incidents can be drastically reduced with an effective updated CMDB. This can be achieved if a proper relationship between configuration items is known and the faulty components can be quickly identified and the faults can be quickly cleared. The accurate CMDB can also be used by the change approval board in order to determine the impact of changes planned on the network. It can help determine the impact and severity of the change on the network.

Finally, the comparison between ITIL and COBIT was discussed and how best to leverage the combination of the two frameworks. The outlines that COBIT processes are focused on the business requirements, and provide guidance in determining what is sufficient to meet these requirements. ITIL, on the other hand, defines best practices processes for ITSM and show how to get there. The two frameworks provide a valuable combination for helping an organisation manage ICT from a business perspective, an approach known as a Business Service Management (BSM).

Chapter 3 will discuss the empirical study and the results obtained through the measuring instrument employed.

CHAPTER 3

RESULTS OF THE EMPIRICAL STUDY

3.1 INTRODUCTION

The development and design of a questionnaire to collect data for the empirical study is of vital importance. In this chapter, the development, design and the structure of the questionnaire for the empirical study as well as the data gathering process is discussed. The results of the empirical study of the four different sections is presented and discussed.

3.2 RESEARCH METHOD

The research method that is used will be based on the scientific method. Marczyk, Dematteo & Festinger (2005:19) assert that the scientific method is best thought of as an approach to the acquisition of new knowledge. To be clear, the scientific method is not actually a single method, as the name would erroneously lead one to believe, but rather an overarching perspective on how scientific investigations should proceed. It is a set of research principles and methods that help researchers obtain valid results from their research studies.

Because the scientific method deals with the general approach to research rather than the content of specific research studies, it is used by researchers in all different scientific disciplines. The biggest benefit of the scientific method is that it provides a set of clear and agreed upon guidelines for gathering, evaluating, and reporting information in the context of a research study (Cozby, 1993:1).

The scientific method is firmly based on the empirical approach. The empirical approach is an evidence-based approach that relies on direct observation and experimentation in the acquisition of new knowledge (Kazdin, 2003:5). In the empirical approach, scientific

decisions are made based on the data derived from direct observation and experimentation.

Contrast this empirical approach to decision-making with the way that most nonscientific decisions are made in our daily lives. Often conclusions are reached or decisions are made that are not necessarily based on data, but rather on opinions, speculation, and a hope for the best. The empirical approach, with its emphasis on direct, systematic, and careful observation, is best thought of as the guiding principle behind all research conducted in accordance with the scientific method (Marczyk *et. al.*, 2005:19).

3.3 COLLECTION OF DATA

A comprehensive questionnaire was designed to evaluate four sections with 35 questions on the basis of a five-point Likert scale. The target population of this research was the top, middle and junior management of the company of choice. The technique used to distribute and complete the questionnaires included: distribution of questionnaires by hand and followed up by telephone calls. Throughout the data collection process the biggest challenge was to persuade all the participants involved to complete the questionnaire.

Each questionnaire was sent with a cover letter that guaranteed the confidentiality of the respondents' data, as well as a return envelope in order to make it as easy as possible for respondents to take part in the research. Respondents were requested to return the completed questionnaires in a sealed provided envelope. The respondents' names were noted down in order to keep track of the respondents. Overall, 38 questionnaires were handed out and 33 usable questionnaires were received back.

The data was statistically analysed by the Statistical Consultation Service of the North-West University. The arithmetic mean and percentages for each question were determined.

3.3.1 Validation of the data

There were about 38 comprehensive questionnaires that were distributed and 33 usable questionnaires were received back. This represents an overwhelming response of about

87% respondents. This represented a very good number of participants from the chosen sample size. The data was further validated by rechecking the data to make sure that it contained no errors arising from mistakes with data entry. This was done in order to eliminate erroneous entries since the data was manually captured.

The results were examined to look for consistency within the data in terms of respondents with similar profiles giving similar answers. This was done in order to look for consistent patterns of responses. The other validation exercise was to use 'check questions' that are deliberately placed within a questionnaire to see whether people's responses are the same to a very similar question. This has proven the data to be authentic and correct and can be used in the empirical study.

3.4 RESULTS AND DISCUSSION

3.4.1 Section 1: Biographical information of respondents

The results of section 1 of the questionnaire are presented in this section. Please refer to Appendix 1 for the detailed questionnaire. The columns are categorised in frequency and percentage. Frequency of events is the count of the frequency with which the categories/items on the observation schedule occur. The percentage is the number of frequencies divided by the total number of respondents.

3.4.1.1 General information age

In table 3.1 the age groups are presented. A total of 33 questionnaires were employed for analysis.

Table 3.1: Age groups of respondents

Age group (Years)	Frequency	Percentage (%)
<30	6	18.18
30-39	15	45.46
40-49	7	21.21
50-59	3	9.09
60+	2	6.06
Total (n)	**33**	**100**

The majority of the respondents are between the ages 30-39 (45.56%), 18.18% are under the age of 30, 21.21%are between the ages of 40 to 49, 99.09% are between the age of 50 to 59 and the rest are over the 60. As the majority of the respondents are between the ages of 30 and 39 they are less likely to resist change and implementation of processes.

