Proceedings of FIKUSZ '13 Symposium for Young Researchers, 2013, 67-76 pp © The Author(s). Conference Proceedings compilation © Obuda University Keleti Faculty of Business and Management 2013. Published by Óbuda University http://kgk.uni-obuda.hu/fikusz

COBIT 5 and the Process Capability Model. Improvements Provided for IT Governance Process

Alex Pasquini

University of Applied Sciences Northwestern Switzerland (FHNW), School of Business

University of Camerino, School of Science and Technology, Computer Science Division

alex.pasquini@students.fhnw.ch

Emidio Galiè

University of Applied Sciences Northwestern Switzerland (FHNW), School of Business

University of Camerino, School of Science and Technology, Computer Science Division

emidio.galie@students.fhnw.ch

Abstract: IT governance and management in an enterprise plays an important part in generating value for the stakeholders [1]. COBIT 5 is a framework for the governance and management of IT enterprises. In 2012 the latest version of this framework was released introducing important features. One of those features is the evolution from COBIT 4.1 Maturity Model to COBIT 5 Process Capability Model. This paper will deal with the evolution of this model and will analyse the attributes which characterise the model in the recent version of the framework. What are the improvements that COBIT 5 provides for IT governance processes? Starting from a general overview of this framework, the structure of the Process Capability Model will be analysed in detail in this paper. Then, a comparison with the Maturity Model of the previous version of the COBIT framework will be discussed. At the end of this paper, it will be seen that the new Process Capability approach results in an improvement of the assessment process; and in particular, in the formality and the rigor of the assessment. With the Process Capability approach a major focus on the purpose of the processes is implemented resulting in a better alignment with the current best practices such as ITIL and TOGAF.

Keywords: COBIT 5, COBIT 4.1, COBIT, Process Capability Model, Maturity Model, Process Assessment.

1 Introduction

The increasing number of regulations and standards requiring compliance makes the governance and the management of enterprise information technology (IT) more important. In particular, as reported by [2] "With Sarbanes-Oxley (SOX) in the U.S. and other legislation enacted worldwide, effective governance over IT has become law for many companies". For this reason more and more frameworks have been developed to respond to continuously change business needs. Control Objectives for Information and Related Technology (COBIT) is a framework created by Information Systems Audit and Control Association (ISACA) for IT management and IT governance and is now extensively used by business [3]. ISACA is a recognised worldwide leader in IT governance, control, security and assurance [4].

This paper will start with a literature review in section 2, commenting on the information retrieved and the general viewpoint adopted. In section 3 the evolution of COBIT will be discussed, analysing the domains in which the various versions of this framework have operated since the first release in 1996 [6], [7].

Then, in section 4, the Maturity Model of COBIT 4.1 [17] and the Process Capability Model of COBIT 5 [10] will be introduced and the new features will be highlited. Finally, in section 5, the results of this approach will be considered, answering the research question: "What are the improvements that COBIT 5 provides for the IT governance processes maturity?"

2 Literature review

IT governance and management is a continuously evolving area because of the increasing number of regulations requiring compliance, and the need to lower risks and avoid actions related to non-compliance. COBIT is the framework for governance and management of IT developed by ISACA, which evolved into the current version - COBIT 5 released in 2012. In this paper the changes in assessment process are analysed, especially the change from the Maturity Model used in COBIT 4.1 to the Process Capability Model implemented in the current version, in order to understand the advantages of the new model.

Except for the documentations provided by ISACA to their members, there is a lack of important documentation from other sources regarding the latest version of the framework. On the other hand, the documentation provided by ISACA gives useful details about structures and documents used by COBIT 5. For this reason, this paper is based on ISACA documentation such as [8]–[10].

Another consideration to bear in mind, is that all the articles listed in the "Reference" section are aligned with the contents of ISACA documentation. Finally, some documentation about the mapping of COBIT 5 Process Capability Model with other standards was retrieved, but because the main aim of this paper is to compare the model used in COBIT 4.1 (Maturity Model) and in COBIT 5 (Process Capability Model) and to underline the improvements in COBIT 5, that documentation is not taken into consideration.

