Association for Information Systems
AIS Electronic Library (AISeL)

ECIS 2007 Proceedings

European Conference on Information Systems (ECIS)

2007

Model-Based IT Governance Maturity Assessments with Cobit

M. Simonsson
Royal Institute of Technolog, ms101@ics.kth.se

P. Johnson
pj101@ics.kth.se

H. Wijkström
hannaw@ics.kth.se

MODEL-BASED IT GOVERNANCE MATURITY ASSESSMENTS WITH COBIT

Simonsson, Mårten, Department of Industrial Information and Control Systems, KTH, Royal Institute of Technology, Osquldas väg 12, 10044, Stockholm, Sweden, ms101@ics.kth.se

Johnson, Pontus, Department of Industrial Information and Control Systems, KTH, Royal Institute of Technology, Osquldas väg 12, 10044, Stockholm, Sweden, pj101@ics.kth.se

Wijkström, Hanna, Department of Industrial Information and Control Systems, KTH, Royal Institute of Technology, Osquldas väg 12, 10044, Stockholm, Sweden, hannaw@ics.kth.se

Abstract

IT governance is an executive level concern in many enterprises today, but a method for credible, reliable, and cost-efficient IT governance maturity assessment has been lacking. Control Objectives for Information and related Technology (Cobit) is best practice in the area, but the method requires an experienced analyst to perform the assessment and the provided analysis framework is vague and ambiguous. This paper presents a Cobit based method designed to overcome these featured problems. It comprises a modeling language for IT governance based on Cobit, and a transparent analysis framework which enables aggregation of single metrics into comprehensive maturity scores. The applicability was tested in a small case study. Results demonstrate that the method can be used to conduct time-efficient, valid and reliable IT governance maturity assessments without the help of an experienced analyst.

Keywords: IT governance, IT organization, modeling, Cobit

1 INTRODUCTION

IT governance (ITG) is an important issue on the agenda for many enterprises today. Although there has been a need to provide guidance on the use of IT since the early days of computing, the actual term IT governance did not appear until the nineties, when Loh and Venkatraman (1992), and Hendersen and Venkatraman (1993) used the term to describe the complex array of interfirm relationships involved in obtaining strategic alignment with business and IT. Effective IT governance provides mechanisms that enable IS/IT management to develop integrated business and IT plans, allocate responsibilities, and prioritize IT initiatives (Korac-Kakabadse 2001, Ross 2003, Weill 2002a and Weill 2002b).

In this paper, we propose a method for IT governance maturity assessment within an enterprise. This kind of assessment is essential for good monitoring, enhancement and management of existing IT governance processes and structures. In particular, by using a method for assessing IT governance maturity, it is possible to compare and rationally select between potential future scenarios. For instance, if the decision-making authority for acquisition of commodity software is moved from business unit level to IT operations level, how would that improve the maturity of the affected processes? The possibility to perform trade-off analysis between potential scenarios is one of the most important benefits of having an efficient IT governance assessment method in place. Another benefit is the possibility to benchmark against other organizations. Also, a good IT governance assessment method can provide useful prescriptive results about what can be done to improve the governance of IT within the organization under evaluation.

Measurement is thus the base for decision and action, but how do we know that our measurements are any good? There are three overarching requirements on measurements systems: validity, reliability and measurement cost. These requirements are also suitable for IT governance maturity assessment methods. There are currently a few such methods aiming to support IT governance. Weill & Ross have developed an ITG framework based on just a few questions that can be used to assign responsibilities for high level IT decision making, but their work gives no further guidance on how the IT organization should actually perform their labor (Weill & Ross 2004). The ISO/IEC 20000 and its preceding IT Infrastructure Library (ITIL) might aid the creation of processes related to delivery and support. ITIL also details establishment and maintenance of service level agreements (SLA) and operation level agreements (OLA). However, ITIL gives no support for strategic IT concerns (ISO/IEC 2005, OGC 2002). The most relevant existing method is Cobit, which is discussed more thoroughly in the third section of this paper.

Based on the concepts of validity, reliability and measurement cost, the second section of this paper contains a list of requirements that a method for ITG maturity assessments should fulfill. Section three presents Cobit, one of the most recognized frameworks for IT governance. Cobit's degree of fulfillment to the requirements is presented in section four. Section five presents the proposed method for IT governance maturity assessments. It is tested against the requirements in section six, and section seven features an example application of the method. The paper ends with conclusions and references.

