Analysis of ICT Governance Initiatives as a Mechanism to Enhance Corporate Governance, with particular reference to Nelson Mandela Bay Municipality.

Prof. Chris Adendorff
Nelson Mandela Metropolitan University
South Africa

Dr. Brink Botha
Nelson Mandela Metropolitan University
South Africa

Sindiswa Tolom
Nelson Mandela Metropolitan University
South Africa

Dr. Gillian Adendorff
Nelson Mandela Metropolitan University
South Africa.

Abstract

Developing countries such as South Africa have tremendous potential for rapid and sustainable economic and social development by leveraging the benefits and advantages of Information and Communication Technology (ICT) and applying it appropriately within the local government sector. In this study, an analysis was made of ICT governance initiatives, as a mechanism to enhance corporate governance, with particular reference to the Nelson Mandela Bay Municipality (NMBM) in the Eastern Cape. While the governance developments have primarily been driven by the need for transparency regarding enterprise risks and the protection of shareholder value, the pervasive use of technology has created a critical dependency on ICT that calls for a specific focus on ICT governance. ICT governance is part of corporate governance, which is the responsibility of the organisation's top executive, to ensure that its information technology supports the goals and objectives of the organisation, through a variety of structural mechanisms, processes and mechanisms for communication. The corporate governance of ICT involves evaluating and directing the plans for the use of ICT to support the Institution and monitoring these. It includes the strategy and policies for using ICT within the institution. These executive authority and executive management are accountable and responsible for ensuring that the governance of ICT is implemented in the institution in line with this framework.

Keywords: corporate governance; development; Information and Communication Technology.
INTRODUCTION

Information and Communication Technology (ICT), such as computer systems and mobile phones, has emerged as a fundamental business asset that promotes and support social development initiatives by government, businesses and international organizations (Flowerday, Blundell, and Von Solms 2006:212). Information is increasingly regarded as the most valuable asset of organisations and the major driver of business success and efficiency. The continuous introduction of new technologies and constant customer demand for real-time information make software and technologies obsolete before delivery (Lee, 2001; Mapp, 2004). This highlights the need for close interaction between the business units in an organisation for Information and Communication Technology alignment, to ensure the achievement of the organisation’s vision and goals.

In an attempt to regulate the quality of corporate governance within organisations, various legal bills and national codes have been published, of which the Sarbanes-Oxley Act in the USA, the Cadbury, Greenbury and Hampel Reports in the UK, the Bosch Report in Australia, the King Reports in South Africa, and the Dey Report in Canada serve as examples (Bota-Avram, 2011:7). According to The South African Local Government Agency (2012:6), the current literature on Information and Communication Technology and planning suggests that the use of Information Technology in local government can enhance the management and functioning of cities. As a result, this study will focus on Information and Communication Technology governance as a mechanism to enhance corporate governance. Information Communication Technology Governance (ICTG) therefore becomes the most fundamental and crucial part of business management as a strategic tool for corporate governance and financial control. Von Solms, in Viljoen (2008:412), defines IT Governance as an integral part of Corporate Governance. Mirela and Maria (2010:1358) state that risk assessment and risk management should be key focus area, if information security management systems (ISMs) are defined as the process of identifying vulnerabilities and threats within the framework of an organization, as well as producing some measurements to minimise their impact over the information resources.

Although Guo, Yuan, Archer and Connely (2011: 204) refer to the misuse of information system by some end-users as non-malicious security violation, the Nelson Mandela Bay Municipality is required to assess its Information and Communication Technology system and develop control measures as part of IT governance. This means that everyone in the Municipality should understand the link between business and ICT strategic goals and accept their responsibilities with respect to the supply of and demand for ICT. Significant ICT expenditure should be informed by the Municipality’s Service Delivery Plan, and ICT architecture, motivated by business cases, must be monitored and evaluated. This study was intended to establish how the NMBM could maximise value from its information technology investments through the implementation of ICT governance initiatives that aim to align ICT strategies and investments with corporate business goals and strategies.