3.4.1.2 Management level

Table 3.2 illustrates the management level of the participants.

Table 3.2: Management level of respondents

Management Level	Frequency	Percentage (%)
Top management	6	18.18
Middle management	14	42.43
Junior management	13	39.39
Total (n)	**33**	**100**

The majority of the participants are middle management at 42.43%, junior management closely follows at 39.39% and the rest are top management on 18.18%. This indicates

an ideal distribution of the management levels in driving the implementation of the ITIL processes.

3.4.1.3 Level of knowledge on CMDB

The level of knowledge of the CMDB of the respondents is presented in table 3.3.

Table 3.3: Level of knowledge of CMDB

CMDB knowledge	Frequency	Percentage (%)
Basic knowledge	10	30.30
Intermediate knowledge	21	63.64
Advanced knowledge	2	6.06
Total (n)	**33**	**100**

A total of 63.64% of the participants have an intermediate knowledge of the CMDB, 30.30% have a basic knowledge and the rest of the participants, at 6.06%, have an advanced knowledge. This is a clear indication of fair knowledge of CMDB of most of the participants, which will make it very easy for the organisation to roll out a complete solution of the CMDB.

3.4.1.4 Level of knowledge of ITIL processes

The level of knowledge of the ITIL processes of the respondents is presented in table 3.4.

Table 3.4: Level of knowledge of ITIL processes

ITIL knowledge	Frequency	Percentage (%)
Basic knowledge	9	27.27
Intermediate knowledge	20	60.61
Advanced knowledge	4	12.12
Total (n)	**33**	**100**

The majority of the participants have fair knowledge of ITIL processes. A total of 60.61% have an intermediate knowledge of ITIL processes with 27.27% with basic knowledge. However much needs to be done to increase the advanced knowledge, which only 12.12% of participants have.

3.4.1.5 Level of knowledge of COBIT

The level of knowledge of COBIT of the respondents is presented in table 3.5.

Table 3.5: Level of knowledge of COBIT

COBIT knowledge	Frequency	Percentage (%)
Basic knowledge	21	63.64
Intermediate knowledge	11	33.33
Advanced knowledge	1	3.03
Total (n)	**33**	**100**

The knowledge of COBIT is not very strong within the organisation as it is indicated that 63.64% of the participants have a basic knowledge of COBIT. It is followed by 33.33% of participants with intermediate knowledge and the rest of the participants, 3.03%, have advanced knowledge. This can be attributed to the fact that the organisation is concentrating on an ITIL framework as indicated in the prior findings.

3.4.1.6 Participants' attitude towards processes

The attitude of participants towards processes is presented in table 3.6.

Table 3.6: Participants' attitude towards processes

Attitude toward processes	Frequency	Percentage (%)
Negative	0	0.0
Acceptable	12	36.36
Totally acceptable	21	63.64
Total (n)	**33**	**100**

A total of 63.64% of the participants have the most positive attitude towards processes; they are being followed by 36.36% of participants with a positive attitude. This gives a clear indication that most of the employees support a process driven environment.

3.4.2 Section 2: Organisation approach to individual ICT components.

In this section, the respondents had to indicate their understanding of organisation approach towards identification of individual ICT components. The mean of the number of respondents is calculated and presented on the table below. The results are subsequently presented from the highest to the lowest ranked questions (See table 3.7). Refer to Appendix 1 for detailed layout of the questionnaire.

3.4.2.1 The seven highest questions

The seven questions, which were evaluated the highest, are subsequently illustrated form the highest to the lowest arithmetic mean value:

1. The organisation has recognised the need to indentify all ICT assets/components within our environment for better service provision (Question 1: x=3.48);
2. The organisation has established documented procedures that describe how ICT assets/components should be identified, recorded and controlled (Question 8: x=3.06);
3. The organisation has documented detailed and useful procedures for making changes to ICT assets/components within the ICT systems (Question 9: x=3.00);
4. Detailed business processes as well as ICT assets/components have been clearly defined and ensured that quality service is offered (Question 12: x=2.97);

5. The organisation has identified and recorded all the ICT assets/components in properly managed and updated database system (Question 2: x=2.94);
6. The organisation has a reliable repository system with information or attributes about each ICT assets/components in the company e.g. Unique Number, name, assets tag, and version (Question 3: x=2.94); and
7. Detailed and understandable documented standards procedures have been established for naming conventions on ICT assets/components (Question 11: x=2.91).