2 REQUIREMENTS ON A GOOD ITG MATURITY ASSESSMENT METHOD

In measurement theory, the goodness of an assessment is specified in terms of validity and reliability (King & Keohane 1994). For practical applications, these benefits need to be traded against the cost of performing the measurement. The remainder of this section presents a set of requirements that a good IT governance assessment method needs to fulfill. In subsequent sections, the proposed IT governance assessment method and its most obvious alternative are evaluated with respect to these requirements.

2.1 Good validity

Validity is often defined as the extent to which a measure accurately reflects the concept that it is intended to measure. As an example from the domain of (kitchen) physics, when measuring the weight of a liquid, it would be a problem of validity if one did not take into account also the weight of the container in which the liquid was placed.

Regarding the validity of the assessments, it is thus important that the method really measures what is considered as IT governance concerns. If the method is inappropriately calibrated, perhaps the general goodness of business processes or just the administrative concerns of IT operations are actually evaluated. Another problem of validity would be if the method was based on a view of IT governance that differed significantly from the common conception. To prevent this from happening, the method should be based on existing state of practice definitions of the subject. This requirement can be summarized as follows:

RQ1: Consistency with common conceptions. The method should be consistent with common conceptions from both academia and practitioners, i.e. based on valid IT governance sources.

2.2 Good reliability

Reliability may be defined as the extent to which a measure yields consistent, stable, and uniform results over repeated measurements of the same unit. Considering the same example as above, when measuring the weight of a liquid, it would be a problem of reliability if different people normally obtained different weights of the same liquid.

Maturity assessment results should reflect an objective rather than subjective view of the evaluated company, so that any given analyst would obtain the same conclusion from the same piece of empirical data. Repeated assessments should lead to the same results each time. To obtain good reliability, the maturity assessment method must be succinctly operationalized. This means that the method must be unambiguous with respect to two important aspects. Firstly, the method should be operationalized with respect to the data that needs to be collected. Secondly, the method should be operationalized with respect to aggregation of data into assessment results (typically presented in terms of a maturity level). Considering data collection, the method needs to detail the entities and relations important for IT governance, including e.g. processes, roles, responsibilities, activities, metrics, and documents. The set of data that should constitute the base for assessment must of course be derived from knowledgeable sources, according to the validity requirement above. Considering aggregation of collected data, the method should unambiguously specify how the analysis of data is to be carried out. For maximum reliability, it should be possible to perform the assessment numerically, basing the assessment on e.g. the existence of a certain entity, the number of occurrences of an entity, and the frequency or goodness of a relation.

RQ2: Descriptive operationalization. The method should be descriptively operationalized, i.e. support unambiguous and objective representation of IT governance.

RQ3: Normative operationalization. The method should be normatively operationalized, i.e. support unambiguous and objective analysis of IT governance.

2.3 Low cost

The cost of the assessment cannot be disregarded. Upon applying academically developed methods in the competitive real world, it is of utmost importance that assessment costs are kept at a minimum. The costs associated with IT governance assessment can be divided in two different parts. Firstly, there is the cost of collecting data, i.e. performing interviews, studying enterprise documentation, etc.

Secondly, there is the cost of performing the analysis by transforming the collected data into an overarching maturity level assessment. For both of these activities, there is the obvious time spent collecting and analyzing. But there is also the cost of learning how to use the method and it is desirable that the method only requires a fairly basic level of assessment knowledge from the analyst. At best, it should be possible to employ the method in-house without the help of expensive consultants.

RQ4: Support for efficient data collection. The method should support efficient data collection, i.e. provide an efficient representation of IT governance.

RQ5: Support for efficient analysis. The method should provide support for efficient analysis, i.e. support efficient normative judgments of IT governance.

3 COBIT’S IT GOVERNANCE MATURITY ASSESSMENT METHOD

Control OBjectives for Information and related Technology, Cobit, is a well-known framework for IT governance improvement, risk mitigation, IT value delivery and strategic alignment maturity assessments (Debraceny 2006, Guldentops 2004, van Grembergen 2004, Holm-Larsen 2006, Ridley 2004, Warland 2005). The framework was first issued by the IT Governance Institute, ITGI, and Information Systems Audit and Control Association, ISACA, in 1998. The framework has been under constant development ever since, and a fourth version became available in December 2005 (ISACA 2005). Cobit describes the IT organization by means of 34 processes, divided among four domains: Plan & Organize, Acquire & Implement, Deliver & Support, and Monitor & Evaluate.

Each process is divided into several activities and a set of detailed control objectives, i.e. statements of the desired results to be achieved by implementing control procedures for the processes. Further, different kinds of metrics such as key performance indicators (KPI), key goal indicators (KGI), and critical success factors (CSF), are suggested in order to monitor the general goodness of each process. Lists of inputs and outputs for each process are presented. Each process has a corresponding capability maturity model (CMM). The latest version of Cobit also contains RACI matrices, which suggest stakeholders to be responsible, accountable, consulted, and informed regarding certain activities. Cobit is a frequently used, best practice based framework, and its use is described in several case studies, c.f. (Sallé 2005, Simonsson 2005).