PROBLEM STATEMENT

Information technology governance underpins institutional operations to such an extent that its violation could cause significant financial loss or a consequential legal risk to the Nelson Mandela Bay Municipality. In its NMBM 2009/2010 and 2010/2011 financial year report the Auditor General has identified financial mismanagement in South African municipalities. This financial mismanagement has led to a shortage of funds, which has resulted in poor service delivery by the Municipality to its residents, culminating in service delivery protests, often accompanied by the burning of tyres and blocking of roads.

Subsequently, the Internal Audit and Risk Assurance Division of the NMBM adopted the System Control Assessment Review (SCAR) approach to evaluate the achievement of control objectives. This approach follows the processes and internal controls that were put in place for their adequacy and tested for effectiveness (through sample selection) to ensure that the identified issues were being addressed. However, the following problems and short comings were identified by the Auditor General.

- Lack of controlled risk management plans;
- Lack of trained ICT personnel to assist the Municipality in complying with current ICT standards; and
- Lack of adequate systems to ensure information security management.

It is clear that the NMBM’s ICT personnel are competent in end-user support services, without due consideration of high information security standards, as determined by ISO 17799 and SANS 17799-2:2003 (Backhouse and Dhillon, 2000:125). It is believed that the Municipality’s ICT does not follow any international standards on ICT, let alone following information system security standards, as the foundation of ICT governance. Furthermore, although the Municipality adopted its Information Security Management Policy on 14 February 2008, neither been implemented nor communicated to municipal staff. The ICT personnel in the Municipality have no knowledge of such Policy, nor does it constitute part of ICT governance. The main goal of the policy was to protect data by defining procedures; guidelines and practices for configuring and managing information security in the corporate environment (NMBM, 2008:5).

According to Cazemier, in Choobineh, Dhillon, Grimaila and Rees (2007:959), information security management is the process of administering people, policies and programmes with the objective of assuming continuity of operations, while maintaining a strategic alignment with the organisational mission. Most breaches to information system security are made by internal personnel and can be attributed to unauthorised system access or simply due to ignorance which, according to Guo, Yuan, Archer and Connely (2011:206), is a non-malicious security violation. Choobineh, Dhillon, Grimaila and Rees (2007:960) identify a cyclic, five phase process to conceptualise the information security management
process, namely Inspection; Protection; Detection; Reaction and Reflection.

Neglecting any one of the five phases could expose the organisation to excessive losses when it inevitably experiences an information incident. This means that the success of any organization depends on its information. If information is incomplete or missing, inaccurate or land in unauthorised hands, major damage may be caused to the company (Michelberger and Labodi, 2009:70). The successful implementation of ICT governance will ensure that vulnerabilities are identified and addressed, in the interest of protecting the NMBM’s business continuity and strengthening the information technology infrastructure. This will invariably maximise the return on the considerable investment required to gather, maintain and process information and ensure a considerable increase in revenue in order to fulfill the organisation’s service delivery mandate. The primary objective of this paper was to investigate and propose ICT governance initiatives as a mechanism to enhance corporate governance within the Nelson Mandela Bay Municipality (NMBM).

HYPOTHEISED MODEL

In order to investigate ICT governance initiatives for the explicit purpose of corporate governance, a number of factors that determine and are related to ICT governance are necessary. These factors were directly extrapolated from the questions found in the ensuing questionnaire of this study. Figure 1 below illustrates the proposed model or framework of testing relationships between primary and secondary factors that determine ICT governance initiatives and, by extension, the relationship between ICT governance initiatives wholly and corporate governance in the NMBM.
INFORMATION COMMUNICATION TECHNOLOGY (ICT) GOVERNANCE

Information communication technology has been the central force behind the progress of developed societies; however, their ICT use and development are seen as a natural evolution in the course of history as these countries have led the transition from the industrial to the information and knowledge age. Developed nations were quick to recognise the economic and social advantages and potential of ICT and it soon underpinned their national development policies in their quest for an advanced position for their local industries in the global market (European Commission, DG-INFSO. 2009).

