Corporate and IT Governance in Local Municipalities – Towards a Best Practice

Emile KASELOWSKI, Rossouw VON SOLMS
Nelson Mandela Metropolitan University, School of ICT, P.O Box 77000 NMMU, Port Elizabeth 6031, South Africa
Tel: +27 41 504 3604, Email: rossouw@nmmu.ac.za

Abstract: South African Municipalities are required, by Law, to perform strategic planning through means of compiling an Integrated Development Plan (IDP) document in order to meet specific, government-defined goals. Information Technology (IT) holds many advantages for the implementation of these goals if the IT systems and the business processes can be aligned with the IDP-goals. It is therefore necessary to govern the IT infrastructure, by means of an IT governance plan, to ensure that the IT goals complement the long-range IDP strategy. This paper discusses the background, criteria and content of such a plan, which is based on COBIT and ISO 17799 International Best Practices.

Keywords: Corporate Governance, IT Governance, Municipalities, COBIT, ISO 17799, Information Security, Management

1. Introduction

The Municipal Systems Act, nr 32 of 2000, states that every municipality in South Africa is required to define and document an Integrated Development Plan (IDP). The IDP is used to perform, document and communicate long-term strategic planning of objectives and processes, which the municipality must perform. The IDP is then used to measure the performance of a municipality at a high-level, concerned with service delivery, meeting objectives etc [1]. A municipality is also required to define and document a Master Systems Plan (MSP) document.

The MSP document describes IT infrastructure in detail, including hardware, software and networking components, which is needed for the municipality to be able to perform its necessary tasks. The MSP document contains short-term strategies for the development of the IT infrastructure, but does not contain any strategic planning information as in the IDP document.

Both IDP and MSP documents are of a strategic nature, but operate at two different levels of abstraction. The IDP operate at a high level, describing general objectives and processes and some information about how to achieve them, while the MSP operate at a very low, detailed level. Unless these two strategies are linked together, the IT systems run the risk of not being able to fully complement the IDP goals.

Ideally, it is necessary to define an IT governance plan in order to link these two strategies together. Thus, it would enable the high-level organizational goals to be converted into lower-level, short-term goals, aimed at the IT function of the municipality.
Figure 1 illustrates how this IT governance plan links the municipal IDP and MSP strategies:

Information is considered the lifeblood of any organization, according to Botha and von Solms [2]. In the human body, blood flows through veins to reach the organs and other parts of the body. This is similar to the flow of information within an organization, in order to “feed” the business processes. Since the cardiovascular system plays a vital role in the human body, therefore the IT systems of the organization (in this case a municipality) should play a vital role in order for the organization to meet their objectives. The Information Technology Governance Institute (ITGI) claims that Corporate Governance and IT Governance can no longer be seen as two separate disciplines [3]. Therefore, IT can no longer be seen as an issue that is only of a technical nature. It is important to encourage a culture in municipalities where IT is an integral part of the overall corporate governance culture. This will ensure that the IT objectives are direct descendants of the overall, municipal, IDP objectives.

The goal of this paper is to introduce an IT governance plan that binds together the high-level IDP and the more detailed MSP. This plan, after implementation, ensures that the IDP objectives can be converted into strategic, IT-level objectives. The reason for this is that the IT systems and objectives should complement (be aligned with) the IDP objectives.

2. Criteria for an IT Governance Plan for Municipalities

There are various factors that should be taken into consideration when defining an IT governance plan for a Municipality. These include factors such as: Municipal legislation, published best practices and guidelines and the yearly IT audit reports from the Auditor General of South Africa.

Current legislation and Municipal Acts are the most important factor to take into consideration. These acts, including the Municipal Finance Management Act and the Municipal Systems Act, define municipalities and dictate their specific functions. It is important that the controls and processes that are defined in the IT governance plan are aligned with the law governing municipalities. Secondly, published best practices and guidelines serve as a solid foundation on which the IT governance plan can be based. These best practices such as COBIT and ISO 17799 is already widely used and recognized all around the world and is continually refined and updated. The third important factor to take into consideration is the yearly audit report produced by the Auditor General, which reports on the status and shortcomings of the IT systems of each specific municipality in South Africa. This yearly audit is a formal and required process for every municipality.

The proposed IT governance plan will only be successful if all of the above-mentioned factors are taken into consideration.
3. The IT Governance Plan

A research project was started at a district municipality and its underlying local municipalities in order to define such an IT governance plan. This project made use of various tools, such as questionnaires, interviews and case studies to determine the current role of IT in local and district municipal governments. The results of this specific project depicts the current state, as well as the acceptable, consensus norm for IT governance in local municipalities.

Thus, the IT governance plan has been defined by using the important factors as mentioned previously, as well as the results of the research project. COBIT and ISO 17799 is briefly discussed in the following sections.

3.1 Control Objectives for Information and related Technologies (COBIT)

COBIT, published by the Information Systems Audit and Control Association (ISACA), was the major framework, in conjunction with the ISO 17799 standard, on which this plan is based. COBIT was chosen for two major reasons. Firstly, because it covers a wide spectrum of IT governance processes and objectives and secondly, because the IT infrastructure of municipalities are audited against COBIT by the Auditor General, before the yearly financial audit.