Table 3.7 follows on next page

Table 3.7: Organisation's approach to individual ICT components

Item	Question	n	Mean
Q2.1	The organisation has recognised the need to identify all ICT assets/components within our environment for better service provision.	33	3.48
Q2.8	The organisation has established documented procedures that describe how ICT assets/components should be identified, recorded and controlled.	33	3.06
Q2.9	The organisation has documented detailed and useful procedures for making changes to ICT assets/components within the ICT systems.	33	3.00
Q2.12	Detailed business processes as well as ICT assets/components have been clearly defined, and ensured that quality service is offered.	33	2.97
Q2.2	The organisation has identified and recorded all the ICT assets/components in a properly managed and updated database system.	33	2.94
Q2.3	The organisation has a reliable repository system with information or attributes about each ICT asset/component in the company, for example, unique number, name, assets tag, and version.	33	2.94
Q2.11	Detailed and understandable documented standards procedures have been established for naming conventions on ICT assets/components.	33	2.91
Q2.10	The organisation has established a comprehensive function to manage the identification and recording of all ICT assets/components (both spares and functional).	33	2.76
Q2.6	The organisation has useful and clear relationships, or links that define how each ICT asset/component is interconnected and interdependent with its neighbours within ICT systems.	33	2.73
Q2.4	The organisation has an authentic set of records that defines the version of each ICT assets/components.	33	2.70
Q2.13	The organisation has a means to assign owners to different ICT assets/components in scope.	33	2.64
Q2.5	The organisation has baselined all ICT assets/components in order to allow monitoring of progress or changes to components on the ICT systems more carefully.	33	2.54
Q2.7	The organisation has established a regularly updated and useful repository/repositories to record all ICT assets/components information in scope.	33	2.54

3.4.3 Section 3: The value gained from implementation of configuration management

This section looks into the benefit gained from the implementation of the configuration management process without a proper CMDB running. The success of the change

management process is also being examined in the absence of a CMDB. The mean of the number of respondents is calculated and presented in the table below.

Table 3.8: The value gained from implementation of configuration management

Item	Question	n	Mean
Q3.5	The success of network changes has improved due to the implementation of configuration management process.	33	3.00
Q3.6	The traceability of changes from defined requirements can be easily executed because of the existing configuration management process.	33	2.88
Q3.7	The organisation is able to achieve required service levels due to the present configuration management process.	33	2.79
Q3.8	The current configuration management system is able to assist in accounting for the number of contractual warranty claims made.	33	2.67
Q3.9	The implemented configuration management process is able to assist with a proper identification of the costs of the organisation services.	33	2.67
Q3.10	The currently running configuration management system is the reason for the shorter time taken to resolve incidents.	33	2.67
Q3.1	The implementation of the configuration management system has seen an improvement on the number of business opportunities through better control of assets and services.	33	2.61
Q3.2	The implementation of configuration management has seen an adherence/compliance with standards, legal and regulatory obligations.	33	2.61
Q3.3	The existing configuration management system has seen an improvement on audit non-conformances received.	33	2.58
Q3.4	The current configuration management process has enabled the organisation to have a better forecasting and planning of network changes.	33	2.42

3.4.4 Section 4: The status and role of CMDB within the organisation

The section presents the status of the CMDB and the role it is suppose to play in the ICT environment. The mean of the number of respondents is calculated and presented in the table below.

Table 3.9: The status and role of CMDB within the organisation

Item	Question	n	Mean
Q4.11	There is a means within the organisation to receive notification from, or provide information to change management relating to every configuration item to be changed or introduced.	33	2.73
Q4.4	There is a working system that links changes and configuration records together within the organisation.	33	2.64
Q4.5	There is a working system that links incident/service requests and configuration records together within the organisation.	33	2.64
Q4.8	The organisation has a reliable configuration data which is routinely used to perform configuration change impact assessments.	33	2.64
Q4.12	The organisation has a means to provide reliable and accurate configuration information to the Service Desk regarding new Configuration Items.	33	2.64
Q4.9	The organisation has a reliable configuration database used routinely when building or installing new configuration items.	33	2.52
Q4.7	The organisation has clear mechanisms in place for retrieving, updating and analysing configuration items information.	33	2.42
Q4.10	The organisation has accurate configuration data to be used routinely for capacity planning purposes to ascertain the actual growth of configuration items within the organisation.	33	2.39
Q4.6	There is an effective system that links configuration records and known errors together within the organisation.	33	2.27
Q4.13	The organisation has a means to provide reliable and accurate configuration information to capacity management concerning growth estimates based on CMDB.	33	2.27
Q4.2	The organisation has implemented tools to automatically check and verify the validity of the CMDB data.	33	2.27
Q4.3	The effective tools that baseline the ICT components in the production/live environment are currently being implemented and running within the organisation.	33	2.24
Q4.1	A comprehensive and effective CMDB system across ICT is currently running effectively within the organisation.	33	2.18

3.6 CONCLUSION

The overall findings of the study are that the implemented processes are not achieving the intended objectives. The majority of the mean scores are slightly under the "slightly agree" score towards "slightly disagree". This is an indication that processes cannot run effectively without a proper and updated CMDB (CMDB) in place.

The ITIL framework and CMDB awareness in a form of more development and training is also need to be undertaken as most of the respondents have only basic knowledge of the ITIL framework and the CMDB.

The benefit of the ITIL processes and mainly the importance of implementing a comprehensive CMDB must be emphasized. There is a need to clearly outline a business case on why CMBD is important. As a detailed investment proposal, include within the business case a detailed analysis of all the costs, benefits, and risks associated with the proposed investment of implementing CMDB. The investment decision must be put into the context of strategic business goals.

Planning and forecasting is part of any growing and developing organization, and this can only be achieved by an updated CMDB. The configuration management information and mature processes must be implemented in order to allow for clear planning of ICT projects and a proactive analysis of those projects' real impact on both the ICT environment and the overall capability of the business.