The DANIDA study conducted in April 2012 and aimed at examining strategic opportunities for using ICT for promoting governance and democratisation efforts with the development assistance of the Danish, highlighted a string of shifts as an approach to ICT for development and governance. The shifts, according to the study, can be summarised in the form of two waves:

- A shift from emphasis on infrastructure and hardware to a new focus on the fostering of learning and innovation networks; and

Developing countries are significantly increasing spending on information...
technology, releasing relevant legislation and laws, and promoting ICT usage and services among different government agencies, in an endeavour to not be left behind in the global struggle for competitiveness Viljoen (2008:412). In their study, Wilson and Pollard, (2009) indicated that not summits held in Geneva and Tunisia, in 2003 and 2005 respectively, developed and emerging countries successively created an ICT hype that pushed and initiated programs to cope with the ICT enabled development wave. During the last decade or two, businesses have come to recognise information as one of the most valuable assets, along with capital and human resources. Control over the information assets of an organisation has led to a shift in power into the hands of the information managers. It follows that information resources should be well governed (Viljoen, 2005:49).

The need for ICT governance is related to the importance of information in a modern organisation. The basis for power was historically the ownership of assets. This has changed, following the increased importance attached to innovation through research and development, process innovation and quality improvement in modern organisations. Innovation comes from human capital, and human capital has therefore become more important than physical assets in modern organisations (Symsons, 2005:3-5).

INFORMATION COMMUNICATION TECHNOLOGY GOVERNANCE

The Information Technology Governance Institute (ITGI) (2007:5) defines ICT governance as 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 ICT and its processes. The field of ICT governance has come to the fore in just over a decade, mainly to address organisational issues for ICT delivery to the business (Chitambal, 2006:5).

According to the ICT Governance Institute, as quoted by Tarn, Raymond, Razi and Han (2009:132), the term ‘governance’ is defined as the set of responsibilities and practices exercised by the senior management of an enterprise; it is designed to establish and communicate strategic direction, ensure the realisation of goals and objectives, mitigate risk, and verify assigned resources that are used in an effective and efficient manner. Establishing a security management structure to assign explicit individual roles, responsibilities, authority, and accountability is also one of the principles identified by the Information Technology Governance Institute (ITGI 2007:5).

The IT Governance Institute (IT Governance Institute, 2004b:17) also identifies four main focus areas for IT governance, all driven by stakeholder value. Two of them are outcomes - value delivery and risk mitigation - while the other two are drivers - strategic alignment and performance measurement. (Weill and Ross, 2004a:3) define IT governance as “specifying the decision rights and
accountability framework to encourage desirable behaviour in using IT.” These
distinguish between the behavioural view of IT governance and the normative view
of IT governance and corporate governance. The behavioural side of governance
defines the formal and informal relationships and assigns decision rights to
specific individuals or groups of individuals. The normative side defines the
mechanisms for formalising the relationships and providing rules and operating
procedures to ensure that objectives are met (Weill and Ross, 2004a:9-10).

