Applying COBIT in an ERP environment, with specific reference to Qmuzik

FRÈDA KIEVIET

Assignment presented in partial fulfilment of the requirements for the degree of Master of Computer Auditing at the University of Stellenbosch.

Study leader: Dr Willie Boshoff

December 2006

DECLARATION

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

Signature: ……………………………….
Date: ……………………………….

ABSTRACT SUMMARY

ERP applications have evolved into enterprise-wide applications, which are generally acknowledged today as a critical component in an organisation's information strategy.

When implementing an ERP application, the control and governance of all IT processes are critical to ensure that value is delivered, risks are managed and that the investment in IT (ERP) delivers a reasonable return.

It should, therefore, be important to focus on mitigating IT process risks that have an impact on the ERP environment, so that the level of residual risk is acceptable and aligned with the business objectives.

This assignment focuses on using the generally accepted IT framework, **COBIT** (Control Objectives for Information and related Technology), as governance and control model. The criticality of each COBIT control objective (IT process) is evaluated by applying the COBIT control objectives in an ERP environment. Specific reference is also made to **Qmuzik** as an ERP application.
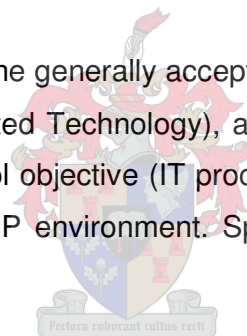
By applying COBIT in an ERP environment, the most critical IT processes applicable to ERP are identified, in order to ensure that the minimum process controls for these IT processes are designed and implemented.

OPSOMMING

ERP-stelsels het oor die afgelope dekades ontwikkel in sake-omvattende inligtingstegnologie (IT) stelsels, en word vandag algemeen as 'n kritiese komponent van 'n organisasie se inligtingstrategie erken.

Met die implementering van 'n ERP-stelsel, is die beheer en kontrole van IT prosesse dan ook krities om te verseker dat die investering in IT (ERP) die verwagte opbrengs kan lewer.

Dit is daarom belangrik om veral te fokus op die risiko's wat 'n impak het op 'n ERP omgewing, en dit só te bestuur dat die oorblywende risiko aanvaarbaar is en in ooreenstemming is met die onderneming se doelwitte.

Hierdie werkstuk fokus op die toepassing van **COBIT** (Control Objectives for Information and related Technology) as 'n algemeen aanvaarde IT-raamwerk. Die belangrikheid van COBIT se beheerdoelwitte (IT prosesse) word geëvalueer deur dit toe te pas in 'n ERP-omgewing. Spesifieke verwysing word dan ook na **Qmuzik** as ERP-stelsel gemaak.
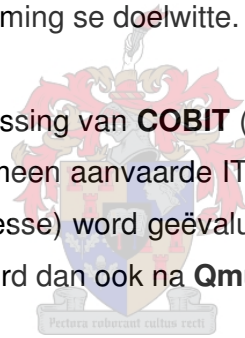
Deur COBIT as raamwerk toe te pas in 'n ERP omgewing, word die mees kritiese IT prosesse geïdentifiseer en sigbaar gemaak en dit kan verseker dat die minimum proseskontroles vir IT korrek ontwerp en geïmplementeer word.

TABLE OF CONTENTS

1   INTRODUCTION

In the present global information era there is an increasing dependence on information technology (IT) and on the systems that deliver this information. This makes the management of IT and related information technology critical to ensure the survival and success of organisations using such technology.

With the evolution of Information Technology it was possible for companies to streamline business processes, communicate more efficiently and most importantly to have information immediately available to ensure better and quicker management decisions. (Umble, Haft & Umble, 2003)

But IT is also exposed to various vulnerabilities and threats and with the rapidly changing business environment, new risks are identified and introduced virtually daily.

When delving a level deeper and focusing specifically on ERP applications, the same IT risks apply and these have a direct impact on the success and the value that ERP applications contribute to the process in question. (ISACA, 2003)

Enterprise resource planning (ERP) software has established itself in recent years as a vital IT component for companies to be able to integrate all their business functions (Hong & Kim, 2002). Apart from the increasing dependence on ERP applications, the regulatory environment is also enforcing stricter control over information – and, therefore, IT related risk should be proactively managed to ensure complete it governance. (Stolovitsky, 2005)

The question arises as to how do organisations control all these IT risks to ensure that the ERP application delivers the value that it is intended to do? How do they manage and control risks to ensure that the ERP application is aligned with the IT, infrastructure, technology and resources? To be able to bridge this gap a reference framework is needed to align business needs, internal control and technology matters. (Cevera, 2005)

This assignment focuses on using a generally accepted IT framework, **COBIT** (Control Objectives for Information and related Technology), as governance and

1

control model. The criticality of each COBIT control objective (IT process) will be evaluated by applying COBIT in an ERP environment, and where specific reference will be made to Qmuzik as ERP system. This assignment will conclude that by applying COBIT in an ERP environment, this could result in an ERP environment that is controlled and manageable.

1.1   Purpose of assignment

This assignment focuses on identifying the most critical IT processes that need to be controlled in order to achieve a successful ERP implementation and sustainable ERP environment.

This assignment will demonstrate that the application of COBIT principles and practices could result in an ERP environment that is controlled, manageable and is contributing to overall IT governance and compliance.

Specific reference is also made in this assignment to an ERP application, Qmuzik; but the intention of the assignment is to show the applicableness of COBIT on a specific ERP application. The application of COBIT is, therefore, not only limited to Qmuzik as an ERP application, but also to ERP applications in general.

1.2   Research approach

The research approach for this assignment is to use a generally accepted IT framework as governance and control reference and to map the control objectives (IT Processes) to an ERP environment. The purpose of mapping COBIT to an ERP environment is to identify the most critical IT processes to be able to manage and control them in an ERP environment.

The specific ERP application that will be referenced is **Qmuzik**. The selected model is **COBIT**.

1.3 Assignment structure

```
┌────────────────────────────────────────────────────────────────────────┐
│  ┌──────────┐      ┌──────────┐      ┌──────────┐      ┌──────────┐     │
│  │   2:     │      │   3:     │      │   4:     │      │   5:     │     │
│  │  ERP &   │ ──▷  │  COBIT   │ ──▷  │ COBIT &  │ ──▷  │ SUMMARY  │     │
│  │  QMUZIK  │      │          │      │  QMUZIK  │      │          │     │
│  └──────────┘      └──────────┘      └──────────┘      └──────────┘     │
└────────────────────────────────────────────────────────────────────────┘
```
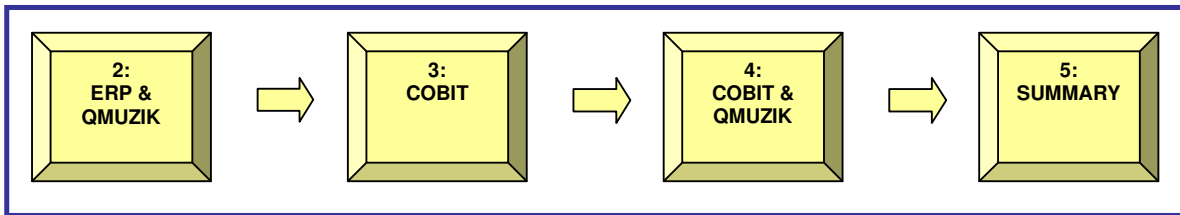
ERP & QMUZIK: Chapter 2 provides a brief overview of ERP. It will show the value that ERP contributes to organisations and also the inherent risks that accompany ERP applications. The chapter continues and gives a brief background on the selected ERP application: Qmuzik.

COBIT: Chapter 3 gives a background on control frameworks, and an overview of the control framework selected for this assignment, which is COBIT. It also states why COBIT is the selected framework for this assignment, and emphasise on the IT governance advantages of COBIT.

COBIT & QMUZIK: Chapter 4 then maps the control framework and ERP application. This identifies which are the critical processes to be managed in an ERP environment. A matrix is used to assess the importance of every COBIT high level control objective towards each information and resource criteria, from an ERP client's perspective.

The second part of this chapter elaborates on the most important control objectives arising from the matrix and allocates responsibility and actions to be considered between Qmuzik and the ERP client. Specific reference to supporting documentation and Qmuzik functionality is also included.

SUMMARY: Chapter 5 contains a concluding summary which will demonstrate that by mapping COBIT to Qmuzik, the critical IT processes could be controlled to ensure IT governance and a sound ERP environment.

1.4 Scope restriction

The scope of this assignment is limited to Qmuzik (Release 7.2) as ERP application. It also focuses on identifying and elaboration on the most important IT processes in an ERP environment. The details of how to perform the identified tasks and activities for each IT process do not lie within the scope of this document.

Arising from this assignment, a further project could be to define template documentation for essential policies and procedures required for each IT process.

2 ERP and QMUZIK
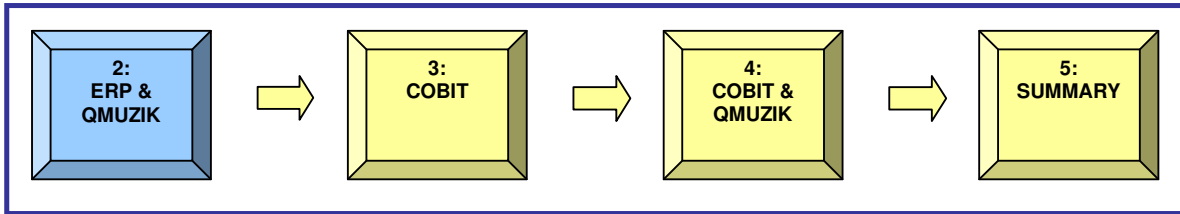
This chapter provides a brief overview of the background of ERP, why ERP applications are selected by organisations today and also what the inherent risks are that accompany ERP applications. Further more it also explains why there is a need for the use of a control framework to assist in controlling ERP risks and to achieve IT governance in the ERP application. It also provides a background of the ERP application selected, which is Qmuzik.