The implementation and running of the ITIL framework processes can only succeed if a proper CMDB is up and running. Their incident is not being resolved timeously, primarily because the incident management is not optimally utilized, due to lack of CMDB. The change management process does not function as it should function due to a lack of proper configuration management with configuration Items updated.

3.6 SUMMARY

The study has formulated a measuring instrument in the form of a questionnaire in order to evaluate the importance and the role of CMDB in the ICT environment.

The participants were extremely helpful in compiling and completing the questionnaires during their working time, despite the fact that in some departments they were very busy with tight deadlines. The process office inputs were very valuable on how to structure and formulate relevant questions that constituted the questionnaire. The Department of Statistics and Consultation Services from the North-West University (Potchefstroom campus), was also very helpful on conducting the statistical analysis in the completed questionnaires.

Highlights of the results are the following:

Some 42.43% of the respondents (the highest figure), were middle management. This reflects a true situation as middle management in an organisation has the primary job responsibility to monitor activities of subordinates while reporting to upper management. Junior management is second at 39.39% of the respondents. This indicates an ideal distribution of the management levels in driving the implementation of the ITIL processes.

The 63.64% of the participants have intermediate knowledge of the CMDB, which is an indication that the organisation has undertaken an initiative to educate staff members on the ITIL framework. However, much needs to done on the advanced knowledge of CMDB in the organization as the percentages stand at only 6.06%.

The awareness of the participants on ITIL processes stand at 60.61% for the intermediate knowledge and a lot of work still needs to be carried out to improve employees knowledge to the advanced stage as only 12.12% have advanced knowledge.

The majority of the participants in the study have a basic knowledge of COBIT. There are 63.64% of participants with the basic knowledge of COBIT and the smallest percentage were employees with the advanced knowledge.

There is a positive attitude of the respondents toward the ITIL framework and processes. Some 63.64% of the participants totally accept and encourage the implementation of the ITIL processes. Another 36.36% of the participants had only an acceptable attitude toward ITIL processes implementation.

The majority of the respondents, with a mean = 3.48, have emphatically agreed that the organisation has recognised the need to identify all the ICT components within the organisation environment for better service provision. The other recognisable observation is that the majority of the respondents agree that the company will have to ensure that a reliable repository system to identify the assets is in place as majority of the respondents mean is (x = 2.94), which is way below the acceptable level.

The respondents unanimously agreed that the organisation has not established a regularly updated and useful repository to record all ICT assets or components information in scope. The mean of the respondents is just over the mean (x = 2.54) which is half way between the "slightly disagree" and "slightly agree" scale.

The respondents have indicated that not enough value have been gained from the implementation of the configuration management without a proper CMDB in place. The mean score is between x = 3.00 "slightly agree" scale and x = 2.42 which is just over "slightly disagree".

The group has indicated that there is no proper repository system like CMDB in place. The highest mean score achieved is x = 2.73 which is slightly below the scale slightly agree and the lowest score achieved is x = 2.18 which is slightly above the scale slightly disagree. The lowest mean was on whether the organisation has a comprehensive and effective CMDB system across ICT running effectively within the organisation.

Chapter 4 presents the conclusions and recommendations of the study.

CHAPTER 4

CONCLUSIONS AND RECOMMENDATIONS

4.1 INTRODUCTION

In this final chapter conclusions and recommendations are made to the organisation of choice on its current state of the lack of working configuration Items repository systems like the CMDB. A proper repository system will ensure that the organisation gets value from other current implemented processes such as configuration and change management processes.

The recommendations will be based on:

- The literature study that has been conducted during the research;
- The empirical study that was conducted; and
- The researcher's experience and knowledge within the ICT sector.

4.2 CONCLUSIONS

The arithmetic mean of the evaluation of the sections and questions by all staff members that participated in the survey indicates a general criterion that the current processes cannot function optimally without a proper CMDB system in place.

If one compares the sections and questions relatively with each other, the following conclusions may be drawn from this study.

4.2.1 General Information

A total of 63.64% of the staff members from the respondents that participated in the study have a totally positive and acceptable attitude towards the implementation of ITIL processes, including a comprehensive CDMB system.

The challenges are that the majority of the respondents have a limited knowledge on the ITIL processes and the CMDB knowledge. Some 60.61%, which are the majority of the respondents, have an intermediate knowledge on the ITIL processes and 63.64% have an intermediate knowledge on the CMDB. There is a lot of awareness around ITIL and CMDB that will need to be carried out by the organisation.

4.2.1 The organisation's approach to individual ICT components

The respondents unanimously agree that the organisation has recognised the need to identify all ICT assets/components within the ICT environment for better service provision. This is indicated by a mean which is half to strongly agree and slightly agree ($x = 3.48$). The participants slightly agree ($x = 3.00$) that the organisation has documented detailed and useful procedures for making changes to the ICT assets/components within the ICT systems. However, the score moves below to slightly agree ($x = 2.94$) on whether the organisation has identified and recorded all the ICT assets/components in a properly managed and updated database system. This score indicates the lack of proper and functioning CMDB and this does not help even though proper procedures are in place as indicated above. The score of $x = 2.94$ further confirms that the organisation has no reliable repository system with information or attributes about each ICT assets/components in the organisation. This further confirms that the absence of the proper CMDB in the organisation is much more evident, and that there is an absolute need for it.