IMPORTANT OF INFORMATION COMMUNICATION TECHNOLOGY
GOVERNANCE

ICT governance reflects the broader corporate governance principles (Weill and
Ross 2004a:8) as the goal of corporate governance is to align the actions and
choices of managers with the interests of stakeholders. ICT governance is
recognised as an extension of corporate governance (Sharma, 2007:2).
According to the South African Local Government Association’s (SALGA) ICT
roadmap (2012:14), developing countries such as South Africa have a tremendous
potential for rapid and sustainable economic and social development by leveraging
the potential of ICT and applying it appropriately within the local government sector.
As such, the vision of the Local Government Turnaround Strategy (LGTAS) states
that each municipality must have the necessary ICT infrastructure and connectivity;
and that ICT systems must be put in place across all municipalities to accelerate
ICT is a fundamental component of virtually every aspect of the Nelson Mandela
Bay Municipality. Service delivery, financial control and administration - all rely on
ICT and use ICT intensively. Information technology has a major impact on
organisational outcomes and represents significant investments (staff, finance,
equipment, geographic information, etc). ICT is also a key enabler of
transformational change; it changes the way in which organisations are able to
communicate and work (Ridley, 2006:2). The SALGA ICT roadmap indicates why it
is important to improve the status of ICT governance within municipalities.

RESEARCH METHODOLOGY

The research design for this study comprised a quantitative, explorative and
descriptive survey. Quantitative research is a formal, objective, systematic process
in which numerical data are utilised to obtain information (Burns and Grove,
2001:186). The data collecting instrument was designed in such a way that the
information collected could be quantitatively interpreted. The purpose of exploratory
research is to determine whether or not a phenomenon exists and to gain familiarity
with and an understanding of such phenomenon.

A convenience sampling technique was utilised to ascertain the responses of one
hundred and twelve (112) top level executives, managers, directors and deputy
directors that constituted the top level management team of the Nelson Mandela
Bay Municipality. According to Nisha (2012:6), convenience sampling is
a non-probability sampling technique that selects a group of elements based on their ease of access. The abovementioned author further states that available respondents are selected until a sample of the required size are attained.

There are a number of reasons why a convenience sample would be used instead of probability techniques, such as random sampling. Often, it is either impossible or impractical to collect data from an entire population. This might be due to a number of restrictions on the researcher, including the sheer size of the population to be analysed and financial (budgetary) and time constraints (Nisha, 2012:6). For the purposes of this study, a convenience sample was used, based on time constraints and the availability of top level management to respond to the questionnaire at hand. The aim of this and any sampling approach is to draw a representative sample from the entire population. The analysis and subsequent results of the sample are then generalised back to the population (Marshall, 1996:522).

Data were collected through the administering of a self-administered structured questionnaire. The questionnaire was divided into three sections. Section A comprised seven questions requiring biographical information. Sections B and C were on the Lickert scale. The data collection process was undertaken over the period 1 to 30 April 2013. Prior to the commencement of data collection, permission was first obtained from the Executive Director: Corporate Services Directorate in the Nelson Mandela Bay Municipality.

**METHOD OF ANALYSIS**

The purpose of data analysis is to reduce large amounts of data into smaller portions, from which inferential statements can be derived. For the purpose of data analysis the validity and reliability of the measuring instrument need to be evaluated. On the completion of this evaluation, the data is then described by means of descriptive statistics. Descriptive statistics are a set of coefficients used to describe a sample or population; these include measures of central tendency (mean, median and mode), and measures of variability such as variance and standard deviation (www.investopedia.com). In this study, after the descriptive statistics, Pearson’s product moment correlations calculated. The purpose of this was to evaluate the correlations between the factors of ICT governance in the NMBM Municipality.

For the purpose of this research, construct validity was evaluated. Construct validity is assesses whether the measurements of a variable act in the same manner as the variable itself (psucd8.wordpress.com). In other words, construct validity measures how well the actual characteristics of the variable in question are being measured. There are two subsections of construct validity namely convergent and discriminant validity. Convergent validity evaluates whether the characteristics of variables that are expected to be related are actually related, while discriminant validity evaluates whether the characteristics of variables that are not related are actually not related (Shuttleworth, 2009).
The validity of the independent variables was evaluated using a method called exploratory factor analysis. Leedy and Ormrod (2010) define factor analysis as a multivariate statistical method that reduces many variables into a smaller set of variables or factors whilst providing validity evidence of scales. It is an analysis used to describe variability between correlated factors. The validity of the dependent variable, *the perceptions regarding the extent of corporate governance*, is assessed by means of a confirmatory factor analysis. A confirmatory factor analysis is an approach used to test the proposed hypothesis (Leedy *et al.* 2010).