2.1 ERP background

The evolution towards ERP systems started in the 1960s. It began with manufacturing systems focusing specifically on inventory control. The problem of maintaining large quantities of inventory led to the introduction of Material Requirements Planning (MRP) systems in the 1970s. The ability of a planning system that schedules discreet material requirements was a huge step forward. MRP systems continued to expand and in the 1980s evolved into MRP II. Manufacturing Resource Planning (MRP II) represented the incorporation of financial systems with manufacturing and materials management systems. (Technology Evaluation Centre, 2005)

Technology steadily continued to improve and by the early 1990s, MRP II expanded by incorporating resource planning for the entire enterprise, and finally **ERP** - Enterprise Resource Planning was introduced (Umble *et al.*, 2003).

2.2 Why ERP?

"ERP relates to the software infrastructure that holds the entire company together internally on the one hand and supports the external business processes the company engages in, on the other." (Aberdeen Group, 2004)

According to the Aberdeen Research Group, the key features of ERP solutions are:

- ERP applications address business processes
- ERP applications are integrated
- ERP applications include a company's reach beyond its walls to its suppliers, customers and other business partners
- ERP applications are generally modular

The major benefits that ERP provide in comparison to non-integrated systems are defined by Umble *et al.* (2003) as:

- a unified enterprise view of the business that integrates ALL functions and business processes
- a single enterprise database where all business transactions are captured, processed, monitored and reported

With this unified view that ERP applications provide, it also increases the requirement for interdepartmental cooperation and coordination, but simultaneously it enables companies to achieve their objectives of increased communication and responsiveness to all key role-players.

A survey by Hong and Kim (2002) shows that the majority of IT managers perceived their ERP applications as the company's most strategic computing platform. Despite this perception as ERP being one of the most critical IT components, many ERP projects in the industry are still classified as failures and do not meet the predetermined goals as set by the organisation.

There are many risk factors that may contribute to the failing of an ERP application in an organisation. One of these is that many new ERP clients commit the error of regarding ERP as simply a software system and its implementation as primarily a technological challenge. They do not understand that ERP may fundamentally change the manner in which the company operates.

An ERP implementation involves changes in business processes, organisational structure, resources and technology, all usually within a short time period. (Umble *et al.*, 2003)

Umble *et al.* (2003:245) further state that with an ERP implementation, the ultimate goal should be to improve the business – and not to implement software. The implementation should be business driven directed by business requirements and not the IT department.

A great deal has been researched and documented regarding the question as to why ERP projects fail (Motwani, Mirchandani, Madan & Gunasekaran, 2002), what the critical success factors are for implementing ERP systems and common pitfalls in ERP projects (Hong & Kim, 2002*)*. This chapter will not explore further any details of implementing ERP, but would rather focus on risk control in an ERP environment and on the reason why there is a need for a control framework to assist in managing an ERP environment.

2.3   ERP environment and risks

In an ERP environment business processes are enabled and monitored by the ERP application. An ERP environment includes the following elements (Motwani *et al.*, 2002):

- *ERP Application* (e.g. Qmuzik)
- *People*; such as management, end-users, ERP implementation team, internal/external auditors
- *Organisation*; such as an ERP supplier, IT service providers, suppliers, customers

- *Infrastructure*; which includes hardware, network, operating systems, third party software applications

The IS Auditing Guideline (ISACA, 2003) indicates that an ERP application, because of its integrated nature, also contributes to risks which are related to

- Industry and business environment
- User and/or management behaviour
- Business processes and procedures
- System functionality
- Application security
- Underlying infrastructure
- Data conversion and integrity
- Ongoing maintenance and support
- Business continuity

ISACA (2003) concludes that the risks associated with the implementation and ongoing use of an ERP application should not be determined or controlled by only regarding in isolation the ERP application risks, but should rather be considered in conjunction with risks from the complete ERP environment. ERP systems are implemented to support the operations of the business. To be successful, all significant elements in an ERP environment should be pro-actively managed to ensure a successful ERP application.

2.4   ERP and IT governance

What is the right level of control for my IT such that it supports my enterprise objectives?

It is already known that ERP applications as such are complex systems and contain many inherent risk factors. One should also consider that a software application cannot perform in isolation, but strongly depends on the internal IT processes in order to be able to perform optimally.

ERP is not only a vital information source, but also a critical corporate governance tool. Management obtains financial information directly from the ERP application and, to achieve compliance with several regulatory and legislation acts, management needs to ensure the accuracy, completeness and timeliness of information. This needs to be done by establishing sound internal controls on ERP processes related to financial reporting. The application controls of an ERP application need to also take into consideration regulatory and legislation requirements to ensure IT governance and compliance. (ISACA, 2003)

Therefore, when implementing an ERP application, the control and governance of all IT processes that impact on the ERP environment are critical to ensuring that value is delivered, risks are managed and that the investments in IT (ERP) deliver a reasonable return. It is consequently evident that there is a need for a control framework as reference model for risk control in IT and also specifically in an ERP environment.

This assignment will elaborate further in chapter 3 why COBIT is the selected IT governance framework selected for this assignment.

2.5 QMUZIK as ERP application

Qmuzik is one of the registered software products of Cosource (Pty) Ltd, trading as Qmuzik. Qmuzik is a locally developed ERP application that was developed in the early nineties. The application was developed because the major ERP players at that stage lacked the necessary functionality and were too expensive for local companies. Since the first implementation, the number of Qmuzik's clients has grown rapidly in South Africa and also internationally.

One of the advantages of Qmuzik being a locally developed product is that support and implementation costs are affordable to local companies. Qmuzik are also business process driven, rather than a functionally driven solution, and this allows Qmuzik to initiate chain-on events without human intervention spanning the extended enterprise. The intuitive business process methodology and the role-based nature of
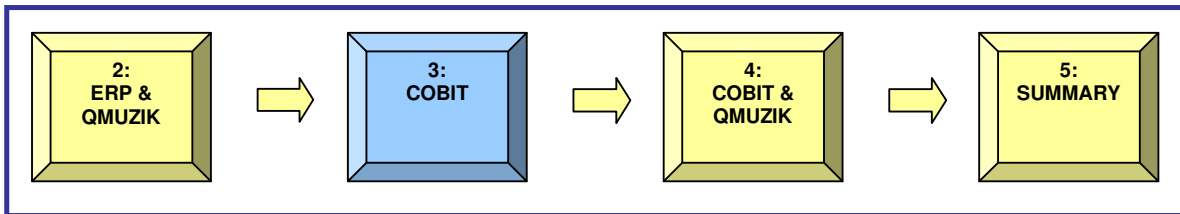
Qmuzik facilitate ease of use and rapid deployment of the system resulting in radically low life cycle cost. (Qmuzik, 2005).

Qmuzik is a real-time integrated ERP system and more detail on the technical architecture and specific Qmuzik ERP environment will be covered in chapter 4 when mapping each COBIT control objective (IT process) to Qmuzik.

3 COBIT

This chapter contains a brief overview of the control framework selected for this assignment, namely COBIT. The basic concepts and objectives of the COBIT framework will be explained. The focus is to provide some background as to why COBIT is the model selected and why this model is applicable for use in an ERP environment.

3.1 Control frameworks

What is a control framework? Cevera (2005) defines a standard framework as a set of best practices that are usually expressed as a set of repeatable processes that are created by an organisation (a professional association, university, public administration etc.) These frameworks are also referred to as bodies of knowledge or methodologies. The Institute of Internal Auditors (IIA, 2002) states that a control framework forces one to consider all aspects and provides one with a starting point. Without a framework one may end up with gaps and probably too much emphasis on the objectives that are not necessary the most important ones.

According to Rasmussen (2006), having a structured approach is a major step towards compliance with different standards and legislation, as this allows companies to prioritise IT controls. Rasmussen continues and states that this structured approach can be found when using a standard control framework.

Cevera (2005) lists several advantages of using a standard framework, which are:

- You can take advantage of the work done by experienced professionals in the field
- It establishes a standard terminology that enhances communication both internally and externally
- Software suppliers create products that are compliant with the framework

- Mainstream frameworks evolve over time and keep track of all new technology and risk issues

The most commonly known standard frameworks that were developed are (IIA, 2002):

- **CoCo's** **Guidance on Control**, issued by the Criteria of Control (CoCo) Board at the Canadian Institute of Chartered Accountants (CICA)
- **COSO** or *Internal control – Integrated framework*, published by the Committee of Sponsoring Organisations (COSO) of the Treadway Commission from the United States
- **The Cadbury Report**, Code of Best Practice, issued by the Cadbury Committee of the United Kingdom
- **The King Report** from South Africa
- **ITCG** – *Information Technology Control Guidelines,* published by the Canadian Institute of Chartered Accountants (CICA)
- **ITIL** – *IT infrastructure library,* which is a set of best practices documents and standards developed by the UK Office of Government Commerce (OCG)

Cevera (2005) continues and states that all these frameworks cannot necessarily be applied "out of the box" as they are aimed at a wide spectrum of organisations and need to be customised to the level of internal control and compliance required by each organisation. This is accomplished when each organisation translates the best practices of the framework into concrete procedures and policies that take into account the specific characteristics and environment of the organisation.

So where does COBIT fit in? COBIT is the acronym for **Control Objectives for Information and Related Technology**, and is an open standard for control over information technology. It was developed and supported by the IT Governance Institute (ITGI), formed by the Information Systems Audit and Control Association (ISACA) in 1998 specifically to advance the understanding and adoption of IT governance principles. The first edition of COBIT was published in 1996; the

second edition in 1998; the third edition in 2000 (the on-line edition became available in 2003); and the fourth edition in December 2005.

The mission of COBIT is "to research, develop, publicize and promote an authoritative, up-to-date, international set of generally accepted information technology control objectives for day-to-day use by business managers and auditors." (ITGI, 2005)

3.2 Why COBIT?

According to Stolovitsky (2005), COBIT standards are being increasingly adopted by companies as best practices in the governance of information, IT and risk. The COBIT Executive Overview (ITGI, 2005:7) confirms this and states that COBIT is accepted as the internal control framework for IT, where COSO is generally accepted as the framework for internal control for enterprises. COSO was developed as an overall business control model and is mainly aimed at management.

This brings us to the question: Why COBIT? Why not COSO? The major differences between COBIT and COSO are in the way they each define internal control, control objectives and also their intended audiences. Here follows more detail on the major differences, and subsequently why COBIT was selected for this assignment. (ITGI, 2005; Simmons, 2002).