It is possible to argue for the fact that Cobit is becoming a de facto standard for IT governance maturity assessment. But is its focus the same as required by practitioners and in academic literature? This concern deals with the validity of a Cobit based IT governance maturity assessment and whether it is really IT governance that is assessed. A previous study has shown that the focus of Cobit, regarding different concerns within IT governance, is quite similar to the foci of practitioners and academics (Simonsson 2006). The main difference identified in the study concerns Cobit’s strong emphasis on monitoring, i.e. there are lots of metrics but little support for improved decision-making.

One of the biggest disadvantages with Cobit - and perhaps the main reason why the framework is not used more frequently by practitioners, is that a lot of knowledge about the framework is needed in order to apply it as a tool to support IT governance or assess the IT organization’s performance. Even though a vast number of processes, activities, and responsibilities are described, the connection between e.g. the determined goodness of an activity and how that is reflected in the featured maturity model is not specified. The maturity model is mainly a stand-alone analysis tool that provides only a very shallow analysis of the situation. Due to this, it takes an experienced analyst to conduct a credible maturity assessment of an IT organization by the use of Cobit. Further, there is no support to assure that two such experienced analysts would come to the same conclusion regarding the maturity of a company’s IT organization.

4 COBIT’S FULFILLMENT TO THE REQUIREMENTS

As mentioned in the introduction, Cobit was the only identified IT governance maturity assessment method available for public use that could possibly fulfill the requirements stated. In this section, we consider the degree of fulfillment, requirement by requirement.

RQ1: Consistency with common conceptions. Cobit is a de facto standard in the field and is often referred to as *the* assessment framework for IT governance, c.f. (Debraceny 2006, Guldentops 2004, van Grembergen 2004, Holm-Larsen 2006, Ridley 2004, Warland 2005). Requirement fulfilled.

RQ2: Descriptive operationalization. Cobit contains all the processes, activities, documents, etc. needed to correctly represent all ITG concerns. Nonetheless, some incongruence exists within Cobit, e.g. the dual notion of detailed control objectives and quite similar activities discussed earlier. Requirement partly fulfilled.

RQ3: Normative operationalization. Cobit provides a vast amount of metrics that can be used to assess the maturity of IT governance. These are however not arranged in a way such that the aggregation from separate metrics into a comprehensive maturity level is supported. The analysis cannot be made transparently, and the requirement is therefore not fulfilled.

RQ4: Support for efficient data collection. Cobit does not aid efficient data collection, and no option to just partly implement the framework is suggested. Analysis and data collection are not clearly separated and must both be carried out by experienced analysts. Requirement not fulfilled.

RQ5: Support for efficient analysis. The analysis part of Cobit is neither transparent nor automated. The result of a Cobit supported IT governance maturity assessment might vary from one time to another, mainly depending on the analyst. Requirement not fulfilled.

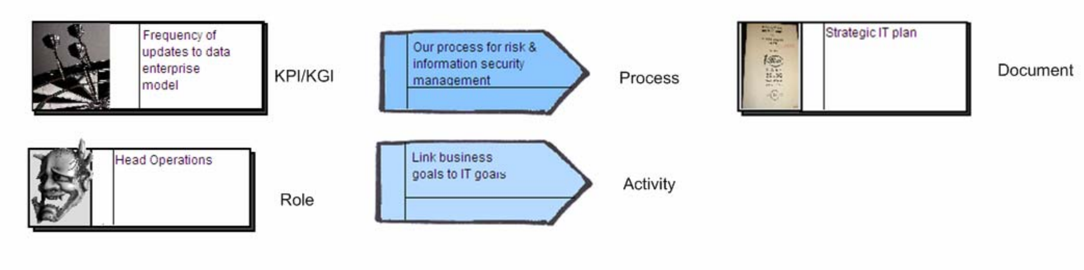

Frequency of updates to data enterprise model
KPI/KGI
Our process for risk & information security management
Process
Strategic IT plan
Document
Head Operations
Role
Link business goals to IT goals
Activity

Figure 1. The entities employed in the modeling language for IT governance.