COBIT consists of four major domains covering a wide spectrum of IT processes. These domains are subdivided into 34 high-level objectives for IT governance. Appendix A describes some of the important COBIT objectives to provide better understanding. These objectives are made up by a total of 314 detailed objectives. Table 1 contains the 34 high-level objectives, as well as the domain in which they are classified [4]:

<table>
<thead>
<tr>
<th>COBIT Processes</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
</tr>
</thead>
<tbody>
<tr>
<td>Planning and Organizing - PO</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Acquire and Implement – AI</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deliver and Support – DS</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Monitoring – M</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Each of these objectives can be measured according to their maturity as implemented in the municipality. COBIT specifies 6 levels of process maturity [4]. These are:

0. Non Existent
1. Initial / Ad hoc
2. Repeatable
3. Defined
4. Managed and Measurable
5. Optimal.

The goal of the COBIT Maturity Model is to identify an acceptable balance between the importance, practicality and efficiency of each objective and its processes. Because all organizations are different to one another, some processes might be more important than others, while some processes might not even be applicable. For this reason, the maturity model was used to identify the acceptable level of governance for each of the 34 objectives. The following paragraphs describe the information security aspect of the IT governance plan.
3.2 Using ISO 17799 in conjunction with COBIT

Security is also a very important aspect of IT governance, since information is as valuable to the organisation as blood is to the human body. It is therefore necessary to protect the integrity of information to ensure that it is not rendered worthless. Although the COBIT DS5 objective deals specifically with IT security, there are various security processes contained in the other objectives as well which deals with security. In order to complete the IT governance plan, the ISO 17799 standard has been incorporated into this plan.

According to Von Solms there are various reasons why COBIT can be used in conjunction with ISO 17799 [5]:

a) COBIT contains IT governance objectives and processes, which is spread over a wide spectrum of IT governance. ISO 17799 deals specifically with IT security issues

b) COBIT’s processes are described at a higher level than those of ISO 17799

c) There are various processes that are included in both the COBIT and ISO17799 standards

d) COBIT explains what must be done, while ISO 17799 describes how it should be done.

Although COBIT and ISO 17799 complement one another to a certain degree, it is not always clear as to which COBIT process corresponds to which ISO 1779 process. Therefore, the ITGI published a document called “Mapping of ISO/IEC 17799 with COBIT” which contains the mapping and explanations between the processes in COBIT and ISO 17799. Thus, the numerous advantages of using COBIT in conjunction with ISO 17799 are self-explanatory. The following paragraphs briefly describe how the case studies were performed, using COBIT and ISO 17799 to obtain the necessary information on which to base the IT governance plan.

Case studies, in conjunction with questionnaires and interviews, were conducted at the participating, local municipalities to determine which COBIT processes are relevant to a municipality, as well as which maturity level is acceptable for each applicable process. This process involved discussing and evaluating each of the 34 high-level COBIT objectives against the requirements of the municipality, taking the audit requirements into account. Three results were obtained from each of the case studies: firstly, whether the objective was indicated as being an important objective for the municipality. Secondly, the current level of maturity for each process was determined by evaluating the current municipal process against the COBIT maturity model. The minimum acceptable maturity level for each of the processes were also investigated and determined using the maturity model. This process involved the discussing of each of the objectives and how each objective should be implemented and executed. The municipal IT audit report also provided important information on at which maturity level the objectives should be. The results were captured using a tool that was developed to be able to conduct the case studies. This tool produced a report for each case study to show the risk, or ‘gap’, between the current level of governance and the minimum acceptable level of governance. The results were then combined and used to form part of the basis of the IT governance plan for the district. This plan has been defined in such a way so that the highest priority and risk processes are attended to first.

The minimum acceptable level of maturity for each COBIT process were identified while taking factors such as importance, trade-off between cost and effectiveness, applicability to the municipality etc. For certain processes, the IT audit reports states various minimum requirements which must be met. These requirements were compared to the maturity model and the corresponding level chosen as the acceptable minimum maturity level. Table 2 depicts the findings of the acceptable minimum maturity level for each of the 34 COBIT processes:
Table 2: The Minimum acceptable maturity level for each process – Not true values

<table>
<thead>
<tr>
<th>COBIT Processes</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
</tr>
</thead>
<tbody>
<tr>
<td>Planning and Organizing – PO</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>4</td>
<td>5</td>
<td>4</td>
<td>2</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Acquire and Implement – AI</td>
<td>2</td>
<td>4</td>
<td>4</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deliver and Support – DS</td>
<td>5</td>
<td>3</td>
<td>4</td>
<td>4</td>
<td>5</td>
<td>3</td>
<td>4</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>4</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>Monitoring – M</td>
<td>4</td>
<td>3</td>
<td>3</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

From the table above, the following conclusions were drawn:

1. Every process is applicable to IT governance in local and district municipalities and so it is important to implement each one.
2. Each process is required in both a district and local municipality.
3. Some processes are more important than others. Those with a higher maturity level than others require more strategic implementation than those with a lower minimum acceptable maturity level.