Internal control:

- **COBIT** approaches IT control by looking at all information that is needed to support business requirements and the associated IT resources and processes
- **COSO** Internal control – Integrated framework states that internal control is a process established by an entity's board of directors, management, and other personnel; and is designed to provide reasonable assurance regarding the achievement of stated objectives.

Control objectives:

- **COSO** control objectives focus on effectiveness, efficiency of operations, reliable financial reporting, and compliance with laws and regulations.

- **COBIT** control objectives is extended to cover quality and security requirements in seven overlapping categories, which include effectiveness, efficiency, confidentiality, integrity, availability, compliance, and reliability of information.

Audience:

- **COSO** is mainly intended for use by senior management
- **COBIT** is intended for management, users, and auditors.

The final distinguishing feature of COBIT is that it provides a comprehensive and user-friendly control model that focuses on business objectives and, specifically, for the requirement of **internal control in IT.** Therefore, to summarise why COBIT was selected, and also defining the major advantages of implementing COBIT as governance framework over IT (ITGI, 2005:8):

- COBIT is accepted internationally, based on professional and practical experiences

- COBIT is compliant with ISO/IEC17799: 2005, and fulfils COSO requirements for an IT control environment

- A shared understanding between all stakeholders based on a common language

- COBIT is objective, it is continually evolving, and maintained by a non-profit organisation

- COBIT is management-orientated and easy to use

- COBIT has a flexible and adaptable approach to suit different organisations, cultures and requirements

- COBIT is the industry acknowledged IT governance guidance tool

3.3 COBIT product family

COBIT consists of a set of six publications, a brief overview of which is provided below (ITGI, 2005). The objective of the COBIT family of products is to ensure that IT is aligned with the business; IT enables the business and maximises its benefits; IT resources be used responsibly; and IT-related risks be managed appropriately.

- The **COBIT Executive Summary** is specifically designed with top management as audience, to give an executive overview of COBIT's key concepts and principles.

- The **COBIT Framework** consists of 34 high-level control objectives that explain how IT processes deliver the information that the business needs to achieve objectives. The framework defines how the seven information criteria as well as IT resources are critical for the IT processes to fully support the business objective.

- The **COBIT Control Objectives** provides the insight needed to define a clear policy and good practice for IT controls. It also states the 215 specific control objectives and the statements of desired results to be achieved when implementing these objectives.

- The **COBIT Implementation Toolset** is designed to assist project managers to facilitate the implementation of COBIT into organisations. It consists of case studies, frequently asked questions (FAQs), management awareness and IT control diagnostics to be able to help introduce COBIT to new audiences.

- The **COBIT Management Guidelines** comprises maturity models, critical success factors, key goal indicators and key performance indicators. These guidelines are intended to assist management to be able to measure whether an IT control process is meeting its objective and to compare the processes against an industry norm.

- The **COBIT Audit Guidelines** defines and suggests the actual audit activities to be performed corresponding to each of the 34 IT control objectives. This publication is an invaluable tool for IT auditors in providing management assurance and guidelines for improvement.
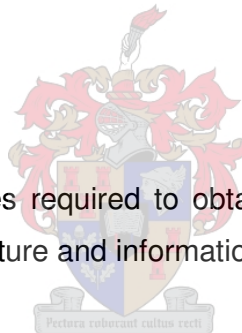
3.4 COBIT framework

The COBIT framework can best be understood as a three-dimensional framework (Yan & Makal, 1999). Interaction between these dimensions is needed to ensure that business objectives are met. The three dimensions are:

Information Criteria. These are minimum standards information needs to meet in order to fulfil business objectives. The criteria can either be primary or secondary in nature. They are:

- Effectiveness
- Efficiency
- Confidentiality
- Integrity
- Availability
- Compliance
- Reliability

IT Resources. The resources required to obtain and manage information include people, applications, infrastructure and information.

IT Processes. The IT processes need to ensure that information is gathered properly by the IT resources and meet the information criteria. The COBIT framework identifies 34 IT processes (high level objectives), and 215 detailed control objectives and audit guidelines to assess the 34 IT processes. The IT processes are categorised into four domains (ITGI, 2005:16):

- **Plan and organise domain**

  The plan and organise domain covers the use of technology and how best it can be used in a company to help achieve the company's goals and objectives. It also highlights the organisational and infrastructural form IT is to take in order to achieve optimal results and to generate the most benefits from the use of IT.

- **Acquire and implement domain**

This domain addresses identifying IT requirements, acquiring the technology, and implementing it within the company's current business processes. It also addresses the development of a maintenance plan that a company should adopt in order to ensure the continuity of an IT system and its components.

- **Delivery and support domain**

  The deliver and support domain focuses on the delivery aspects of the information technology. It covers areas such as the execution of the applications, data processing, as well as the support processes that enable the effective and efficient execution of these IT systems. These support processes include security issues and training.

- **Monitor and evaluate domain**

  The monitor and evaluate domain deals with a company's strategy in assessing the needs of the company and whether or not the current IT system still meets the objectives for which it was designed, and the controls necessary to comply with regulatory requirements. Monitor and evaluate also covers the issue of an independent assessment of the effectiveness of an IT system in terms of its ability to meet business objectives and the company's control processes by internal and external auditors.
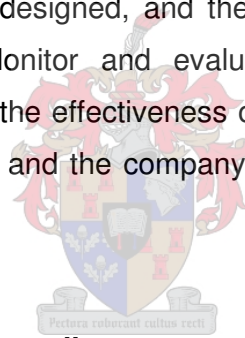
3.5 COBIT, IT governance and compliance

According to Stolovitsky (2005) one of the major goals for IT management is to maximise the value of their IT investments and, as in the case of this assignment, specifically ERP applications. Identifying risk, resource utilisation and earned value with a portfolio of IT projects necessitates the implementation and adoption of standards and processes to track and respond to any "red flags" that may appear. Stolovitsky claims that this can be accomplished by establishing IT governance.

COBIT was developed with **IT governance** as its focus point. COBIT defines IT governance as follows: "*... a structure of relationships and processes to direct and control the enterprise in order to achieve the enterprise's goals by adding value while balancing risk versus return over IT and its processes.*" (ITGI, 2005:3).

Stolovitsky further states that the difference between success and failure in today's high technology environment is based on the IT governance framework that companies adopt, and that the standards and processes put in place by COBIT as IT governance framework can also assist organisations with compliance issues, and specifically compliance with the Sarbanes-Oxley Act of 2002. Wise (2006) summarises the Sarbanes-Oxley Act (SOX) as follows:

- The Sarbanes-Oxley Act was established to protect investors from potential fraudulent accounting.

- The Sarbanes-Oxley Act affects any public corporation competing in the international marketplace.

- As a result of the Sarbanes-Oxley Act not only have financial controls become stricter, but responsibility for accurate financial reporting of financial results has been placed in the hands of organisational heads, namely the chief executive officers (CEOs) and the chief financial officers (CFOs) to ensure accurate financial and auditing information.

Armstrong (2006) concurs with Stolovitsky, and also states that while COBIT adoption is not mandatory for Sarbanes-Oxley compliance, it has becomes the "de facto" framework for making IT compliant with SOX regulations.

For the purpose of this assignment, it is proposed that by applying COBIT in an ERP environment it could result in an ERP environment that is controlled, manageable **and also** contributing to IT governance and compliance. As stated by Armstrong (2006), Stolovitksy (2005), and Wise (2006), COBIT is accepted internationally as the standard for IT governance and compliance management and it is therefore only logical that COBIT is the IT governance framework selected for this assignment.

4 COBIT and QMUZIK
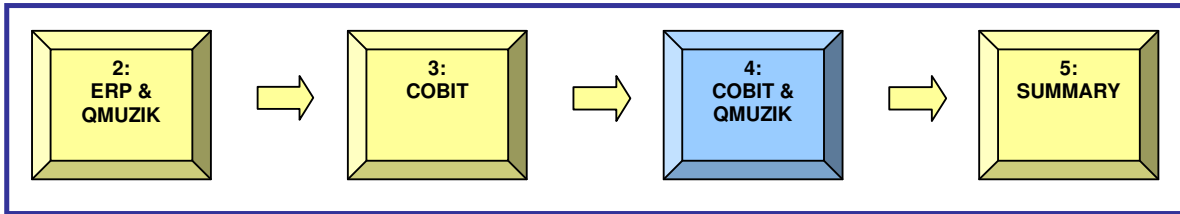
This chapter considers the control framework (COBIT) and maps the 34 control objectives to an ERP environment. The first matrix takes each IT process (COBIT control objective) and evaluates the criticality of each process from an ERP viewpoint.   This matrix analyse which are the most critical processes to be managed in a Qmuzik ERP environment. The second part of this chapter is then used to elaborate on the critical processes as identified in the first matrix and then allocate responsibilities, actions, supporting documentation and specific Qmuzik functionality to each critical IT process (control objective).

4.1   Assessment matrix of COBIT IT processes and QMUZIK environment

How important is each IT process in an ERP environment?
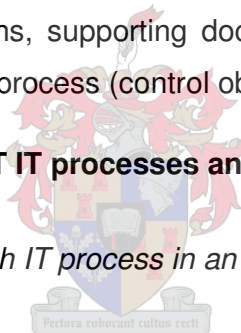
The following matrix evaluates the importance of each COBIT control objective with respect to an ERP environment from a client's viewpoint.

A rating of low, medium and high is allocated according to each COBIT information and resource criteria. This assessment is done taking the Qmuzik technical architecture, application controls, and ERP processes into consideration.

See the reference number noted next to specific IT processes to be elaborated in more detail in section 4.2.