5 A MODEL-BASED METHOD FOR IT GOVERNANCE MATURITY ASSESSMENT

As demonstrated in the previous section, Cobit did not fulfill all requirements for a good ITG maturity assessment method. In particular, Cobit performs weakly with respect to requirements RQ3 to RQ5. This paper proposes a method for model-based maturity assessment of ITG which is based on the existing Cobit framework, leveraging the benefits of Cobit and mitigating the weaknesses. The proposed method can thus be viewed as an extension of Cobit. It contains two parts: A modeling language and an analysis framework. The modeling language provides support for the descriptive activities of IT governance assessment, i.e. the (non-judgmental) representation of how IT is governed within the assessed company. The analysis framework provides support for the normative activities of an assessment, i.e. the judgment on whether the given IT governance structure is good or bad. Both are detailed in the remainder of this section.

5.1 The modeling language

As mentioned previously, we decided to base our IT governance modeling language on the existing Cobit framework. The structure of Cobit allowed us to identify entities and relations quite easily. These are listed in Figure 1 and presented in further detail below.

5.1.1 Entities

The notion of *processes* to describe the IT organization is commonly used and was taken directly from Cobit. The content of 34 processes relevant for management, control and operation of IT is detailed. However, we choose not to use the exact descriptions of the content for each process as building blocks of our modeling language, since no single organization employs processes exactly the same way. For instance, a company might have a process that covers both information security and risk management activities, instead of separating these issues into two distinct processes as suggested in Cobit (PO9: Assess and Manage IT Risks, DS5: Ensure Systems Security). Rather, we chose the notion of a general process serving as a container of elements with finer granularity, namely activities.

Cobit distinguishes between *activities* and detailed control objectives, but the difference between the two is not explained in the framework. It the belief of the authors of this paper that, given Cobit's origin of being a tool for IT auditors, the detailed control objectives are relics from the old days. Control objectives are certainly convenient for auditors performing a check-list style revision of a company's IT. The activities were introduced in version 4.0 of the framework, together with the RACI matrices. Even though there is a conspicuous overlap between the detailed control objectives and activities, they are not completely alike. The activities, but not the control objectives, appear in the RACI matrix of each process in Cobit, and the activity notion was therefore chosen for our modeling language. In the modeling language, each process contains one or more activities, and in contrast to the process entity, they represent the actual content of the work performed within the IT organization. Returning to the example of a company hosting a joint process for information security and risk management, this combined process would typically contain activities from the Cobit processes PO9: Assess and Manage IT Risks, and DS5: Ensure Systems Security. An activity contains the lowest granularity of tasks performed in an IT organization that are implemented in the modeling language. In order to correctly represent how well an activity is performed, the "Activity execution" property was created. Upon studying the generic Cobit maturity model, it was concluded that each activity can be represented by a) whether management is aware of the importance of issues related to the activity, b) if monitoring of the activity is performed, c) if the activity and its inputs and outputs are documented, and d) if activity improvement actions take place on a regular basis. These four characteristics were combined into the Activity Execution property.

It is frequently stated in Cobit, and it is even a part of the generic maturity model, that certain *documents* should be produced to assure that activities are correctly executed. However, Cobit does not feature a detailed list with all the documents that the IT organization is supposed to keep updated. Rather, in order to create the document entity of our modeling language, the inputs and outputs to and from each process were studied. This list contains mainly documents, e.g. the strategic IT plan, security incident definition, risk assessment, and cost/benefit report, but also artifacts such as databases and general directions. The content of this list are the documents to be modeled.

Cobit lists a vast number of metrics that can be used to monitor the progress of each process and its maturity; typically about a dozen for each process. These are represented as *KPI/KGI* entities in the modeling language. Moreover, Cobit contains an equally large amount of goals for activities, processes and IT in general. These were however excluded from the modeling language, as we did not want to assess the existence of goals within an organization, but rather desired to focus on the current achievements. A very important aspect of IT governance concerns the locus of IT decision making. Therefore, it may seem quite odd that it was not until the latest version of Cobit that roles and responsibilities were introduced in the framework. Today Cobit clearly states that the Board, Chief Executive Officer, Chief Financial Officer, Business Executives, Chief Information Officer, Business Process Owners, Head Operations, Chief Architect, Head Development, Head IT Administration, Program Management Officer, Compliance, audit, risk and security personnel, Deployment Teams, Training Department, Service Managers, Service Desk/Incident Managers, Configuration Managers, and Problem Managers are the main stakeholders upon governing IT. These are included in the *role* entity of our modeling language.