**REGRESSION ANALYSIS**

In this study, a multiple regression analysis was undertaken to investigate whether relationships existed between the perceptions of corporate governance in the NMBM and various ICT governance factors. The various ICT governance factors served as the independent variables and the perceptions of corporate governance of respondents served as the dependent variable. A multiple regression analysis is a general and very flexible data analytic system used in circumstances where the dependent variable needs to be studied as a function of, or in relationship to, the independent variable. According to Chatterjee and Hadi (2006:1), regression analysis is a tool for investigating functional relationships between variables. A regression model is expressed as an equation where the relationship between single dependent variables is connected to one or more independent variables. A multiple regression analysis is a means of statistical analysis that looks for an equation that represents the impact of two or more independent variables on a single dependent variable. A multiple regression analysis is used to analyse relationships between variables, enabling the researcher to isolate the quantitative impact of specific factors from many other contributing factors.

**NATURE AND FORM OF RESULTS**

In an attempt to influence the establishment of the quality of corporate governance within the NMBM, the researcher has undertook to evaluate ICT governance initiatives within the NMBM as a mechanism to enhance corporate governance, as a primary cause. The intention was in fact to establish how the NMBM could maximise value from its information technology investments through the implementation of ICT governance initiatives, aimed at aligning ICT strategies and investments with corporate business goals and strategies. For this reason, following a preliminary analysis and consultations with NMBM stakeholders in order to identify key governance policy areas most impacted by ICT, a relevant literature review was conducted. A proper research methodology was employed in order to arrive at reliable information from NMBM internal stakeholders.

The research results have identified some form of ICT governance standards and norms within NMBM structures. The assessment questionnaire evaluates whether a clear governance framework with supporting policies and standards exists. This
framework is key in ensuring that ICT investments in the NMBM are optimised and coordinated for maximum value creation. It is clear through responses received, that service delivery performance within the NMBM is not satisfactory, as indicated in the Auditor General’s reports. In order to improve ICT within the NMBM and to address the needs of citizens, business and potential investors, it is necessary to create a culture of service delivery and high performance, reinforced through transparent and robust ICT governance.

PERCEIVED SUCCESS OF ICT GOOD GOVERNANCE WITHIN NMBM

A confirmatory factor analysis was undertaken to assess the validity of the dependent variable Perceived success of ICT Good Governance within the NMBM. There were five intended factors measuring Perceived success of ICT Good Governance within the NMBM, and these were loaded together. Perceived success of ICT Good Governance within the NMBM explained 2.721% of the variance in the data. It was observed that factor loadings of between 0.917 and 0.545 were returned for this factor. Sufficient evidence of the validity of this construct was therefore provided. Perceived success of ICT Good Governance within the NMBM returned a Cronbach-alpha coefficient of 0.66, which is less than the lower limit of 0.7, but greater than the secondary lower limit of 0.6. Acceptable evidence of reliability for this factor was therefore provided.

INDEPENDENT VARIABLES

PROVISION AND SUPPORT OF ICT PROTOCOLS

An exploratory factor analysis was undertaken of each of the categories of independent variables, namely provision and support of ICT protocols; technology and ICT governance; risk and security management; ICT related organisational polices; and ICT systems and performance. Exploratory factor analysis answers the question posed by construct validity namely whether the scores of the test measure what the test is supposed to be measuring.