COBIT and QMUZIK

4.1 COBIT assessment matrix

	Control Objective	Reference Note	Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability	People	Applications	Infrastructure	Information
PLANNING & ORGANISATION DOMAIN													
PO1	Define a strategic IT plan and direction		Low	Low	Low	Low	Low	Low	Low	Low	Low	Low	Low
PO2	Define the information architecture		Low	Low	Low	Low	Low	Low	Low	Low	Medium	Low	Medium
PO3	Determine technological direction		Low	Low	Low	Low	Low	Low	Low	Low	Low	Medium	Low
PO4	Define the IT processes, organisation and relationships	4.2.1	Medium	Low	Low	Low	Medium	Low	Low	**High**	Low	Low	Low
PO5	Manage the IT investment		Low	Low	Low	Low	Low	Low	Low	Low	Low	Low	Low
PO6	Communicate management aims and direction		Low	Low	Low	Low	Low	Medium	Low	Medium	Low	Low	Low
PO7	Manage IT human resources		Low	Low	Low	Low	Low	Low	Low	Low	Low	Low	Low
PO8	Manage quality	4.2.2	**High**	**High**	Low	Medium	Low	Low	Medium	**High**	**High**	Low	Medium
PO9	Assess and manage risks	4.2.3	Low	Low	Medium	Medium	Medium	Low	Medium	**High**	Medium	**High**	**High**
PO10	Manage projects	4.2.4	Medium	Medium	Low	Low	Low	Low	Low	**High**	Low	Medium	Low
ACQUIRE AND IMPLEMENT DOMAIN													
AI1	Identify automated solutions		N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
AI2	Acquire and maintain application software	4.2.5	Medium	Medium	Low	Medium	Low	Medium	Medium	Low	**High**	Low	Medium

COBIT and QMUZIK

	Control Objective	Reference Note	Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability	People	Applications	Infrastructure	Information
			Information Criteria							**Resource criteria**			
AI3	Acquire and maintain technology infrastructure	4.2.6	Medium	Medium	Low	Low	Medium	Low	Low	Low	Low	Medium	Low
AI4	Enable operation and use	4.2.7	Medium	Medium	Low	Low	Medium	Medium	Medium	High	Medium	Low	Low
AI5	Procure IT resources		Low	Low	Low	Low	Low	Low	Low	Medium	Low	Medium	Low
AI6	Manage changes	4.2.8	**High**	**High**	Low	**High**	**High**	Low	Medium	**High**	**High**	Low	**High**
AI7	Install and accredit solutions and changes	4.2.9	**High**	Low	Low	**High**	Medium	Low	Medium	**High**	**High**	Low	**High**
DELIVER AND SUPPORT DOMAIN													
DS1	Define and manage service levels	4.2.10	Medium	Medium	Low	Low	Low	Low	Low	**High**	Medium	Low	Low
DS2	Manage third party services	4.2.11	Low	Low	Low	Low	Low	Low	Low	**High**	Medium	Medium	Low
DS3	Manage performances and capacity	4.2.12	Medium	Medium	Low	Low	Medium	Low	Low	Medium	**High**	**High**	Low
DS4	Ensure continuous service	4.2.13	Medium	Medium	Low	Low	**High**	Low	Medium	Medium	Medium	Medium	Medium
DS5	Ensure systems security	4.2.14	Low	Low	Medium	**High**	Medium	Medium	Medium	**High**	**High**	**High**	**High**
DS6	Identify and allocate costs		Low	Low	Low	Low	Low	Low	Low	Medium	Medium	Low	Low
DS7	Educate and train users	4.2.15	**High**	Medium	Low	Low	Low	Low	Low	**High**	Low	Low	Low
DS8	Manage service desk and incidents	4.2.16	**High**	**High**	Low	Low	Low	Low	Low	**High**	Low	Low	Low
DS9	Manage the configuration	4.2.17	Medium	Low	Low	Low	Medium	Low	Medium	Low	Medium	Low	Low
DS10	Manage problems	4.2.18	Medium	Medium	Low	Low	Medium	Low	Medium	**High**	**High**	Medium	**High**
DS11	Manage data	4.2.19	**High**	Low	Low	**High**	Low	Low	High	Medium	Low	Low	**High**

	Control Objective	Reference Note	Information Criteria							Resource criteria			
			Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability	People	Applications	Infrastructure	Information
DS12	Manage physical environment		Low	Low	Low	Low	Low	Low	Low	Low	Low	Low	Low
DS13	Manage operations		Low	Medium	Low	Low	Medium	Low	Low	Medium	Medium	Low	Medium
MONITOR AND EVALUATE DOMAIN													
M1	Monitor and evaluate IT processes	4.2.20	Medium	**High**	Low	Low	Low	Low	Medium	**High**	**High**	Low	Medium
M2	Monitor and evaluate internal control	4.2.21	**High**	**High**	Low	**High**	Medium	**High**	Medium	**High**	Medium	Low	Medium
M3	Ensure regulatory compliance	4.2.22	Medium	Low	Low	Low	Low	**High**	Medium	Medium	Medium	Low	Medium
M4	Provide IT governance		Medium	Medium	Low	Low	Low	Medium	Low	Medium	Medium	Low	Low
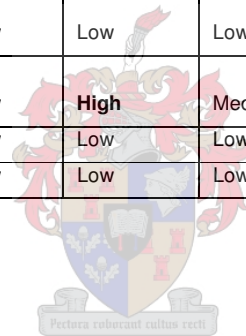
4.2   Qmuzik responsibility / action detail

COBIT Framework (ITGI, 2005:15) states that part of effective governance of IT processes is that the roles and responsibilities for each IT process are clearly understood. The following section defines the responsibility and critical activities or tasks that need to be considered by either the client or ERP (Qmuzik) supplier, in order to fulfil the applicable IT process (control objective).

The IT processes which are rated with an average rating of medium to high in the previous matrix are detailed in this section. The COBIT IT processes (control objectives) that are not referenced in the matrix are due to their criticality rating having been assessed as an average of low. The primary reason for this is that these IT processes do not necessarily have a high impact on the effective administration, performance, maintenance and support of the Qmuzik application. However, these processes might have a major role outside of the Qmuzik ERP environment, and as part of the overall IT function. The specific scenario and scope of each project can also reasonably alter this assessment's rating and might cause specific processes to be included or omitted as critical to the Qmuzik ERP environment.
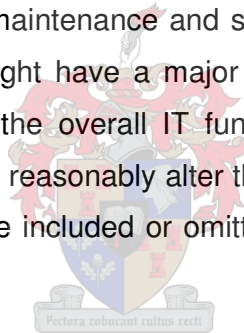
This section was compiled after a discussion session with senior business analysts from Qmuzik (Kieviet, 2005). The following COBIT documents were taken into consideration:
- COBIT high level control objectives (ITGI, 2005)
- COBIT detailed control objectives (ITGI, 2005)
- COBIT RACI (Responsible, Accountable, Consulted and/or Informed) chart (ITGI, 2005)
- Enterprise Resource Planning Systems Review (ISACA, 2003).

The IS Auditing Guidelines (ISACA, 2003) consider documented policies and procedures as essential for good control and also as a matter of continuity and

good practice. A lack of documentation should be considered a cause for review for any specific IT process. Therefore, the following are also detailed for each IT process:

- **Supporting documentation** – These documents can either be input or output documentation for each IT process and can apply to Qmuzik and/or the client.
- **Qmuzik specific functionality** – If the functionality exists primarily to manage the specific IT process, it is indicated by a 'P', or, if it supports the IT process, it is indicated by an 'S'. A brief statement of referenced Qmuzik functionality can be found in Appendix A.

The overall objective or outcome of defining these responsibilities, actions and documentation is to achieve the following for each IT process:

- Defined and documented processes
- Defined and documented policies
- Define and ensure clear responsibilities and accountabilities
- Create awareness at management for strong support and commitment
- Establish appropriate communication between all role-players
- Establish consistent measurement practices.
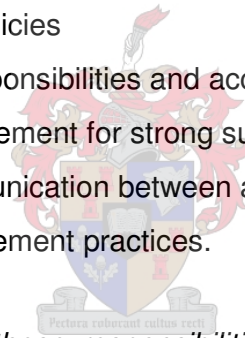
Please note: The intention of these responsibilities and actions is only a general guideline and not intended to be exhaustive. COBIT is a well documented framework and should be referred to for more detail on each IT process.

PLANNING & ORGANISATION DOMAIN

4.2.1 Organisational support structures for Qmuzik

COBIT defines this IT process (control objective) as follows:

"An IT organisation must be defined considering requirements for staff, skills, functions, accountability, authority, responsibilities, and supervision. This organisation is to be embedded into an IT process framework that ensures transparency control as well as the involvement of senior executives and business management. A strategy committee should ensure oversight of IT and one or more steering committees, in which business and IT participate, should determine prioritization resources in line with business needs. Processes, administrative policies and procedures need to be in place for all specific attention to control, quality assurance, risk management, information security, data and systems ownership, of duties. To ensure timely support of business requirements, IT is to be involved in relevant decision processes." (ITGI, 2005:41)

	QMUZIK (ERP)	CLIENT/ THIRD PARTY
RESPONSIBILITY / SUCCESS FACTORS	• Define clear roles and responsibilities between Qmuzik and client • Qmuzik relies on internal IT to setup client installations, adequate network access, user profiles, installation of printers and all other hardware • Participate in IT steering committee • Establish and maintain relationships	• Define IT organisational structure • Define and identify key IT personnel • Define responsibility for quality assurance, security, compliance and IT risk management • Ensure and implement effective segregation of duties and IT supervision. • Identify and allocate data and system ownership • Define IT policy and procedures for external consultants • Establish and maintain relationships • Establish IT steering committee
DOCUMENTS	• IT organisational structure • Non disclosure agreement • Electronic communication policy	
QMUZIK FUNCTIONS	• Business Model Viewer (S) • External Object Linking (S) • Document Management (S) • Qmuzik Explorer (S)	

4.2.2 Quality activities necessary in Qmuzik ERP environment

COBIT defines this IT process (control objective) as follows:

"A quality management system should be developed and maintained, which includes proven development and acquisition processes and standards. This is enabled by planning, implementing and maintaining the quality management system by providing clear quality requirements, procedures and policies. Quality requirements should be stated and communicated in quantifiable and achievable indicators. Continuous improvement is achieved by ongoing monitoring, analysing and acting upon deviations, and communicating results to stakeholders. Quality management is essential to ensure that IT is delivering value to the business, continuous improvement and transparency for stakeholders." (ITGI, 2005:59)

	QMUZIK (ERP)	CLIENT/ THIRD PARTY
RESPONSIBILITY / SUCCESS FACTORS	• Documented system development lifecycle methodology • Ensure system to perform to defined standards • Define standards for development and testing • System testing and documentation • Quality assurance reviews and reporting • Separation between development and testing responsibilities	• Define organisational structure for quality management • Define quality management system • Establish quality assurance responsibilities • Training and involvement of all users • Communicate quality standards and policies to all users • Measure, monitor and review quality standards
DOCUMENTS	• Quality management plan • System development plan • System test plan • Quality testing checklist	