3 The evolution of COBIT

ISACA was founded in 1967, by individual industries working in the same field. Then, in 1969 they were incorporated as Electronic Data Processing (EDP) Auditors Association [11]. Members of ISACA worked together to develop and create best practices, one of which being the COBIT framework. The first version of this framework was released in 1996 [6], [7], and was called "Control Objectives for Information and related Technology", covering the area of audit [12]. The second edition with enhancements on control assessment was released in 1998 [13]. The third edition was released two years later, and according to [12] "The big change came with the publication of COBIT Third Edition, with its business objective orientation. At this time, COBIT was termed as an IT management framework. The third edition identified that an organization needs IT not just for information processing, but also to achieve business objectives". In 2005 ISACA introduced a new, fourth version of COBIT with a clear focus on IT governance [14]. A further version of this framework is COBIT 4.1, released in 2007, accepting the generally used frameworks such as "IT Infrastructure Library (ITIL)", "ISO 27000 series" and "Capability Maturity Model® Integration (CMMI)" [5], [15]. The current version of the framework, COBIT 5, was released in 2012. It is built upon the previous version of the framework and two complementary frameworks from ISACA (Val IT and Risk IT); and is aligned with the current best practices such as ITIL and TOGAF [9].

4 From COBIT 4.1 Maturity Model to COBIT 5 Process Capability Model

In this section, the Maturity Model of COBIT 4.1 and the Process Capability Model of COBIT 5 will be compared. These two models are used in the related frameworks to understand the state of internal IT-processes, to assess them ("as-it" maturity of the enterprise), to define the requirements for the evolution of those processes ("to-be" maturity of the enterprise) and to evaluate the gap between these two views.

This kind of method was used in COBIT 4.1 and an evolved version is implemented in the current framework. For this reason users of COBIT 4.1 should be familiar with the Process Capability Model in COBIT 5, since the assessment processes of the two versions use different, but similar criteria.

4.1 COBIT 4.1 Maturity Model

With the introduction of COBIT 4.1 in 2007, a new Maturity Model was proposed. According to [16], this Maturity Model, whose aim is to improve the IT processes, assesses the process maturity in order to define the future level of process maturity needed to achieve (target maturity level) and finally evaluates the gap between these two levels.

To do this, COBIT 4.1 uses a range of levels to assess the maturity as shown in Figure 1. According to [17], these levels are:

Level 0: Non-existent. An internal control is not required for the company based on culture or internal mission. The related risks and deficiencies are considered to be very high.

Level 1: Initial/ad hoc. An internal control is considered necessary. However this internal control is ad hoc and not organised. The employees are not aware of their responsibilities. Deficiencies are not identified.

Level 2: Repeatable but intuitive. Controls are implemented but not documented, since they depend on the knowledge and motivation of individuals. The employees may not be aware of their responsibilities.

Level 3: Defined. As at the previous level the controls are implemented, but in this level an adequate documentation exists. Unlike level 2, the employees are aware of their responsibilities for control.

Level 4: Managed and measurable. The risk management and the implementation of internal controls are effective. The evaluation of internal controls is formally documented based on periodic reviews. However also with these efforts, not all the issues are identified.

Level 5: Optimised. Risks and controls are managed by a good program that provides continuous and effective control and risk issues resolution. The enterprise practices encompass internal control and risk management. Unlike at the other levels, the employees are pro-actively involved in controlling the improvements produced.

As shown in Figure 1, in the COBIT 4.1 Maturity Model there are six different generic Maturity Attributes (MAs), which should be applied for each process. These attributes provide more details in the process view. Indeed the results of the assessment done on IT processes are based on these six attributes. They are not the only aspects considered in the assessment. In fact each of COBIT 4.1's IT process has a number of Process Controls and Control Objectives for achieving effective control on IT processes themselves, "control" meaning the alignment with policies, procedures, practices and organisational structures.