The items expected to measure the independent variable Provisions and support of ICT Protocols were assessed for validity by means of an exploratory factor analysis. All five items were loaded together. The factor loadings for this construct ranged between 0.948 and 0.740, proving that these factors are valid. Perceptions and support of ICT Protocols explained 4.04% of the variance in the data. The Cronbach-alpha coefficient for Provisions and support of ICT Protocols was 0.935, suggesting that the scale measuring this factor was highly reliable.
TECHNOLOGY AND ICT GOVERNANCE

The items expected to measure the independent variable *Technology and ICT governance* were assessed for validity by means of an exploratory factor analysis. Only item B3.4 was omitted, as the factor loading was below 0.5 and it was therefore not selected by the factor analysis model. The factor loadings for this construct ranged between 0.915 and 0.848, proving that these factors were valid. *Technology and ICT governance* explained 3.087% of the variance in the data. The Cronbach-alpha coefficient for *Technology and ICT governance* was 0.753, suggesting that the scale measuring this factor was reliable.

RISK AND SECURITY MANAGEMENT

The items expected to measure the independent variable *Risk and Security Management* were assessed for validity by means of an exploratory factor analysis. All five items were loaded together. The factor loadings for this construct ranged between 0.944 and 0.826, proving that these factors were valid. *Risk and Security Management* accounted for 3.988% of the variance in the data. The Cronbach-alpha coefficient for *Risk and Security Management* was 0.847, suggesting that the scale measuring this factor was reliable.

ICT RELATED ORGANISATIONAL POLICIES

The items expected to measure the independent variable *ICT related organisational policies* were assessed for validity by means of an exploratory factor analysis. All five items were loaded together. The factor loadings for this construct ranged between 0.917 and 0.779, proving that these factors were valid. *ICT related organisational policies* accounted for 3.848% of the variance in the data. The Cronbach-alpha coefficient for *ICT related organisational policies* was 0.613. Although this value is less than 0.7, it is higher than 0.6, which is the minimum acceptance level expressed in some research.

ICT SYSTEMS AND PERFORMANCE

The items expected to measure the independent variable *ICT systems and performance* were assessed for validity by means of an exploratory factor analysis. All five items were loaded together. The factor loadings for this construct ranged between 0.940 and 0.877, proving that these factors were valid. *ICT systems and performance* accounted for 3.976% of the variance in the data. The Cronbach-alpha coefficient for *ICT systems and performance* was 0.750, suggesting that the scale measuring this factor was reliable.

THEORETICAL FRAMEWORK AND HYPOTHESES

The operationalisation of the factors was formulated using factor analysis and the revised framework of hypothesis, displayed in Figure 2. The revised operational...
definitions are summarised in Table 1 and the revised hypotheses are depicted in Figure 2.

<table>
<thead>
<tr>
<th>TABLE 1: Operational definitions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Factor</strong></td>
</tr>
<tr>
<td>Provision and support of ICT protocols</td>
</tr>
<tr>
<td>Technology and ICT governance</td>
</tr>
<tr>
<td>Risk and security management</td>
</tr>
<tr>
<td>Executive ICT policy management</td>
</tr>
<tr>
<td>ICT systems and performance</td>
</tr>
<tr>
<td>Perceptions and extent of corporate governance</td>
</tr>
</tbody>
</table>

The formulated hypotheses are as follows:

H\(^{1a-1b}\): There is a positive relationship between the provision and support of ICT protocols as applicable to the NMNB, and the *Perceived success of ICT Good Governance within the NMNB*.

H\(^{2a-2b}\): There is a positive relationship between technology and ICT governance as applicable to the NMNB and the *Perceived Success of ICT Good Governance within the NMNB*.

H\(^{3a-3b}\): There is a negative relationship between risk and security management as applicable to the NMNB, and the *Perceived success of ICT Good Governance within the NMNB*.

H\(^{4a-4b}\): There is a positive relationship between executive ICT policy management as applicable to the NMNB, and *Perceived success of ICT Good Governance within the NMNB*.
H\textsuperscript{5a-5b}: There is a positive relationship between ICT systems and performance as applicable to the NMBM, and the \textit{Perceived success of ICT Good Governance within the NMBM}.