	QMUZIK (ERP)	CLIENT/ THIRD PARTY
QMUZIK FUNCTIONS	• External Object Linking (S) • Document Management (S)	

4.2.3 Risk management in Qmuzik ERP environment

COBIT defines this IT process (control objective) as follows:

> "Create and maintain a risk management framework. The framework documents a common and agreed level of IT risks, mitigation strategies and agreed-upon residual risks. Any potential impact on the goals of the organisation caused by an unplanned event should be identified, analysed and assessed. Risk mitigation strategies should be adopted to minimise residual risk to an accepted level. The result of the assessment should be understandable to the stakeholders and expressed in financial terms, to enable stakeholders to align risk to an acceptable level of tolerance." (ITGI, 2005:63)

	QMUZIK (ERP)	CLIENT/ THIRD PARTY
RESPONSIBILITY / SUCCESS FACTORS	• Define optimal environment for Qmuzik to minimise risk	• Allocate risk management ownership and accountability • Obtain knowledge of different kinds of risks (technology, security, continuity, regulatory) • Identify potential risks applicable to ERP environment • Define and document risk policy • Define and document disaster and data recovery plan • Regular assessments and updates to documents

28

		QMUZIK (ERP)	CLIENT/ THIRD PARTY
DOCUMENTS		• Disaster recovery plan • Risk action plan • Risk log	
QMUZIK	**FUNCTIONS**	• Document Management (S) • Business Model Viewer (S) • External Object Linking (S) • Qmuzik Explorer (S)	

4.2.4 Management of Qmuzik ERP related projects

COBIT defines this IT process (control objective) as follows:

"Establish a programme and project management framework for the management of all IT projects. The framework should ensure the correct prioritisation and co-ordination of all projects. The framework should include a master plan, assignment of resources, definition of deliverables, approval by users, a phased approach to delivery, quality assurance, a formal test plan, and testing and post-implementation review after installation to ensure project risk management and value delivery to the business. This approach reduces the risk of unexpected costs and project cancellations, improves communications to and involvement of business and end users, ensures the value and quality of project deliverables, and maximises their contribution to IT-enabled investment programmes." (ITGI, 2005:67)

		QMUZIK (ERP)	CLIENT/ THIRD PARTY
RESPONSIBILITY /	**SUCCESS FACTORS**	• Assist with identification of Qmuzik related projects. • Assist with impact assessment on Qmuzik	• Identify, prioritise and manage IT projects

	QMUZIK (ERP)	CLIENT/ THIRD PARTY
DOCUMENTS	• Detailed project plan • Project risk management plan • Project performance report • Qmuzik online help and training	
QMUZIK FUNCTIONS	• Project Management Module (P)	

The impact of IT related projects on the ERP application could differ depending on the scope of the project. E.g. the project management process is critical when implementing a new ERP application, or when a third party application need to be integrated with the ERP application, but the impact is not as critical when upgrading desktops or printers. Therefore the factors listed above are not intended to be exhaustive and are therefore only listed on a high level.

ACQUIRE AND IMPLEMENT DOMAIN

4.2.5 Maintenance of Qmuzik application software

COBIT defines this IT process (control objective) as follows:

"Applications have to be made available in line with business requirements. This process covers the design of the applications, the proper inclusion of application controls and security requirements, and the actual development and configuration according to standards. This allows organisations to properly support business operations with the correct automated applications." (ITGI, 2005:83)

	QMUZIK (ERP)	CLIENT/ THIRD PARTY
RESPONSIBILITY / SUCCESS FACTORS	• Management of application software life-cycle • Translate business requirement into technical requirement specification for new application controls • Define and follow formalised application development procedure which contribute to internal control • Ensure application controls in place to validate data for completeness, accuracy, authentication and data integrity • Define software quality assurance plan • Separation of development, testing and operational activities • Assist/advise in upgrades/changes to existing system	• Manage acquisition and maintenance of application • Define clear functionality, operability, acceptability and sustainability requirements • Define detailed business requirement and acceptance criteria • User involvement and buy in (change management) • Allocate functional testing and acceptance responsibilities • Allocate and manage business process ownership

	QMUZIK (ERP)	**CLIENT/ THIRD PARTY**
DOCUMENTS	• Business processes / Blueprint • User requirement specification • Technical requirement specification • Application development procedure • System test plan • Software quality assurance plan • Gap analysis	
QMUZIK FUNCTIONS	• Business Model Viewer (P) • External Object Linking (P) • Qmuzik Explorer (P) • Document Management (P)	

4.2.6 ERP technology architecture support and maintenance

COBIT defines this IT process (control objective) as follows:

> "Organisations should have processes for the acquisition, implementation and upgrade of the technology infrastructure. This requires a planned approach to acquisition, maintenance and protection of infrastructure in line with agreed technology strategies and the provision of development and test environments. This ensures that there is ongoing technological support for business applications." (ITGI, 2005:81)

	QMUZIK (ERP)	CLIENT/ THIRD PARTY
RESPONSIBILITY / SUCCESS FACTORS	• Provide guideline for future technology architecture changes • Define adequate infrastructure requirements • Assess impact of changes in infrastructure on Qmuzik • Consult / advise on implementation of infrastructure changes	• Define upgrade, conversion and migration plans of infrastructure rollouts • Provide test environment infrastructure • Configure infrastructure components • Implement internal control, security and audit ability measures • Define maintenance plan for infrastructure • Ensure appropriate training, change management and knowledge transfer
DOCUMENTS	• Performance and capacity plan • Business requirements feasibility study • Technical infrastructure requirement specification • Technological infrastructure acquisition/maintenance plan	

The following are the technological architecture of Qmuzik and should be taken into consideration when changing/planning for infrastructure changes:

- **Qmuzik operating system:** The server operating system could be either Windows 2000/2003 server or Windows Advanced Server. Workstation operating systems could be Windows 2000 or Windows XP.

- **Qmuzik network technology:** Qmuzik may be deployed on a LAN (Local Area Network) or a WAN (Wide Area Network), depending on user requirements and the relevant geographical layout.

- **Qmuzik database platform**: The database platform is Microsoft SQL Server 2000 or 2005. Qmuzik architecture is based on a multi-tier deployment that includes the use of thin client terminals.

- **Qmuzik reporting interface**: All standard reports are presented using Microsoft Excel. Seagate Software Crystal reports are used for all business forms (invoices, delivery notes, credit notes, purchase orders, etc).

4.2.7 Enable operation and use of Qmuzik application

COBIT defines this IT process (control objective) as follows:

"Knowledge about new systems needs to be made available. This process requires the production of documentation and manuals for users and IT, and provides training to ensure proper use and operations of applications and infrastructure." (ITGI, 2005:85)

	QMUZIK (ERP)	CLIENT/ THIRD PARTY
RESPONSIBILITY / SUCCESS FACTORS	• Define application administration processes • Ensure standard help and training material available and up to date • Ensure training of all users during implementation project • Assist in integration of business processes with Qmuzik application • Assisting with business process re-design/blueprint • Implement standard framework for documentation and procedures • Advice on proper use and performance of the Qmuzik application	• Define and document user procedures and controls • Document standard operating procedures • Document business processes • Document user specific training/operation manuals • Review and maintenance of procedures • Ensure knowledge transfer to all stakeholders • Ensure proper use and performance of the Qmuzik application

		QMUZIK (ERP)	CLIENT/ THIRD PARTY
DOCUMENTS		• Qmuzik online help and training • Customer specific training /procedure manuals • Standard operating procedures (SOP) • Business processes / Blueprint	
QMUZIK	**FUNCTIONS**	• Business Model Viewer (P) • External Object Linking (P) • Qmuzik Explorer (P) • Document Management (P)	

4.2.8 Change management processes for Qmuzik

COBIT defines this IT process (control objective) as follows:

"All changes, including emergency maintenance and patches, relating to infrastructure and applications within the production environment must be formally managed in a controlled manner. Changes (including procedures, processes, system and service parameters) must be logged, assessed and authorised prior to implementation and reviewed against planned outcomes following implementation. This assures mitigation of the risks of negatively impacting the stability or integrity of the production environment." (ITGI, 2005:93)

	QMUZIK (ERP)	CLIENT/ THIRD PARTY
RESPONSIBILITY / SUCCESS FACTORS	• Impact assessment of change • Formal testing procedures • Documentation of test results • Release management policy • Software distribution policy • Configuration and audit trial management	• Define formal change management procedures • Authorisation of changes • Categorisation, prioritisation and authorisation of emergency procedures • Communication of procedures to user community • Updating of system and user documentation, procedures, manuals
DOCUMENTS	• System release notes • Change policy • Request for change template • System test plan • Exception reports • Standard functional reports	

	QMUZIK (ERP)	CLIENT/ THIRD PARTY
QMUZIK FUNCTIONS	• Request and Failures (P) • Transaction History (S)	

Qmuzik version control:

Qmuzik has different levels of version control for each object in the application. Version numbers are assigned to each object for a specific release. The Qmuzik application verifies with user login whether the correct versions are implemented on each user's terminal. If these versions are not correct, then the system will warn the user that a later version of the function is available and should be implemented as soon as possible. This means that when a change is made to the system this control will ensure that the change be implemented at all users, and not allow users to continue with work on an incorrect version of the application and cause possible further damage to the data.

Qmuzik advised change control procedures:

Qmuzik advises strict change control procedures to ensure that a complete history record of all changes are kept and are auditable. The following procedures are advised by Qmuzik to their clients: (Qmuzik system administration training manual)

• All changes should be formally requested with an internal request number.

• All requests have to be approved by the line manager/appropriate person.

• A simulation/training database should be available on which users could test and simulate data. This simulation database should reflect the live production data and production database backups to be restored on the simulation database every day/week/month, or as required.

• All new functionality, reports or data updates are to be first tested in a simulation environment and formally signed off by the client before being implemented on the live database.

- All data updates scripts should be saved electronically with a corresponding internal request number and any additional documentation (e.g. test results, reconciliation notes).
- All changes need to be done only by approved users with the appropriate technical skills and knowledge of the system.
- The system administrator password has to be protected and may only be given to authorised users.
- Strict backup policies should be implemented to ensure that previous backups can be successfully restored if changes were incorrectly applied.