The IT governance plan has been defined using the following methodology:

The applicable COBIT objectives and processes were identified which is applicable to both local and district municipalities. For each of these objectives, the minimum acceptable maturity level was identified using the various above-mentioned methods. The corresponding ISO 17799 controls were then added to the COBIT processes. The COBIT processes were then prioritised according to the importance and business impact.

To ease the task of implementing the 34 COBIT processes and their respective ISO 17799 security processes, they were grouped into implementation phases containing five COBIT processes. Processes in Phase 1 should be implemented first. This COBIT assessment provided a good understanding of the requirements for IT governance in municipalities. Security requirements were also needed to be determined in the form of a risk assessment, since the ISO 17799 standard was incorporated in the IT governance plan.

To enhance the effectiveness of the IT governance plan’s security component, a comprehensive “ISO 17799 analysis” was conducted at the district municipality to determine which ISO 17799 security clauses and controls were relevant to the municipality. The outcome of the analysis was which ISO 17799 controls were applicable, as well as to which extent the required clauses and controls were already implemented. The ‘gap’ between the required and current implementation was then also identified.

The resulting set of clauses and controls from the ISO 17799 analysis was then compared to the mapped controls between COBIT and ISO 17799. The clauses and controls that were determined not to apply to the municipality were then discarded. The mapping between COBIT and ISO 17799 also resulted in ISO 17799 controls being mapped to multiple COBIT processes. This resulted in a redundancy, or false view of the number of ISO 17799 controls to implement in some COBIT processes, since a control only needs to be implemented once to satisfy the security requirement. To address this issue of redundancy, the applicable ISO 17799 controls for the first phase of implementation of the IT governance plan were recorded. For the following phases, the mapped ISO 17799 controls were ignored which had already been addressed in the previous phases.

The end result was an IT governance plan, named the IT Strategic Objective Plan (IT-SOP) was compiled from two main sources, COBIT and ISO 17799. They were both analysed to determine which processes and controls were applicable to a municipality. From COBIT, a list of objectives and their respective target maturity levels were obtained. From ISO 17799, a
list of all the relevant security controls and clauses were obtained. The COBIT objectives were grouped into phases and the security controls mapped to their respective COBIT objectives and processes. Security controls that were redundant were ignored since they have already been addressed in previous implementation phases of the IT governance plan. To facilitate the implementation of this IT-SOP, a project plan was developed that follows the same structure of the IT-SOP and contains the different phases, COBIT objectives, detailed controls and relevant ISO 17799 security controls. Figure 2 graphically depicts the flow of the project:

![Flowchart of IT governance project](image)

4. Conclusion

It is very important that all business processes are based on a solid foundation and that they are correctly developed and managed. Most business processes today are either based on IT systems, or make use of IT systems to a certain degree.

This paper discussed the requirement for better IT governance in local municipalities in South Africa. An IT governance plan has been identified to cater for this need for better IT corporate governance in municipalities. The COBIT framework and the ISO 17799 standard were briefly discussed as well as how they form part of the IT governance plan.

This IT governance plan is of a strategic nature, practical, based on international standards, can be measured against various metrics such as COBIT’s maturity model and conforms to the requirements of South African municipal legislation as well as the yearly municipal IT audit reports. The objective and controls of COBIT and ISO 17799 were analysed to determine their relevance to municipalities in order to provide clear guidance as to what needs to be achieved.
There are many potential advantages to a municipality should it implement this strategic IT governance plan in order to develop and manage its IT governance processes not only to protect the Board members against possible prosecution according to their accountability, but also to expedite public service delivery by aligning its IT system with the municipal IDP objectives and to counter fraudulent activity within a municipality. These two objectives can be achieved by having a secure, healthy IT infrastructure, which is properly governed and supportive of the overall mission and vision of the municipality.

References

APPENDIX A

**PO1 – IT Strategic Planning**
This COBIT objective contains detailed control objectives that, when implemented, ensures that adequate long-range and short-range planning is conducted by the organisation as part of the IT strategic planning process. This objective deals with issues such as the creation of plans, change management for plans, monitoring and updates to the strategic plans.

**PO4 – Define the IT organisation and relationships**
This COBIT objective contains detailed control objectives that deals with the overall governance of IT within the organisation. Amongst other, this objective deals with the placement of IT in the organisational hierarchy, reporting lines, key IT personnel etc.

**AI6 – Manage Changes**
This COBIT objective deals with the issue of change management for IT systems, policies, processes and procedures. It contains detailed objectives which help to ensure that adequate change management is performed by the organisation, including change requests, emergency changes, change communication etc.

**DS4 – Ensure Continuous Service**
This COBIT objective ensures that an organisation has adequate procedures in place in the event of an emergency or disaster. It ensures that a disaster recovery plan is in place and stipulates the content and structure of such as plan, including off-site processing facilities, etc.

**M4 – Provide for independent Audit**
This COBIT objective specifies the processes needed to allow an organisation’s IT systems and policies to be audited on a regular basis to ensure adequacy and completeness in terms of auditing standards.