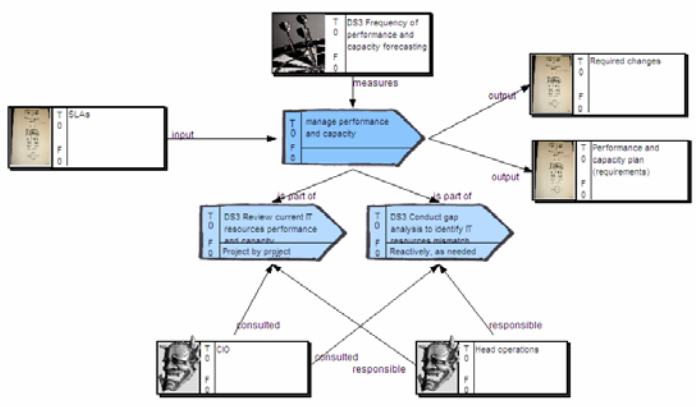

DS3 Frequency of performance and capacity forecasting
measures
SLAs
input
manage performance and capacity
output
Required changes
output
Performance and capacity plan (requirements)
is part of
is part of
DS3 Review current IT resources performance and capacity
Project by project
DS3 Conduct gap analysis to identify IT resources mismatch
Reactively, as needed
consulted
responsible
CIO
consulted
responsible
Head operations

Figure 2. An example of a model based on the proposed modeling language for maturity assessment of IT governance.

5.1.2 Relations

The RACI matrix provided by Cobit states that each IT related activity may be associated with a role, so that the role is either *responsible*, *accountable*, *consulted* or *informed* with respect to the activity. Let us for instance study the ME4 activity "Establish executive and board oversight and facilitation over IT activities". Cobit states that the Board should be accountable for the activity, the CEO responsible, and several other roles should be consulted with respect to it (CFO, Business Executive, CIO, and Compliance, audit, risk and security personnel). The four relation types in italic above were incorporated into the modeling language. As mentioned previously, the interface between processes consists mainly of documents. In order to model this, relations to denote *inputs* and *outputs* were created. The smallest building block of the modeling language is the activity. The last relation was created in respect to activities and processes. To illustrate this relationship in the modeling language, the *is-a-part of*-relation denotes e.g. that a process contains three activities. Figure 2 shows an example, where some of the responsibilities and documents of the DS3 process are modeled.

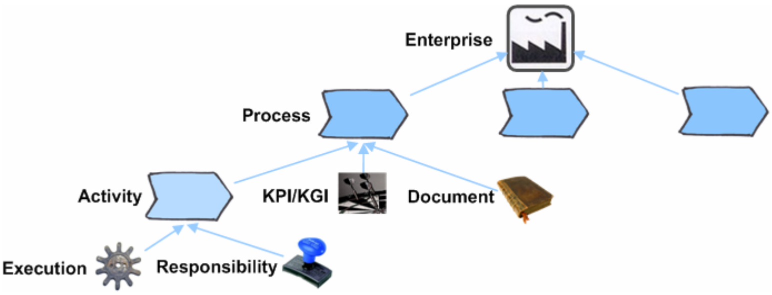


Figure 3. The formalized analysis framework for IT governance maturity assessments contains three levels: The enterprise, the processes and the activities. See also Table 1.

5.2 The formalized analysis framework

In the previous subsection, a language for modeling the parts of an IT organization relevant from an IT governance perspective was presented. By using such a language, it is possible to create a model over any organization’s current or future IT governance structure. In the following subsections, a framework for assessing the maturity of such a model is presented. A standardized set of metrics is presented in subsection 5.2.1. In order to eliminate unnecessary subjectivity from the maturity calculations, a procedure for aggregation of separate metrics into a total maturity score is presented and exemplified in subsection 5.2.2. Table 1 lists the metrics that are taken into account, and presents how maturity levels are assigned. The general design of the analysis framework is presented in Figure 3.

5.2.1 Metrics

Cobit provides a plethora of performance indicators, responsibility assignment suggestions, activities and goals that can be monitored in order to obtain good IT governance. Cobit also contains process level maturity models. However, the maturity models presented in Cobit contain only a few lines of plain text describing the characteristics for each maturity level and each process, and the framework doesn’t detail the connection between the controls and maturity levels. In other words, it is not clarified how monitoring of a single metric would affect the maturity of an entire process. By studying the process level maturity models carefully and generalizing the findings so that they could be valid for activities as well, the authors of this paper identified four generic metrics. These are “Activity execution”, “Assigned responsibilities”, “Documents in place”, and “KPI:s/KGI:s monitored”, c.f. Table 1. The former two are assessed for each activity, while the latter two are assessed at process level, c.f. Figure 3.