The six lowest ranked questions are all drifting from the mean score of slightly agree to slightly disagree. These scores indicate that the organisation has no useful and clear relationships, or links that define how each ICT asset/components is interconnected and interdependent with its neighbours. This, once again, indicates the lack of a CMDB, as one of the functions of the CMDB is to keep records of how the configuration items are interconnected and its relationships. The lowest score is the mean of $x = 2.54$, which indicates that the organisation has not established a regularly updated and useful repository to record all the ICT assets/components.

4.2.3 The value gained from the implementation of configuration management

The mean scores for this section rank from x = 3.00 (slightly agree) down to x = 2.42 (a little bit above the slightly disagree score). The respondents' mean score of (x = 2.88) indicate that they do not completely agree that the traceability of changes from defined requirements can be easily executed because of a lack of a CMDB system. The mean score of x = 2.61 does not agree that the implementation of the configuration management has helped in terms of improving adherence and compliance with standards, legal and regulatory obligations. The study has also established that the presence of the configuration management has not enabled the organisation to have a better forecasting and planning and this proved the mean score of x = 2.42 (closer to slightly disagree scale).

4.2.4 The status and the role of CMDB within the organisation

The mean scores achieved on this section ranges from x = 2.73 down to x = 2.18. This indicates an overall result that the status and the role of the CMDB has not been implemented and defined within the organisation. The mean score of x = 2.73, which is slightly below the scale of slightly agree, indicates that the organisation does not have a means to receive notification from, or provide information to change management relating to every configuration item to be changed or introduced. This information from the CMDB for change management is very important as it assist the organisation to assigns the correct priorities and the impact of the change on the network.

There is no proper working systems that link the changes and configuration records together within the organisation. The mean score of x = 2.64, which is sliding towards slightly disagree on the scale, indicates that the organisation does not have reliable configuration data routinely used to perform configuration change impact assessments. The organisation also lacks a clear mechanism to retrieve, update and analyse configuration items and this is indicated in the mean score of x = 2.42, which is more towards the scale of slightly disagree. The organisation does not have accurate configuration data to be used routinely for capacity planning purposes to ascertain the actual growth of configuration items within the company. The mean score of x =2.27, which is more to slightly disagree scale, indicates that the organisation also lacks the means to provide reliable and accurate configuration information for capacity

management concerning growth estimates based on CMDB. The company does not have effective tools that baseline the ICT components in the production environment. This is one of the major roles of the CMDB and without a proper CMDB the organisation will be unable to baseline the ICT components. Finally, the mean score of x = 2.18 which is very close to slightly disagree, indicate that the organisation has not implemented a proper and working CMDB system.

4.3 RECOMMENDATIONS

The organisation has implemented a number of processes such as configuration and change management. To be successful with using the ITIL change management process, it is important that the people, processes, and technologies work together in a coordinated manner to overcome the political roadblocks that usually inhibit cooperation between groups in the same organisation. The research has indicated that the currently ITIL processes such as change management are not achieving the required results due to a lack of a proper CMDB.

General recommendations on the implementation of the CMDB will be given supported with the purpose.

ACTIONS	PURPOSE
Get executive and Board of Directors support on the implementation of CMDB.	Executive management must clearly support the implementation of CMDB throughout the enterprise. Without this support, the people who must be involved with implementing the necessary changes will not do so and will continue with business as usual. This is in line with King III which recommends that the Board needs to take responsibilities on ensuring that the organisation is compliant with the ICT governance principles. The study indicated 18.18% of top management participated in the research.
The organisation needs to redefine the role of the	This is to enable a broader responsibility and interact regularly on matters of ICT governance with the board. The CIO will adopt and implement an ICT control framework. The CIO will

general manager - ICT to a more appropriate role of Chief Information Officer reporting directly to the board.	ensure that ICT management design the processes which include the CMDB for risk management based on the Board's appetite for risk, the company's defined risk philosophy and the company's short and long-term strategies. This will help the organisation to establish a comprehensive function to manage the identification and recording of all ICT assets/components, both spares and functional.
The organisation must define detailed business processes and procedures.	These procedures will serve as a guideline on how to go about making changes on the CMDB and the monitoring of the changes of configuration items. This will have to be coupled with the risk management plan. The risk management plan should include an implementation plan, which should be monitored and have scheduled reviews.
The organisation must set a clear scope of the CMDB.	The organisation must identify and document the scope for which the CMDB will apply. This must fully define the aims and objectives to be realised on implementing CMDB.
The relevant stakeholders of the CMDB must be identified.	Define, identify, and map the stakeholders for the CMDB implemented. Identify the specific needs for each of the types of stakeholders identified. This information will be used in assessing the success of the CMDB for the corresponding stakeholders. This will assist the organisation not to fall into the trap of implementing something that will not be of value to the customers.
A full state of the current ICT processes must be determined.	The organisation must determine the need to improve upon the ways ICT processes are currently being performed. This calls for a regular ICT audit around processes and compliance requirements and fulfilment. This need must be documented to validate to the stakeholders why change is necessary.
The business case on the CMDB must be formulated and documented.	The single biggest factor in successfully implementing the CMDB will likely be overcoming resistance to change. To overcome the challenge, partner with all its stakeholders to gain their buy-in for the changes as well as using their input for creating the processes to be implemented. Use the information from the assessment and benchmark to build the business case.