![Proposed Framework for statistically testing Perceived Success of ICT Good Governance in the NMBM](image)

Source: Researcher’s own construction

Descriptive statistics were calculated to summarise the sample data, namely the mean, standard deviation and frequency distributions. These results contributed to the achievement of the third secondary objective (state what the mean values are and whether most people agreed or disagreed, etc). Pearson’s product moment correlation was conducted in order to assess the relationships between the various factors under investigation.

Figure 3: Significant Relationships

---

PROVISION AND SUPPORT OF ICT PROTOCOLS

The results of this study show a significant positive relationship between Provision and support of ICT protocols and Perceived Success of ICT Good Governance within the NMBM. In other words, the more provisions and support for ICT protocols in place, the better the perceived extent of corporate governance in the NMBM. The following recommendations are put forward in this regard:

- In order for corporate governance to be implemented correctly, the ICT Sub - directorate has to implement and communicate its ICT policy agenda to the entire organisation.
- The NMBM needs to establish ICT Governance controls to mitigate the risk of ICT accountabilities and responsibilities by:
  - Documenting and formally adopting ICT Governance framework.
  - Documenting and adopting ICT risk and control framework and conduct risk assessments.

TECHNOLOGY AND ICT GOVERNANCE

The assumption that ICT governance was not being effectively managed in the NMBM necessitated the study an ICT governance initiatives. The Auditor General, in his audits and reports on its findings regarding corporate governance and the governance of ICT in the NMBM, has given adverse opinions. The
results of this study show a significant positive relationship between technology and ICT governance and perceptions regarding the extent of corporate governance in the NMBM. In other words, the more the value of technology is appreciated and the application of ICT regulatory mechanisms is intensified, the better the perceived extent of corporate governance in the NMBM. The following recommendations are therefore made:

- That a sustained enabling environment be created for directing the implementation of corporate governance of and governance of ICT.
  - That the corporate governance of ICT be evaluated and managed in such a way as to achieve continuous improvement of ICT enabled service delivery.
  - That ICT performance, conformance and risk management and monitoring are reported (Department of Public Service and Administration, 2012:21).

ICT RISKS AND SECURITY MANAGEMENT

The results of the study indicate a need for the NMBM to establish ICT risk and security management systems. In other words, the extent of corporate governance depends on the extent of security of the critical information of the municipality. The NMBM needs to design and implement adequate user access controls to mitigate the risk of unauthorised access to information systems that are not intended to be accessed. ICT risk and security management includes the following:

- How business related ICT risks are managed and how capacity is created in the risk management function to address ICT related risks.
- Ensuring that classified information; intellectual property and personnel information are protected within ICT systems.
- Ensuring that a business continuity plan is developed, informed by the operational, information and data requirements of the business.

ICT RELATED ORGANISATIONAL POLICIES

The NMBM has to institutionalise ICT governance as an integral part of municipal corporate governance. Through their responses, the respondents indicated a positive relationship between ICT related organisational policy and perceptions regarding the extent of corporate governance in the NMBM. The policy framework adopts principles and practices in support of a flexible and sustainable approach to the corporate governance of ICT systems.

ICT SYSTEMS AND PERFORMANCE

The financial and intangible benefits created by ICT should be increased to enable operational efficiency and a competitive advantage. The significant positive relationship between the ICT systems and performance and the perceived success of ICT good governance within the NMBM was demonstrated by the respondents in this study. The respondents were critical about the performance of NMBM ICT
systems as a service delivery tool and in the planning and controlling of resources. It is expected that the ICT must support the achievement of the Municipality’s strategic goals. The ICT systems and performance should describe the process that the Municipality will follow in the planning of the ICT enablement of its business. This should be aligned with the NMBM’s current strategic planning and management regime.