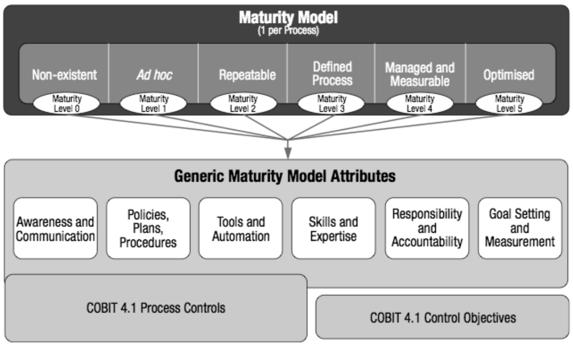

Figure 1
COBIT 4.1 Maturity Model [10]

4.2 COBIT 5 Process Capability Model

In COBIT 5 the Maturity Model is changed, assigning more importance to the processes. The task of the new Process Capability Model is the same as the Maturity Model, but the structure of the framework is modified. As seen in Figure 2, the number of levels for assessing a process is the same (six) compared to the Maturity Model, although the name, the meaning, and especially the attributes for assessing a process are different. According to [10] the two frameworks could seem similar, but there are differences in scope and intents. The difference of intents between levels is linked to the significant focus on the achievement of the IT processes purposes and a more formal assessment brought by the new framework. Moreover, according to [10], in practice, the score an enterprise can achieve with COBIT 4.1 Maturity Model usually is greater than or equal to the score reachable with COBIT 5 Process Capability Model. This will be clearer after the explanation of the six levels for assessing the IT processes in COBIT 5.

The assessment task in COBIT 5 is based on ISO/IEC 15504 underlining the strong alignment of this framework with the most generally accepted best practices and standards.

According to [10], the six levels of the COBIT 5 Process Capability Model are:

Level 0: Incomplete process. The process is not placed or it cannot reach its objective. At this level the process has no objective to achieve. For this reason this level has no attribute.

Level 1: Performed process. The process is in place and achieves its own purpose. This level has only “Process Performance” as process attribute.

Level 2: Managed process. The process is implemented following a series of activities such as planning, monitoring and adjusting activities. The outcomes are established, controlled and maintained. This level has “Performance Management” and “Work Product Management” as process attributes.

Level 3: Established process. The previous level is now implemented following a defined process that allows the achievement of the process outcomes. This level has "Process Definition" and "Process Deployment" as process attributes.

Level 4: Predictable process. This level implements processes within a defined boundary that allows the achievement of the processes outcomes. This level has "Process Management" and "Process Control" as process attributes.

Level 5: Optimising process. This level implements processes in the way that makes it possible to achieve relevant, current and projected business goals. This level has "Process Innovation" and "Process Optimisation" as process attributes.

In COBIT 5 to achieve a given level of capability, the previous level has to be completely achieved.

There is a big gap between "Level 0: Incomplete process" and "Level 1: Performed process". Indeed, achieving the first level means that a process largely achieves its task. Thus, according to [10] "In this assessment scheme, achieving a capability level 1, even on a scale to 5, is already an important achievement for an enterprise". Furthermore, according to [10] "In the COBIT 4.1 Maturity Model, a process could achieve a level 1 or 2 without fully achieving all the process objectives", this is not true in the COBIT 5 Process Capability Model, where there would be a lower score of Level 0 or Level 1. This explains why in COBIT 4.1 Maturity Model the same process does not attain a lower result compared to the assessments done by COBIT 5 Process Capability Model, but achieves the same or, at least, a greater result.