Set goals on what the CMDB will have to achieve.	Establish documented goals to be able to know whether the efforts are successful. Clearly define the goals for the specific organisation for implementing of the CMDB.
The organisation must create a plan on the implementation of the CMDB.	Carefully develop the implementation plan. Too many organisations spend too little time planning implementations, and then end up spending ten or twenty times more doing the actual implementation than they would have spent if they had just invested more planning time upfront.
Identify responsibilities on maintaining the CMDB.	This is necessary to ensure that the CMDB is maintained and the configuration items get regularly updated. This will identify the process owners and the department that will assume the responsibility of updating the CMDB regularly. This will also ensure that the organisation has a means to assign owners to different ICT assets/components in scope.
Create awareness within the organisation around CMDB.	The implementation plan and the purpose of the CMDB must be clearly and effectively communicated to each of the key stakeholders. Ask for feedback to ensure that the needs from each of areas are adequately incorporated into the CMDB as well as to obtain ongoing support. The majority of the participants at 60.61% only have basic ITIL knowledge and 63.64% have intermediate knowledge of CMDB. The CMDB and ITIL awareness will have to be improved.
Training on CMDB must be offered to the personnel.	Success cannot be accomplished with a group of implementation folks who have no knowledge about what must be done around the CMDB. Training the team members for the CMDB is yet another key to success for the process implementation. This will also help create awareness on the team members around the CMDB.
The organisation must baseline all ICT assets.	This will assist to establish a control mechanism for making changes to the systems, and insist that every change go through the mechanism that has been described.
Plan for ongoing management of the	To keep the CMDB effective, the organisation needs to develop and consistently follow plans for ongoing

CMDB.	management and operations activities. These activities can be simplified and made more efficient through automation.

The study revealed that there is a dire need for an implementation of a central repository system like the CMDB to support other service delivery and support processes. If the recommendations are implemented within Sentech, the company will secure a more effective and efficient service delivery on the ICT platform. Furthermore, Sentech can become an ICT leader and gain a competitive advantage over its fellow competitors.

REFERENCES

ADDY, R. 2007. Effective IT service management to information technology infrastructure library and beyond. Springer-Verslag. Berlin: Heidelberg Press. 364 p.

ANDERSON, D.H. & REID, R.C. 2003. A study of the growth of the information system function and the Nolan development model. *Journal of computer information systems*, 38(3):44-48.

ANON. 2005. IT Governance Institute (IGTI). 2005. COBIT 4. 10 p. [Web]: www.itgi.org/ Date of access: 10 June 2009.

ANON. 2007. White Paper on configuration management database -options for the Fortune 100 000. Kace Networks. [Web]: www.kace.com/pdf/?doc=KACE-Scales-to-Larger-Enterprise. Date of access: 7 May 2009.

BENAMATI, J., LEDERER, A.L. & SINGH, M. 2005. Information technology change: the impact on IT management. *Journal of computer information systems*, 38(4):9-13.

BERKHOUT, M., HARROW R., JOHNSON, B. & SHIRLEY, L. 2003. Information technology infrastructure library: the key to managing information and communication technology services. Service Support. TSO. 16 p.

BETZ, C. 2006. Architecture and patterns for IT service management, resource planning and governance: making shoes for Cobbler's children. Boston, Mass.: Morgan Kaufmann. 100 p.

BISHOP, T. 2005. White Paper on information technology infrastructure library and configuration management database synergy – enhanced service management. [Web]: http://www.thinkhdi.com/resources/whitePapers/archive.aspx Date of access: 20 August 2009.

BMC SOFTWARE. 2006. The configuration management database: relief for your IT headaches. Houston, TX.: BMC Publishers. 5 p.

CLINE, M.K. & GUYNES, C.S. 2004. A study of the impact of information technology investment on firm performance. *Journal of computer information systems*, 41(3):15-19.

COZBY, P. C. 1993. Methods in behavioral research. 5th ed. Mountain View, CA.: Mayfield. 170 p.

DELUCCIA, J. 2008. IT compliance and controls: best practices for implementation. Indianapolis, IN.: Wiley. 160 p.

DETTMER, K. & WATSON, A. 2006. White Paper on project guideline for implementing a configuration management database. [Web]: http://whitepapers.techrepublic. com.com/abstract.aspx?docid=270376&promo=100511. Date of access: 02 February 2009.

GILBERT, A.H., PICK, R. A. & WIRD, S.G. 2004. Role of the CIO: enduring MIS issues. *Journal of computer information systems*, 40(1):8-14.

HEROLD, R. 2007. IT service management and automation. Realtime Publishers. Available on Realtime. [Web]: http://nexus.realtimepublishers.com/authors/Rebecca_ Herold.php Date of access: 20 October 2009. 103 p.

HEROLD, R. 2008. IT service management and automation. Realtime Publishers. 88 p. Available on Realtime. [Web]: http://nexus.realtimepublishers.com/authors/Rebecca_ Herold.php Date of access: 20 October 2009. 11 p.