4.2.9 Installation and accreditation of Qmuzik application

COBIT defines this IT process (control objective) as follows:

> "New systems need to be made operational once development is complete. This requires proper testing in a dedicated environment with relevant test data, definition of rollout and migration instructions, release planning and actual promotion to production, and a post-implementation review. This assures that operational systems are in line with the agreed expectations and outcomes." (ITGI, 2005:97)

	QMUZIK (ERP)	CLIENT/ THIRD PARTY
RESPONSIBILITY / SUCCESS FACTORS	• Clearly defined upgrade, conversion and migration plans with specific milestones and allocated responsibilities • Ensure project team resources and skills • Training of all business process owners • Provide test environment that simulates live environment • Ensure installation of approved and accredited components trouble-free • Define test plan according to technical and user specification • Implementation reviews and feedback	• Manage installation and accreditation of application • Pre-implementation analysis and impact assessment • Ensure that adequate resources are available • Business process ownership and involvement • Business continuity requirements • Continuous quality improvement plans • Define test plan according to user specification • Documentation of test results • Implementation reviews and feedback

		QMUZIK (ERP)	CLIENT/ THIRD PARTY
DOCUMENTS		• Implementation project plan • Migration plan • User requirement specification • System test plan • Technical requirement specification • Development standards checklist • Project acceptance certificate	
QMUZIK	**FUNCTIONS**	• Migration tools e.g. Transfer Manager (P)	

DELIVER AND SUPPORT DOMAIN

4.2.10 Manage service levels for Qmuzik environment

COBIT defines this IT process (control objective) as follows:

"Effective communication between IT management and business customers regarding services required is enabled by a documented definition and agreement of IT services and service levels. This process also includes monitoring and timely reporting to stakeholders on the accomplishment of service levels. This process enables alignment between IT services and the related business requirements." (ITGI, 2005:103)

	QMUZIK (ERP)	CLIENT/ THIRD PARTY
RESPONSIBILITY / SUCCESS FACTORS	• Define optimal service environment for application	• Define service requirements and performance measures • Establish formal service level agreements • Definition of service • Non disclosure agreements • Define monitoring and reporting requirements • Review of service level agreement and contracts
DOCUMENTS	• Non disclosure agreement • Service level agreement (SLA) • Operating level agreement (OLA)	
QMUZIK FUNCTIONS	• Service Requisition (P) • Contract Management (P) • Project Management (P)	

4.2.11 Contracting and measuring Qmuzik service providers and consultants

COBIT defines this IT process (control objective) as follows:

"The need to assure that services provided by third parties meet business requirements requires an effective third-party management process. This process is accomplished by clearly defining the roles, responsibilities and expectations in third-party agreements as well as reviewing and monitoring such agreements for effectiveness and compliance. Effective management of third-party services minimises business risk associated with non-performing suppliers." (ITGI, 2005:107)

	QMUZIK (ERP)	CLIENT/ THIRD PARTY
RESPONSIBILITY / SUCCESS FACTORS	• Ensure that service level is according to SLA • Internal performance review against SLA • Service level improvement plan • Client relationship management	• Define service requirements and performance measures • Contract management • Supplier relationship management • Supplier risk management • Ensure adequate facilities and infrastructure available for third party services • Monitor and measure suppliers performance against SLA • Cost/Benefit analysis
DOCUMENTS	• Non disclosure agreement • Service level agreement (SLA) • Performance measurements	
QMUZIK FUNCTIONS	• Contract Management (P) • Service Requisition (P) • Requisition Cash flow schedule (S) • Project Management module (P)	

4.2.12 Qmuzik performance and capacity management

COBIT defines this IT process (control objective) as follows:

"The need to manage performance and capacity of IT resources requires a process to periodically review current performance and capacity of IT resources. This process includes forecasting future needs based on workload, storage and contingency requirements. This process provides assurance that information resources supporting business requirements are continually available." (ITGI, 2005:114)

		QMUZIK (ERP)	CLIENT/ THIRD PARTY
RESPONSIBILITY / SUCCESS FACTORS		• Regular review of Qmuzik performance and capacity • Ensure Qmuzik resource availability • Define adequate infrastructure for optimal performance	• Regular review of infrastructure performance with impact on Qmuzik performance • Monitor hardware and software price/performance changes • Regular review of Qmuzik and resource performance and capacity • Contingency and forecasting plan for optimising performance • Ensure optimal allocation of resources and facilities • Monitoring and reporting of performance
DOCUMENTS		• Performance and capacity plan • IT resource schedule • Contingency plan	

4.2.13 Ensure continuous Qmuzik services

COBIT defines this IT process (control objective) as follows:

"The need for providing continuous IT services requires developing, maintaining and testing IT continuity plans, offsite backup storage and periodic continuity plan training. An effective continuous service process minimises the probability and impact of a major IT service interruption on key business functions and processes." (ITGI, 2005:115)

	QMUZIK (ERP)	CLIENT/ THIRD PARTY
RESPONSIBILITY / SUCCESS FACTORS	• Provide inputs for appropriate backup and recovery plans • Define escalation/incident procedure • Ensure resource availability	• Identify critical IT resource components • Service monitoring • Define business continuity plans • Maintenance and testing of contingency and continuity plan • Back up, recovery and redundancy practices in place • Establish alternative procedures • Offsite backup storage • Training and knowledge transfer to users
DOCUMENTS	• Business continuity plan • Contingency plan • ESCROW Agreement	

4.2.14 Ensuring Qmuzik application security

COBIT defines this IT process (control objective) as follows:

"The need to maintain the integrity of information and protect IT assets requires a security management process. This process includes establishing and maintaining IT security roles and responsibilities, policies, standards and procedures. Security management also includes performing security monitoring and periodic testing and implementing corrective actions for identified security weaknesses or incidents. Effective security management protects all IT assets to minimise the business impact of security vulnerabilities and incidents." (ITGI, 2005:119)

	QMUZIK (ERP)	CLIENT/ THIRD PARTY
RESPONSIBILITY / SUCCESS FACTORS	• Confidentiality and privacy requirements • User training on security aspects • Tools for monitoring compliance, intrusion testing and reporting • User identification and authorisation profiles • Ensure user password encryption and security	• Configure and manage authorisation, authentication and access controls • Create culture of awareness of security • Incident handling, reporting and follow up • Centralised security and Qmuzik user account management • Periodic review of user profiles and rights
DOCUMENTS	• Security policy • Security application form	

	QMUZIK (ERP)	CLIENT/ THIRD PARTY
QMUZIK FUNCTIONS	• Security Profiles (P) • Profile Access Search (P) • Physical Security Module (P) • Transaction History (S)	

Qmuzik access control:

All users captured as employees in Qmuzik need to be allocated to certain profiles or security groups. These profiles allow or disallow rights to enquire, add, change or delete specific Qmuzik functions. Access to functions could be maintained by front-ends exposing these users, profiles and functions. A search function is available to reduce set-up and maintenance requirements of these profiles. Employee passwords are encrypted and could be configured to expire every 30 days, or as required.

External application interfaces:

Qmuzik's back end is exposed and all business objects can be invoked by external event engines or communication signals, e.g. the Internet. This means that Qmuzik is not restricted to the presentation layer (front end) and, therefore, custom presentation applications could be used for capturing and/or inquiring of data e.g. MS Excel.

These back-end objects (Intelligent Business Objects), methods and properties allow for integration between Qmuzik and other third-party products/applications to occur, without compromising the performance and data integrity of the Qmuzik database. Appropriate controls should however be implemented to ensure that interfaces with third-party products are secure and that access controls are in place. If data updates are done to the system via external applications, these should use the systems back-end objects to ensure that data are verified with the same security and integrity checks as when processed by Qmuzik's front end.

4.2.15 Education and training of Qmuzik users

COBIT defines this IT process (control objective) as follows:

"Effective education of all users of IT systems, including those within IT, requires identifying the training needs of each user group. In addition to identifying needs, this process includes defining and executing a strategy for effective training and measuring the results. An effective training program increases effective use of technology by reducing user errors, increasing productivity and increasing compliance with key controls such as user security measures." (ITGI, 2005:127)

	QMUZIK (ERP)	CLIENT/ THIRD PARTY
RESPONSIBILITY / SUCCESS FACTORS	• Provide standard training curriculum • Use of current training technologies and methods • Training of users in similar environments • Training certification • Training accreditation	• Training awareness campaigns • Senior management support • Actively manage training and education program • Corporate policy to require all users to receive basic training • Evaluation and feedback of training received
DOCUMENTS	• Qmuzik online help and training • Training policy • Training certificates	
QMUZIK FUNCTIONS	• Qmuzik Standard Help (P) • Qmuzik Standard Training courses (P)	

4.2.16 Service desk assistance/advise to Qmuzik users

COBIT defines this IT process (control objective) as follows:

> "Timely and effective response to IT user queries and problems requires a well-designed and well-executed service desk and incident management process. This process includes setting up a service desk function with registration, incident escalation, trend and root cause analysis, and resolution. The business benefits include increased productivity through quick resolution of user queries. In addition, the business can address root causes (such as poor user training) through effective reporting." (ITGI, 2005:131)

	QMUZIK (ERP)	CLIENT/ THIRD PARTY
RESPONSIBILITY / SUCCESS FACTORS	• User query and problem response • Ensure Qmuzik support line availability • Trend analysis • Development of knowledge base (FAQ's) • Root cause analysis • Problem tracking and escalation • Provide management monitors	• Ensure helpdesk in place • Ensure service agreement in place • Communicate formal request procedure for assistance and problem solving
DOCUMENTS	• Qmuzik online help and training • Service desk call logging procedure • Service level agreement (SLA)	
QMUZIK FUNCTIONS	• Customised Help and training (P) • Request and Failure (P) • Request and Failure Analysis (P)	

4.2.17 Manage the Qmuzik configuration

COBIT defines this IT process (control objective) as follows:

"Ensuring the integrity of hardware and software configurations requires establishment and maintenance of an accurate and complete configuration repository. This process includes collecting initial configuration information, establishing baselines, verifying and auditing configuration information, and updating the configuration repository as needed. Effective configuration management facilitates greater system availability, minimises production issues and resolves issues faster." (ITGI, 2005:135)