CONCLUSION

The most important conclusion is that when IT governance is well deployed, it results in many businesses and IT benefits. Effective IT governance ensures that IT supports business goals. It results in better returns on IT investments. Good governance ensures that IT risks are appropriately managed, which protects the stakeholders. In this study the need to adhere to a high standard of generally accepted good governance practices was highlighted. Assurance that good governance principles are applied adds value to any organisation, because trust in the organisation increases. The same conclusion was reached by several authors (Haes and van Grembergen 2004). Significant benefits associated with the application of technology in business are usually realised if they are accompanied by changes in business processes. This requires the involvement of top management, as well as mechanisms to facilitate cooperation across functional business areas. It may be argued that unless these governance mechanisms are well established, major process innovations in the NMBM environment will be limited, and the return on ICT spending in this environment will be low.

This is an important reason why ICT governance in the NMBM must improve. In this study, the relationship between corporate governance and IT governance was highlighted. The IT function can be regarded as a business, inside a business with appropriate strategic committees performing the function of a board to the ICT business. A different perspective of IT as a valuable resource that must be governed in the same way as the other resources (such as HR and finance) by the board and executive management of the organisation as a whole was also identified in this study. The first view fits in well with IT as a service function, and the organisation “buying” services from IT as a strategic business unit or a strategic partner. Alternatively, ICT can be viewed as an integral part of the business, in terms of which good governance, rather than the management of a service agreement, is required.

A number of valuable models, tools and techniques that can be used in IT governance have been identified or used in this study. These tools are valuable for managers to compare, analyse, categorise and diagnose situations and to support decision making. The value of COBIT for the purpose of directing, managing and controlling IT processes was established. Implementing a framework such as COBIT should make it easier for an institution to obtain additional relevant ISO certification (e.g. ISO 17799, ISO 9000 or BS15000).

It is recommended that COBIT be accepted as a standard approach for IT.

governance in the NMBM. It could be used with benefit as a guideline by
SAQUA to evaluate the ICT services of the NMBM. COBIT is an overall IT
governance framework, incorporating best practices from a number of more
specialised standards.

It is anticipated that IT governance as a discipline, and COBIT as a governance
framework, will be widely implemented in corporations worldwide. This will create a
growing need for individuals skilled in the use of COBIT. The NMBM would benefit
significantly from using this widely accepted standard to define its own IT
governance processes, and can also help to meet the required manpower
skills by incorporating COBIT into the curriculum for graduates. The discipline of IT
governance is yet in its infancy, and it has been suggested that the IT governance
paradigm may more suitably be based on the principles of collaboration,
competency and flexibility than on control, authority and efficiency (Peterson,
2004:73). Collaboration, competency and flexibility are particularly important
in complex and uncertain environments, such as the IT environment. Institutions
can derive much benefit from improving their IT governance and adopting and
adapting a well-researched and well recognised IT governance framework, such as
COBIT.

REFERENCES:

and development. The OECD Observer, 235, 29.

(October 10, 2009).

Bota-Avram, C. 2011. Some arguments that justify the audit trinity’s approach
in the context of Corporate Governance. Studies in Business and Economics, 6(1),
5-18. Babeş-Bolyai University, Cluj-Napoca, România

Buehpring, A. Casell, C. and Symon, G. 2006. Evaluating quantitative management
research: towards a contingent criteriology. International Journal of management
reviews, 8(3).

qualitative research. British Journal of Nursing, 16(12).

Cassell, C., Buehring, A., Symon, G. and Johnson, P. 2006. Qualitative methods in
management research: an introduction to the themed issue. Management Decision,
44(2), 161-166.

Cater-Steel, A. and Pollard, C. 2008. Conflicting views on ITIL Implementation:
Managed as a Project or Business as Usual? Proceedings of 2008 International


Chiabiro, R. 2006. An analysis of Information and Communications Technology initiatives needed to enhance Business value at Transwerk. (Master in Business Administration, NMMU).


Michelberger P. and Labodi C. 2009. Development of information security management system at the member of supply chain, University of Petroșani Economics.