HILL, P. & TURBIT, K. 2006. Combine ITIL and COBIT to meet business challenges. Houston, TX.: BMC Software Publishers. 19 p.

KAHAI, P.S., SNYDER, C.A. & CARR, H.H. 2003. Decentralizing the IS function: resources and locus of decisions. *Journal of computer information systems*, 42(2):44-60.

KAZDIN, A. E. 2003. Research design in clinical psychology. 4th ed. Boston, Mass.: Allyn & Bacon. 203 p.

KING, W.R. & POLLALIS, Y.A. 2003. IT-based coordination and organisational performance: a gestalt approach. *Journal of computer information systems*, 41(2):64-75.

KLOSTERBOER, L. 2008. Implementing information technology infrastructure library configuration management. Armonk, N.Y.: IBM Press. 10 p.

LACY, S. & MACFARLANE, I. 2006. Implementing information technology infrastructure library V3: service operations. Core practice book no 3. London, UK: The Stationary Office of the Office of General Commerce. 10 p.

LEE, A. 2006. White Paper on configuration management – the "not so obvious" starting point. [Web]: http://whitepapers.techrepublic.com.com/abstract.aspx?docid= 156881 Date of access: 2 February 2009.

LIELL-COOK, S., GRAHAM, J. & HILL, P. 2007. IT governance aligned to King III. IT Governance Networks. http://www.itgovernance.com/00/index.php/articles-aamp-news-mainmenu-2/51-itgovking Date of access: 26 October 2009

MARCZY, G., DEMATTEO, D. & FESTINGER, D. 2005. Essentials of research design and methodology. San Francisco, CA.: Wiley. 150 p

MEZGAR, I. 2006. Integration of information and communication technology in smart organisations. Istanbul: Idea Publishing House. 122 p.

MINOLI, D. 2005. A networking approach to grid computing. San Francisco, CA.: Wiley. 231 p.

MOELLER, R. 2008. Sarbanes-Oxley Internal Controls: Effective Auditing with AS5, CobiT, and information technology infrastructure library. Indianapolis, IN.: Wiley. 96 p.

OLDFIELD, A., STERBENS, R. & WASCHKE, M. 2005. White Paper on CMDB, Change and Configuration Management. [Web]: http://whitepapers.bx.businessweek.com/index.php?option=com_advsearch&task=search&searchword=cmdb Date of access: 13 August 2009.

RUDD, C. 2004. Introduction to information technology infrastructure library - pocket guide. 2nd ed. London: ItSMF. 42 p.

SCOTT, D. 2006. Conference poll on configuration management databases shows some progress. Gartner research. [Web]: http://www.gartner.com/DisplayDocument?ref=blog&id=491590 Date of access: 5 October 2009. 6 p.

WARD, J. & PEPPARD, J. 2004. Strategic planning for information systems. 3rd ed. Hoboken, NJ.: Wiley. 774 p.

ANNEXURE 1: QUESTIONNAIRE

Purpose of the questionnaire

The purpose of this survey is to examine the importance and the need of the CMDB in the ICT. Business-critical environments tend to have a significant number of processes that use the CMDB and require strict adherence to maintain a reliable production state and regulatory compliance (Dubie, 2006: 2).

You are invited as a prospective participant to complete this questionnaire.

Prospective participants are requested to focus on the following aspects:

- Participation in the completion of this questionnaire is voluntary and anonymous.
- To complete this questionnaire should not take longer than thirty (30) minutes.
- Please use a black pen to complete the questionnaire.
- The researcher strives to maintain absolute confidentiality and anonymity and therefore encourages participants to answer this questionnaire with honesty.

Outlay of the questionnaire

Section 1: General information about the participant.
Section 2: Organisation approach to individual ICT components.
Section 3: The value gained from implementation of configuration management.
Section 4: The importance and the role played by CMDB in ICT environment.

Thank you very much for completing this questionnaire. Your responses and comments are valued very dearly. After completion please place the questionnaires in the provided sealed envelope and send to the return address.

Section 1: General information

The following information is needed to help with the statistical analysis of the data for comparisons among different interest groups. All responses will be treated confidentially. Individual responses will not be seen by anyone in the organisation. We appreciate your help in providing this important information.

Mark the applicable block with a cross (X).
Complete the applicable information.

1. In which age group do you fall?

< 30	
30 – 39	
50 - 59	
60+	

2. In what post leve are you?

Top management	
Middle management	
Junior management	

3. Level of your knowledge on CMDB

Basic knowledge	
Intermediate knowledge	
Advanced knowledge	

4. Level of your knowledge on ITIL processes

Basic knowledge	
Intermediate knowledge	
Advanced knowledge	

5. Level of your knowledge on COBIT processes

Basic knowledge	
Intermediate knowledge	
Advanced knowledge	

6. What is your attitude towards processes?

Negative	
Acceptable	
Totally acceptable	

7. In which functional department do you work in?

Operations	
Technology & Planning	
Administration	

Section 2: Organisation approach to individual ICT components

Virtually all the questions may be answered by making a cross (X) in the relevant block. Use the following key: **1 = Strongly disagree; 2 = Slightly disagree, 3 = Slightly agree; 4 = Strongly agree; 5 = Not sure. You must select the number which best describes how you feel about the item. It is important that you complete all the questions**.