Metric/ Maturity level	**Activity execution**	**Assigned responsibilities**	**Documents in place**	**KPI:s/ KGI:s monitored**
Level 0	No awareness of the importance of issues related to the activity. No monitoring is performed. No documentation exists. No activity improvement actions take place.	No RACI-relationships assigned.	0 %	0 %
Level 1	Some awareness of the importance of issues related to the activity. No monitoring is performed. No documentation exists. No activity improvement actions take place.	25 % of RACI-relationships assigned.	20 %	20 %
Level 2	Individuals have knowledge about issues related to the activity and take actions accordingly. No monitoring is performed. No documentation exists. No activity improvement actions take place.	More than 26 % of RACI-relationships assigned. 25 % or less of the identified relationships are in line with COBIT.	40 %	40 %
Level 3	Affected personnel are trained in the means and goals of the activity. No monitoring is performed. Documentation is present. No activity improvement actions take place.	More than 26 % of RACI-relationships assigned. 26- 74 % of the identified relationships are in line with COBIT.	60 %	60 %
Level 4	Affected personnel are trained in the means and goals of the activity. Monitoring is performed. Documentation is present. The activity is under constant improvement. Automated tools are employed in a limited and fragmented way	More than 51 % of RACI-relationships assigned. 51- 99 % of the identified relationships are in line with COBIT.	80 %	80 %
Level 5	Affected personnel are trained in the means and goals of the activity. Monitoring is performed. Documentation is present. Automated tools are employed in an integrated way, to improve quality and effectiveness of the activity	100 % of RACI-relationships assigned. 100 % of the identified relationships are in line with COBIT.	100 %	100 %

Table 1. The metrics for IT governance maturity assessment employed in the proposed analysis framework

As mentioned previously, little support for assignment of maturity levels related to the metrics is provided in Cobit. For the “Activity execution” metric, the generic maturity model defined for Cobit’s processes was transformed to better fit assessment of activities. The maturity levels for the “Assigned responsibilities” metric are assigned in terms of the number of RACI relationships specified for each activity and role (0-25-50-75-100 % assigned), and how well these are aligned to the relationships stated in Cobit (0-25-50-75-100 % assigned according to Cobit). For “Documents in place” and “KPI:s/KGI:s monitored”, a linear assumption of Cobit’s focus on quantity in documentation and collection of metrics was made, and a maturity model that counts the percentage of documents and metrics in place was set up. The proposed metrics allow an organization to assess their performance using a maturity model with well defined levels. The next step is to aggregate the disparate metrics into a single, comprehensive maturity score.

5.2.2 Aggregation of metrics

The metrics are aggregated into maturity scores on three different levels: Activity level, Process level and Enterprise level, c.f. Figure 3. The activity level maturity is calculated as an average of two different metrics. The process level maturity is the average of all underlying activity maturities, plus two more metrics. The enterprise level maturity is likewise the average of the maturities of all underlying processes. We further assume that all metrics have the same weight.

Let us now illustrate how aggregation of metrics is performed with a brief example. The Cobit process PO6: Communicate Management Aims & Directions consists of three activities, c.f. Table 2. Further, nine metrics in terms of Key Performance Indicators, Process Key Goal Indicators, and IT Key Goal Indicators are provided in Cobit, together with three input documents and two output documents. Cobit also recommends what roles should be assigned responsibility and accountability for the activities, and which roles to be consulted and informed about them.

Assume that an organization under evaluation has two of the three activities in place. The activity not in place is therefore assigned level 0 on all metrics. The remaining two activities are assessed to maturity level 2 according to the metric “activity execution” presented in Section 5.2.1. The first of the implemented activities has roles being responsible and accountable for its execution (50% of RACI relations assigned), yet these roles are not the ones suggested in Cobit (0 % assigned according to Cobit). However, the accountability and responsibility for the second activity are assigned just as stated in Cobit (50 % assigned, 50 % assigned according to Cobit). According to Table 1, this results in assignment to maturity levels 2 and 3 regarding the activity execution metric for the two activities respectively. The equivalent activity level maturity for the three activities is calculated according to Table 2. An average activity maturity is also calculated.

	Activity	**Maturity of activity execution**	**Maturity of assigned responsibilities**	**Activity level maturity**
	Establish and maintain an IT control environment and framework	2	2	2
	Develop and maintain IT policies	2	3	2.5
	Communicate the IT control framework and IT objectives and direction	0	0	0
	Average activity level maturity	▨	▨	**1.5**

Table 2. An example of calculation of activity level maturity for Cobit process PO6: Communicate Management Aims and Directions.

Continuing with the example for PO6, three out of five documents listed in Cobit exist within the organization. This equals 60 % or maturity level 3 according to Table 1. Nevertheless, just two of the suggested KPI:s/KGI:s are continuously monitored, which is equivalent of 22 % or maturity level 1. The process level maturity is equal to the average of these two metrics and the average activity maturity according to Table 3.