	QMUZIK (ERP)	CLIENT/ THIRD PARTY
RESPONSIBILITY / SUCCESS FACTORS	• Provide guidelines for optimal application and infrastructure configuration • Release management policy in place • Automated distribution and upgrade process in place	• Establish configuration baselines • Identification of configuration items • Configuration change management • Review and maintain configuration integrity
DOCUMENTS	• User, operational, technical, administration and support manuals • License documents	
QMUZIK FUNCTIONS	• System Configuration (P) • System Administration Training Manual (S)	

4.2.18 Problem management in Qmuzik environment

COBIT defines this IT process (control objective) as follows:

"Effective problem management requires the identification and classification of problems, root cause analysis and resolution of problems. The problem management process also includes identification of recommendations for improvement, maintenance of problem records and review of the status of corrective actions. An effective problem management process improves service levels, reduces costs and improves customer convenience and satisfaction." (ITGI, 2005:139)

	QMUZIK (ERP)	CLIENT/ THIRD PARTY
RESPONSIBILITY / SUCCESS FACTORS	• Assist/ advise in Qmuzik related problems • Qmuzik support line to be available • Feedback and progress status to be communicated • Timely resolution of Qmuzik related problems	• Identify and classify problems • Root cause analysis and resolution • Define supplier responsibilities • Coordination with change and configuration management • Maintain record of problems
DOCUMENTS	• Error and request logs • Incident report • Process performance report	
QMUZIK FUNCTIONS	• Request and Failures (P) • Qmuzik online help and training (S)	

4.2.19 Manage data in Qmuzik environment

COBIT defines this IT process (control objective) as follows:

> "Effective data management requires identifying data requirements. The data management process also includes establishing effective procedures to manage the media library, backup and recovery of data, and proper disposal of media. Effective data management helps ensure the quality, timeliness and availability of business data." (ITGI, 2005:143)

	QMUZIK (ERP)	CLIENT/ THIRD PARTY
RESPONSIBILITY / SUCCESS FACTORS	• Advise on backup interval and recovery configuration in Qmuzik application	• Define and allocate data ownership • Data input, processing and output integrity standards are formalised and enforced • Data storage and retention procedures in place • Manage onsite and offsite storage of data • Testing of restoration on regular basis • Ensure IT compliance with laws and regulations
DOCUMENTS	• Backup storage and retention plan • Operating level agreements (OLA) • Disaster recovery plan	

	QMUZIK (ERP)	CLIENT/ THIRD PARTY
QMUZIK FUNCTIONS	• System configuration (P) • Qmuzik online help and training (S)	

Qmuzik database administration:

The database backup interval and recovery settings are specified in a system configuration function in Qmuzik. Transaction logging is also backed up, and this interval could be specified in a frequency of minutes. The retention period for each backup and transaction logging is also specified. The default configuration is that a full backup is taken every weekday and the default for transaction logging is every hour, but the interval and frequency could be altered according to individual requirements. The system configuration settings may only be accessed by a user with specific access profiles, e.g. database administrator.

This IT process (control objective) has been rated with a critical factor of high in the assessment matrix; due to the fact that Qmuzik is a real-time integrated application with workflow capability and it is crucial that the recoverability of the database is well configured and tested, as it can lead to loss of data if not. With the setup as detailed above it implies that the database could be recovered to the last 60 minutes before failure.

MONITOR AND EVALUATE DOMAIN

4.2.20 Monitor and evaluate the ERP support processes

COBIT defines this IT process (control objective) as follows:

"Effective IT performance management requires a monitoring process. This process includes defining relevant performance indicators, a systematic and timely reporting of performance, and prompt acting upon deviations. Monitoring is needed to make sure that the right things are done and are in line with the set directions and policies." (ITGI, 2005:155)

	QMUZIK (ERP)	CLIENT/ THIRD PARTY
RESPONSIBILITY / SUCCESS FACTORS	• Provide tools for management reporting on process performance • Assess performance • Identify improvement actions	• Establish and define monitoring approach • Define measurable objectives • Performance assessments • Benchmarking and scorecards • Report performance • Knowledge base of historical performance • Identify and initiate remedial action • Identify improvement actions
DOCUMENTS	• Support performance feedback reports • User satisfaction assessments • Customer satisfaction assessments • Cost vs. benefit report • Remedial/improvement action plans	
QMUZIK FUNCTIONS	• Request and Failure Analysis (S) • Executive Information System (P)	

4.2.21 Maintain and evaluate internal control in Qmuzik environment

COBIT defines this IT process (control objective) as follows:

 "Establishing an effective internal control programme for IT requires a well-defined monitoring process. This process includes the monitoring and reporting of control exceptions, results of self-assessments and third-party reviews. A key benefit of internal control monitoring is to provide assurance regarding effective and efficient operations and compliance with applicable laws and regulations." (ITGI, 2005:159)

		QMUZIK (ERP)	CLIENT/ THIRD PARTY
RESPONSIBILITY / SUCCESS FACTORS		• Provide error and exception reports • Provide management reporting • Ensure compliance with legal and regulatory requirements • Provide assurance of adequate Qmuzik internal control through third-party reviews	• Monitoring internal control framework • Allocate responsibilities for internal control review and supervisory • Perform control self assessments • Record and assess control exceptions • Obtain independent assurance • Continuous review of Qmuzik application controls with impact in internal control (e.g. review segregation of duties and authority matrices) • Identify and initiate remedial actions
DOCUMENTS		• Process performance reports • Business processes / Blueprint	

|		QMUZIK (ERP)	CLIENT/ THIRD PARTY
QMUZIK FUNCTIONS		• Employee Profile (S) • Profile Access Search (S) • Electronic Funds Transfer Authorisation Matrix (P) • Requisition Authorisation Matrix (P) • Bank transaction access (P) • Store employee access (P)	

4.2.22 Regulatory compliance requirements that impacts Qmuzik

COBIT defines this IT process (control objective) as follows:

"Effective regulatory oversight requires the establishment of an independent review process to ensure compliance with laws and regulations. This process includes defining an audit charter, auditor independence, professional ethics and standards, planning, performance of audit work, and reporting and follow-up of audit activities. The purpose of this process is to provide positive assurance related to IT compliance with laws and regulations." (ITGI, 2005:163)

	QMUZIK (ERP)	CLIENT/ THIRD PARTY
RESPONSIBILITY / SUCCESS FACTORS	• Qmuzik need to keep track of external legal and regulatory requirements that impact functionality • Ensure updating of functionality with local laws, regulations and contracts in order to be compliant • Evaluate compliance on regular basis	• Identification of laws and regulations with potential impact on Qmuzik • Evaluate compliance • Define and implement procedures for positive compliance assurance • Training of users to ensure correct use of Qmuzik functionality • Regular review of Qmuzik controls to be configured for optimum level of enforcement and required control

	QMUZIK (ERP)	CLIENT/ THIRD PARTY
DOCUMENTS	• Legal and regulatory compliance acts • Compliance assessment reports	
QMUZIK FUNCTIONS	• Asset Depreciation Model (P) • Contract Management (P) • Division – Business rules (P) • External Organisation Groups (P) • Levy and Surcharge types (P) • Product Master (P) • Tax codes (P) • Store – Costing setup (P)	
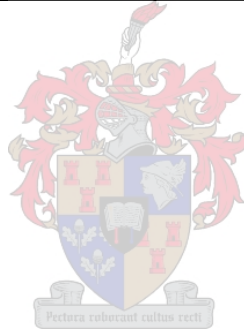
5 CONCLUDING SUMMARY
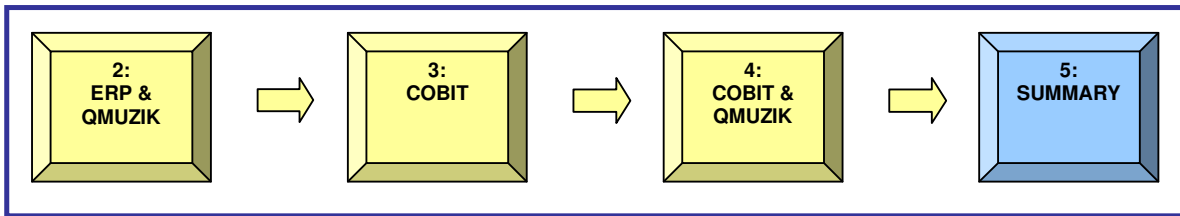
With the exponential growth of the global information era, information and the supporting technology evolved into some of an organisation's most valuable assets and could even constitute part of its intellectual property.

ERP applications have evolved into enterprise-wide applications that are classified as a critical component in an organisation's information strategy.

It should, therefore, be essential to focus on mitigating IT process risks that have an impact on the ERP environment, so that the level of residual risk is acceptable and aligned with the business objectives.

The approach used in this assignment was to use a professional control framework (COBIT) and to map the criticality of each IT process from an ERP environment perspective. Specific reference was also made to Qmuzik as ERP application. This was done referring to:

   o 4.1 IT process assessment matrix - each IT process was rated according to the impact it has on Qmuzik as ERP application.

   o 4.2 Responsibility and action details – the responsibility for critical activities that need to be considered by the Qmuzik supplier and/or client was allocated in this matrix. Supporting documentation and specific Qmuzik functionality were also noted.

Applying COBIT in an ERP environment could ensure that all elements of IT risk are visible and defined and that the minimum process controls may be designed

and implemented effectively. COBIT can thus help build capabilities in delivering reliable, efficient IT services for an ERP environment.

With the increased focus for companies on IT governance and compliance with the Sarbanes-Oxley Act, it is only relevant that COBIT be implemented, as COBIT is designed to be an IT governance tool that helps to proactively manage these subject matters.

To conclude, COBIT provides a control framework which is understandable to user, manager and auditor communities alike. COBIT is the IT governance tool that helps in understanding and managing the risks and benefits associated with IT and could also be successfully applied in an ERP environment, and specifically with reference to Qmuzik as ERP application.

6 REFERENCES

ABERDEEN GROUP. 2004. *The ABCs of ERP: An Executive Primer*. [Online:] http://www.aberdeen.com [Accessed: 14 April 2005].

ARMSTRONG, R. 2006. *PATRIOT: Compliance is now everyone's concern*. Info-Tech Research Group. [Online:] http://www2.cio.com/analyst/report4073.html [Accessed: 6 October 2006].