1) The organisation has recognised the need to identify all ICT assets/components within our environment for better service provision.

1	2	3	4	5

2) The organisation has identified and recorded all the ICT assets/components in a properly managed and updated database system.

1	2	3	4	5

3) The organisation has a reliable repository system with information or attributes about each ICT assets/components in the company, e.g. unique number, name, assets tag, and version.

1	2	3	4	5

4) The organisation has an authentic set of records that defines the version of each ICT assets/components.

1	2	3	4	5

5) The organisation has baselined all ICT assets/components in order to allow monitoring of progress or changes to components on the ICT systems more carefully.

1	2	3	4	5

6) The organisation has useful and clear relationships, or links that define how each ICT asset/component is interconnected and interdependent with its neighbours within ICT systems.

1	2	3	4	5

7) The organisation has established a regularly updated and useful repository/repositories to record all ICT assets/components information in scope.

1	2	3	4	5

8) The organisation has established documented procedures that describe how ICT assets/components should be identified, recorded and controlled.

1	2	3	4	5

9) The organisation has documented detailed and useful procedures for making changes to ICT assets/components within the ICT systems.

1	2	3	4	5

10) The organisation has established a comprehensive function to manage the identification and recording of all ICT assets/components (both spares and functional).

1	2	3	4	5

11) Detailed and understandable documented standards procedures have been established for naming conventions on ICT assets/components.

1	2	3	4	5

12) Detailed business processes as well as ICT assets/components have been clearly defined and ensure that quality service is offered.

1	2	3	4	5

13) The organisation has a means to assign owners to different ICT assets/components in scope.

1	2	3	4	5

Section 3: The value gained from implementation of configuration management

Virtually all the questions may be answered by making a cross (X) in the relevant block. Use the following key: **1 = Strongly disagree; 2 = Slightly disagree, 3 = Slightly agree; 4 = Strongly agree; 5 = Not sure. You must select the number which best describes how you feel about the item. It is important that you complete all the questions.**

1) The implementation of a configuration management system has seen an improvement of a number of business opportunities through better control of assets and services.

1	2	3	4	5

2) The implementation of configuration management has seen an adherence/compliance with standards, legal and regulatory obligations.

1	2	3	4	5

3) The existing configuration management system has seen an improvement on audit non-conformances received.

1	2	3	4	5

4) The current configuration management process has enabled the organisation to have a better forecasting and planning of network changes.

1	2	3	4	5

5) The success of network changes has improved due to the implementation of configuration management.

1	2	3	4	5

6) The traceability of changes from defined requirements can be easily executed because of the existing configuration management process.

1	2	3	4	5

7) The organisation is able to achieve required service levels due to the present configuration management process.

1	2	3	4	5

8) The current configuration management system is able to assist in accounting for number of contractual warranty claims made.

1	2	3	4	5

9) The implemented configuration management process is able to assist with a proper identification of the costs of the organisation services.

1	2	3	4	5

10) The currently running configuration management system is the reason for the shorter time taken to resolve incidents.

1	2	3	4	5

11) Please supply any additional related comments under this section.

Section 4: The status and role of CMDB within your organisation

Virtually all the questions may be answered by making a cross (X) in the relevant block. Use the following key: **1 = Strongly disagree; 2 = Slightly disagree, 3 = Slightly agree; 4 = Strongly agree; 5 = Not sure. You must select the number which best describes how you feel about the item. It is important that you complete all the questions.**

1) A comprehensive and effective CMDB system across ICT is currently running effectively within the organisation.

1	2	3	4	5

2) The organisation has implemented tools to automatically check and verify the validity of the CMDB data.

1	2	3	4	5

3) The effective tools that baseline the ICT components in the production/live environment are currently being implemented and running within the organisation.

1	2	3	4	5

4) There is a working system that links changes and configuration records together within the organisation.

1	2	3	4	5

5) There is a working system that links incident/service requests and configuration records together within the organisation.

1	2	3	4	5

6) There is an effective system that links configuration records and known errors together within the organisation.

1	2	3	4	5

7) The organisation has clear mechanisms in place for retrieving, updating and analysing configuration items (CI) information.

1	2	3	4	5

8) The organisation has a reliable configuration data which is routinely used to perform configuration change impact assessments.

1	2	3	4	5

9) The organisation has a reliable configuration data used routinely when building or installing new configuration items.

1	2	3	4	5

10) The organisation has accurate configuration data to be used routinely for capacity planning purposes to ascertain the actual growth of configuration items within the organisation.

1	2	3	4	5

11) There is a means within the organisation to receive notification from, or provide information to change management relating to every configuration item to be changed or introduced.

1	2	3	4	5

12) The organisation has a means to provide reliable and accurate configuration information to the service desk regarding new configuration items.

1	2	3	4	5

13) The organisation has a means to provide reliable and accurate configuration information to capacity management concerning growth estimates based on CMDB.

1	2	3	4	5

14) Please supply any additional related comments under this section.

Thank you very much for your valued input.