This corresponds to the analysis framework's formalized translation of separate metrics into a single comprehensive score. The procedure for bundling groups of processes into enterprise level maturity levels follows the same steps. For instance, if processes PO6, PO7 and PO8 are assessed to maturity levels 1.8, 1.8 and 0.5, the average maturity for the group of processes would be 1.4.

	Process name	**Average activity level maturity**	**Maturity of documents**	**Maturity of KPI:s/ KGI:s**	**Process level maturity**
⬟	PO6	1.5	3	1	**1.8**

Table 3. An example calculation of process level maturity. PO6 is the process for communication of management aims and directions.

6 THE PROPOSED METHOD'S FULFILLMENT TO THE REQUIREMENTS

The method for ITG maturity assessment proposed in this paper fulfils the requirements in the following way:

RQ1: Consistency with common conceptions. Cobit is a de facto standard in the field and is often referred to as the assessment framework for ITG. The proposed method is solidly based on Cobit. The requirement is thus fulfilled.

RQ2: Descriptive operationalization. Cobit contains the processes, activities, documents, etc. needed to correctly represent all ITG concerns and the proposed method inherits these concepts from Cobit. Objective assessment is improved by detailing precisely what entities and relations to be modeled. The requirement is fulfilled.

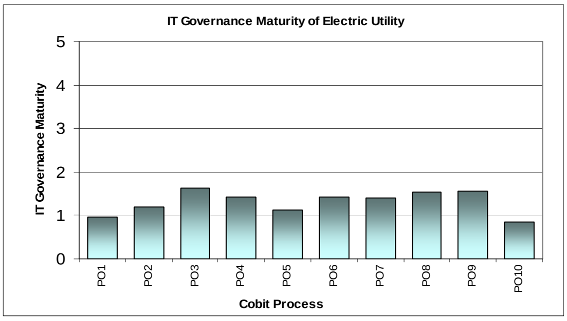
RQ3: Normative operationalization. The proposed method provides a fully transparent and formalized analysis framework that enables aggregation of single metrics to comprehensive maturity scores on process of enterprise level. Requirement fulfilled.

RQ4: Support for efficient data collection. The proposed method provides a modeling language that enables modeling to be separated from analysis. Modeling can be performed by people with little knowledge of the normative aspects of IT governance assessments. Requirement fulfilled.

RQ5: Support for efficient analysis. The analysis framework is fixed and an assessment just requires the organization under evaluation to be modeled. The analysis is made automatically without the need for an experienced analyst. This makes the entire assessment more efficient. Requirement fulfilled.

7 CASE: ASSESSING IT GOVERNANCE MATURITY OF AN ELECTRIC UTILITY

In order to test the proposed method, a case study was carried out. The company under evaluation is a medium-sized company that produces, distributes, and sells energy to 57.000 private and corporate customers in Sweden. The annual turnover of the electric utility is about EUR 120 Million. A small department with six full-time employees has the overall responsibility for enterprise IT, but operation and support is partly outsourced to an external service provider. The purpose of the case study was to show that a person with little previous experience in the field could use the proposed method to assess the level of IT governance at the electric utility. In order to do this, a master thesis student was sent out to perform interviews study relevant documentation. About 15 hours were spent on interviewing five different respondents within the electric utility.



PO1: Define a Strategic IT Plan
PO2: Define the Information architecture
PO3: Determine Technological Direction
PO4: Define the IT Processes, Organization & Relationships
PO5: Manage the IT Investment
PO6: Communicate Management Aims and Direction
PO7: Manage IT Human Resources
PO8: Manage Quality
PO9: Assess and Manage IT Risks
PO10: Manage Projects

Figure 4. The figure details results for an electric utility regarding ten strategically important processes for Planning & Organization according to Cobit.

All processes, activities, metrics, documents and roles and responsibilities in the IT organization (according to Cobit and the described reference model for IT governance) were covered during the interviews. In just a few days, a complete model of the IT organization was created, using the METIS tool for enterprise architecture modeling (Troux Technology 2006). The model was verified by the head of the IT department within the organization, who found data and model representation both accurate and understandable. Then, the entire model of the organization under evaluation, all 34 processes, was subjected to the analysis framework. Since parts of IT operations were outsourced, results for the processes for strategic use of IT were considered most interesting. Results for ten processes from the Plan & Organize domain in Cobit are presented in this paper, c.f. Figure 4.

The analysis takes into account both the maturity of the executed activities, the documentation, the assigned roles, and the number of metrics used. Regarding the case study, it can be said that most activities were executed in a considerable mature way. One conclusion is that the IT department of the electric utility is especially knowledgeable regarding the processes for internal quality management and IT risk management (PO3, PO8 and PO9). Processes with low maturity include IT strategy and project management for IT (PO1 and PO10). The low average maturity of the processes is mainly due to lack of documentation for several processes and scarce use of metrics within the IT organization. This result is however not surprising, since the IT department is quite small and the need for detailed documentation and metrics is limited.