CEVERA, L.R. 2005. *Create your methodology base on a standard framework – part one.* [Online:] http://www.ezinearticles.com/ [Accessed: 6 October 2006].

HONG, K. & KIM, Y. 2002. The critical success factors for ERP implementation: An organizational fit perspective. *Information and Management,* 40 (1): 25-40. [Online:] http://www.sciencedirect.com/ [Accessed: 15 June 2005].

IIA (Institute of Internal Auditors). 2002. *CSA Utilization: Selecting a framework for control.* [Online:] http://www.theiia.org/ecm [Accessed: 15 June 2005].

ISACA (Information Systems Audit and Control Association). 2003. *IS Auditing Guideline - Enterprise Resource Planning (ERP) systems review*, Document 060.010.0, 10 p.

ITGI (IT Governance Institute). 2005. *COBIT 4.0.* Fourth edition. [Online:] http://www.isaca.org/ [Accessed: 18 October 2006].

KIEVIET, F. (Freda.Kieviet@Qmuzik.com). 2005. Discussion of critical IT processes in ERP environment. [Discussion group:] Qmuzik.Support@Qmuzik.com. Sept.15.

REFERENCES

MOTWANI, J., MIRCHANDANI, D., MADAN, M. & GUNASEKARAN, A. 2002. Successful implementation of ERP projects: Evidence from two case studies. *International Journal of Production Economics,* 75: 83-96. [Online:] http://www.elsevier.com/ [Accessed: 10 October 2005].

QMUZIK. 2005. Qmuzik White Paper - Executive Summary. 14 p.

QMUZIK. 2005. Online Help and Training Manuals. [Online:] http://www.qmuzik.com/help/ [Accessed: 6 October 2006].

RASMUSSEN, M. 2006. 7 Steps to a highly effective IT compliance program. *IT AUDIT,* 9, Sept. 10. [Online:] http://www.theiia.org/ITAudit [Accessed: 6 October 2006].

SIMMONS, M.R. 2002. *COSO – The framework for internal control: A strategic approach to internal audits.* [Online:] http://www.facilitatedcontrols.com/internal-auditing/cosobsic.htm [Accessed: 30 October 2006].

TECHNOLOGY EVALUATION CENTRE. 2005. *ERP: Origins, Developments and trends.* [Online:] http://www.technologyevaluation.com/research/center/ERP/index.asp [Accessed: 17 May 2005].

STOLOVITSKY, N. 2005. *IT Governance: Maximizing the Business Investment.* Technology Evaluation Project Management Research Centre. [Online:] http://www.technologyevaluation.com/research/center/ERP/index.asp [Accessed: 10 September 2005].

UMBLE, E.J., HAFT, R.R. & UMBLE, M.M. 2003. Enterprise Resource Planning: Implementation procedures and critical success factors. *European Journal of Operational Research*, 146(2): 241-257, Apr.16. [Online:] http://www.sciencedirect.com/ [Accessed: 10 October 2005].

REFERENCES

WISE, L. 2006. *Using Business-Intelligence Infrastructure to ensure compliance with the Sarbanes-Oxley Act.* Technology Evaluation Business Intelligence Research Centre. [Online:] http://www.technologyevaluation.com/research/ResearchHighlights/BusinessIntelligence.asp [Accessed: 6 April 2006].

YAN, R. & MAKAL, M. 1999. Audit and Control: Two views of internal controls: COBIT and the ITCG. *IS Audit and Control Journal ISACA,* 1.

7 GLOSSARY OF TERMS

| Term	Description
COBIT	Control Objectives for Information and related Technology
COCO	Criteria of Control
COSO	Committee of Sponsoring Organisations
ERP	Enterprise Resource Planning
IFRS	International Financial Reporting Standards
IS	Information System
ISACA	Information Systems Audit and Control Association
IT	Information Technology
ITCG	Information Technology Control Guidelines
ITIL	IT Infrastructure Library
ITGI	IT Governance Institute
OLA	Operating level agreement
RACI	Responsible, Accountable, Consulted and/or Informed
SLA	Service level agreement
SOP	Standard operating procedures
SOX	Sarbanes Oxley Act
SQL	Sequential Query Language

8   APPENDIX A - QMUZIK REFERENCED FUNCTIONALITY

This section is compiled using Qmuzik online help and training manuals (Qmuzik, 2005)

Account Budget Actuals: This function is used to view, create and maintain budgets for selected cost centres and divisions. Budgets are entered and maintained per account per financial period within a selected financial year. The actual costs (account balance) are updated in real-time.   A detailed drilldown to journal level is provided for.

Analysis Reporting Functions: These are reporting functions where an analysis of the specific data can be extracted according to specific user criteria. A report can be created from the result set with user-definable columns. Various functions exist such as:

- Asset Analysis
- Creditors Analysis
- Debtors Analysis
- Document Analysis
- Maintenance Analysis
- Movement History
- Node Analysis
- Purchasing Analysis
- Sales Analysis
- Works order Analysis
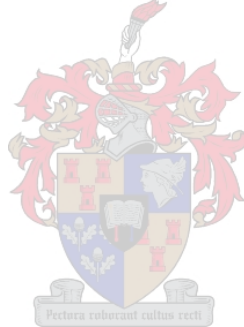
Asset Depreciation Model: This function is used to create and maintain specific asset depreciation methods. These methods can be prescribed according to legal and regulatory requirements and should be configured accordingly. E.g. straight line method, reducing balance method, accelerated depreciation etc.

Business Model Viewer: This function allows all business processes to be defined in a user-friendly graphical display. The business process can be defined in using more than one level with intuitive drilldown to lower level processes. Detail information regarding process, function, training or user can be linked to each entity created. User profiles are fully integrated with the business-modelling tool, which enables easy identification of training required once a change in one of the business processes occurs. This function allows all users to easily navigate through current business processes and the primary aim of this function is knowledge management.

Contract Management: This function is to capture contract related data such as licenses, permit, and other regulatory requirements. The purpose of this function is to manage contracts and have a centralised view of all customer orders, projects, requirements etc related to a specific contract.

Document Management: This function is available to register and control all documents in a company for which a master record are required for the purposes of identification, change control and distribution.

Executive Information System: This function provides easy access to core business data. It allows information to be analysed, providing a method of viewing the big picture while allowing detailed analysis through a flexible drill down structure. It displays the data in the form of charts and grids, therefore utilising both graphical and textual methods of analysing the data. It also provides the ability to create and save personal views over the extracted data.

Explorer: This is a central navigating function from which a company can view/maintain all company business processes, company reports, implementation business processes, Qmuzik standard reports and Qmuzik functions in a file structure that is customisable according to each business (client)

External Object Linking: This function is used to define external objects and to link these objects within the Qmuzik application to a system object e.g. A training manual

can be linked to a Qmuzik business process or a service level agreement can be linked to a supplier number. External objects are electronic files created in an application other than the application i.e. (Microsoft Word files, Bitmap files, Microsoft Excel files, AUTOCAD drawings etc).

External Organisation Groups: This function allows multiple groups to be created and a supplier or customer organisation to be linked to multiple groups. This allows reporting to be extracted according to these specific groups e.g. All sales per customer per region, or all organisations that are identified as related parties for IFRS purposes.

General Ledger Reports: Financial reports such as: Income statement, Balance sheet, General Ledger Detail, VAT report, Trial Balance, Cost Centre management report can be extracted from this function.

Profile Access Search: This is a search function with options to search per security profiles, employees, function and customised function names. Different modes can be selected to view e.g. profiles per employee or all employees for specific profile

Product Master: A product code is used to group parts together that belong to the same product range or group. This grouping does not only serve the purpose to do reporting at product level, but to specify business rules applicable to all items in the group. These business rules apply to the level of engineering change control, sales and profit margin control, stock application rules, trade discount matrixes and authorisation to override sales prices and profit margins. In addition, it identifies responsibility for the product relating to configuration management, trade discounts and product scheduling and allows you to retrieve information by product concerning inventory analysis, budgeting, sales etc.

Project Management: Nodes form the basis for the project management system through which a project can be defined and broken down into program nodes, milestone nodes or activity nodes. A node is also the vehicle to delegate authority,

within cost and time constraints, to perform the tasks needed to complete a project. It provides the manager of the program node with the necessary options to control the budget for the project to the extent it is deemed necessary.

Request and Failures: The purpose of this function is to formally register requests and failures relating to any user-defined request group or category. Any requirement to formally report required actions, investigations, complaints or failures of any nature can be registered via this function. The function allows for a formal approval cycle of requests and prompts users with internal mail when approval, releasing, implementation, user-testing or other actions are required. The beneficiary is also kept up to date as the approval status progresses or when requests are rejected.

Requisitions: Requisitions are the vehicle through which expenses against accounts or projects are initiated. Detail workflow and authorisation matrixes exist to ensure effective segregation of duties.

Requisition Cash flow Schedule: The function provides for the scheduling of service requisition anticipated expenditure, with the option to perform self-billing once the amounts have been confirmed.
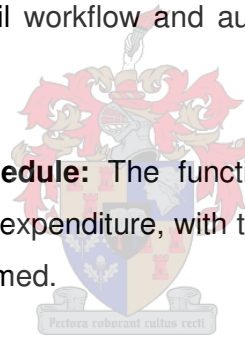
Security Profiles: This function is used to define security profiles in a company that can be applied to groups of employees for the purpose of system access control.

Service Requisition: Requisitions are the vehicle through which expenses against accounts or projects are initiated. A Service requisition is a type of requisition and is used for obtaining services such as consultation, rent, electricity, car rental, etc

Tax codes: This function allows tax codes and effective percentages to be created and maintained to comply with legal and regulatory requirements.

Transaction History: This function is used to inquire on the history of transactions that were performed on the system. Transactions that successfully resulted in data

being added, changed or deleted in the system tables are logged in the Transaction History table and as such provide a detailed audit trail of all transactions performed by system users. This function allows comparison of 'before' and 'after' images of data per transaction.

Transfer Manager: The Transfer Manager function provides a powerful tool to integrate with third party software. This function allows users to insert, delete and update data in the tables or to transfer data between different types of source and destination files. The function is intended for use by advanced users only. This function can be used during implementation to migrate data, to perform mass updates or to create regular data exports or imports.