The overall conclusion drawn from the case study was that in was indeed possible for an analyst with little previous experience of Cobit to perform a complete analysis with little effort spent. According to the master thesis student performing the case study, it was an easy and straight forward task to create the models. In another article soon to be published, the entire analysis of the results will be accounted for and discussed more thoroughly.

8 CONCLUSIONS

This paper has proposed an IT governance maturity assessment method designed to overcome the problems of validity, reliability and cost that are commonly associated with such methods today. One of the major benefits is that the person performing the assessment doesn’t necessarily have to be an IT governance expert, since the analysis part is performed automatically. A small case study was performed to test the general goodness of the method. Results show that the proposed method allows for straight forward modeling and analysis of organizations, thus enabling an efficient way to conduct IT governance maturity assessments based on Cobit.

9 REFERENCES

Debraceny, R.S. (2006). Re-engineering IT Internal Controls - Applying capability Maturity Models to the Evaluation of IT Controls. Proceedings of the 39th Hawaii International Conference on System Sciences.

Guldentops, E. (2004). Governing Information Technology through COBIT. In: Van Grembergen, W. (ed.): Strategies for Information Technology Governance. Idea Group Publishing.

van Grembergen, W., S. De Haes and E. Guldentops (2004). Structures, Processes and Relational Mechanisms for IT Governance. In: Van Grembergen, W. (ed.): Strategies for Information Technology Governance. Idea Group Publishing.

Hendersen, J.C. and N. Venkatraman (1993). Strategic Alignment: Leveraging Information Technology for Transforming Organizations. IBM Systems Journal 32 (1), 472-485.

Holm Larsen, M., M. Kühn Pedersen and K. Viborg Andersen (2006). IT Governance – Reviewing 17 IT Governance Tools and Analyzing the Case of Novozymes A/S. Proceedings of the 39th Hawaii International Conference on System Sciences.

Information Systems Audit and Control Association (2005). Control Objectives for Information and Related Technology, 4th Edition.

International Organization for Standardization (2005). ISO/IEC 20000-1 & ISO/IEC 20000-2.

King, G., R.O. Keohane and S. Verba (1994). Designing Social Inquiry. Princeton University Press.

Korac-Kakabadse, N. and A. Kakabadse (2001). IS/IT Governance: Need For an Integrated Model. Corporate Governance 4 (1).

Loh, L. and N. Venkatraman (1992). Diffusion of Information Technology Outsourcing: Influence Sources and the Kodak Effect. Information Systems Research 3 (4), 334-359.

Office of Government Commerce, OGC. (2003). IT Infrastructure Library Service Delivery. The Stationery Office.

Ridley, G., J. Young and P. Carroll (2004). COBIT and its utilization - A framework from the literature. Proceedings of the 37th Hawaii International Conference on System Sciences, Hawaii.

Ross, J.W. (2003). Creating a Strategic IT Architecture Competency - Learning in Stages. MIT Sloan School of Management Working Paper. No 4314-03.

Sallé, M. and S. Rosenthal (2005). Formulating and Implementing an HP IT Program Strategy Using Cobit and HP ITSM. Proceedings of the 38th Hawaii International Conference on System Sciences, Hawaii.

Simonsson, M. and P. Johnson (2006). Assessment of IT Governance – A Prioritization of Cobit. Proceedings of the Conference on Systems Engineering Research. Los Angeles, USA.

Simonsson, M. and E. Hultgren (2005). Administrative Systems and Operation Support Systems – A Comparison of IT Governance Maturity. In proceedings of the CIGRÉ International Colloquium on Telecommunications and Informatics for the Power Industry, Cuernavaca, Mexico.

Troux Technology (2006). METIS EA Modeling Software, http://www.troux.com, accessed June 11.

Warland, C. and G. Ridley (2005). Awareness of IT Control Frameworks in an Australian State Government: A Qualitative Case Study. Proceedings of the 38th Hawaii International Conference on System Sciences, Hawaii.

Weill, P. and J.W. Ross (2004). IT governance – How Top Performers Manage IT Decision Rights for Superior Results. Harvard Business School Press.

Weill, P. and R. Woodham (2002a). State Street Corporation: Evolving IT Governance. MIT Sloan School of Management Working Paper No 4236-02.

Weill, P. and R. Woodham (2002b). Dont Just Lead, Govern: Implementing Effective IT Governance. MIT Sloan School of Management Working Paper No 4237-02.