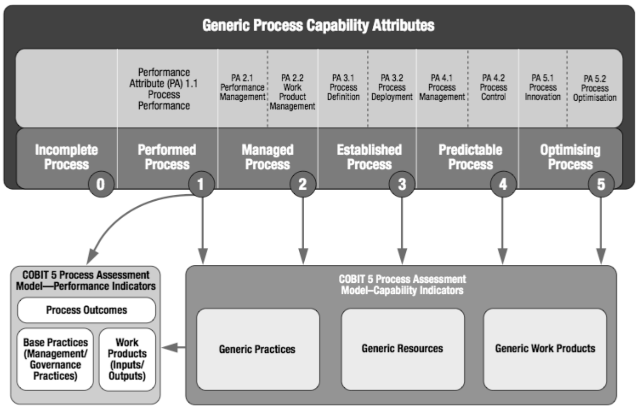
Generic Process Capability Attributes
Performance Attribute (PA) 1.1 Process Performance
PA 2.1 Performance Management
PA 2.2 Work Product Management
PA 3.1 Process Definition
PA 3.2 Process Deployment
PA 4.1 Process Management
PA 4.2 Process Control
PA 5.1 Process Innovation
PA 5.2 Process Optimisation
Incomplete Process
0
Performed Process
1
Managed Process
2
Established Process
3
Predictable Process
4
Optimising Process
5
COBIT 5 Process Assessment Model—Performance Indicators
Process Outcomes
Base Practices (Management/ Governance Practices)
Work Products (Inputs/ Outputs)
COBIT 5 Process Assessment Model–Capability Indicators
Generic Practices
Generic Resources
Generic Work Products

Figure 2

COBIT 5 Process Capability Model [10]

As shown in Figure 2, the Process Capability Model bases its assessment methodology on six levels. Except for the first level (Level 0) in which the goal of the process is not achieved, in all the other levels there is at least one attribute. Thus in order to reach a level, an IT process has to fully achieve the related attributes, which are based on indicators. In particular Level 1 has to fit capability indicators as well as performance indicators, which check the process outcomes, the alignment with the best practices and the resources used. This is because in order to reach Level 1, the purpose of the process has to be achieved. In the higher levels the performance indicators are not involved, because moving beyond Level 1 means that they have been fully achieved. Thus, in the assessment process, from the third level (Level 2) to the last level of maturity (Level 5), only the capability indicators are always involved. They are required to assess the capability level of an IT process. Indeed the purpose of capability indicators is to evaluate the capability of the processes to achieve specific objectives.

5 Results

The introduction of COBIT 5, according to [8], [10], has resulted in new changes. One of those was the transition from COBIT 4.1 Maturity Model and COBIT 5 Process Capability Model explained in the previous section. This has introduced improved features for IT governance processes, according to [18], relating to the non-subjective assessment and evidences required by the approach used in ISO/IEC 15504, that were not required by the Maturity assessment used in COBIT 4.1. According to [10], this approach reduces the resources used by COBIT 4.1 Maturity Model approach such as generic maturity models, process maturity models, control objectives and process controls, for analysing and assessing processes. Moreover, according to [10] the contents are simplified, improving the user friendliness of this approach.

As result, the reliability and repeatability of process capability assessment activities and evaluations have been improved, reducing disagreements on assessments [10].

A further feature that this Process Capability Model has brought is the improved focus on the goal of the process, assessing the achievement of it and the outcomes expected. The assessment is more rigorous and formal, adding more value to this approach as compared to the approach used in COBIT 4.1.

As previously remarked in section 3, since COBIT 5 is built upon common frameworks and best practices, compliance is assured with the support of these generally accepted process assessment standards [9]. In particular COBIT 5 bases its assessment process on ISO/IEC 15504 process capability assessment, making the results of the evaluation process more formal and more focussed on the process purpose. For this reason strong support for the process assessment is generated in the market, providing the opportunity to obtain certifications such as those provided by International Assessor Certification Scheme (iNTACS™) as provisional, competent or principal assessor[1].

Answering the research question, the evolution of COBIT 5, with a new approach for process capability, results in the aforementioned improvements, generating better opportunities for enterprises to identify deficiencies in their internal processes through

[1] For more information visit: https://www.isqi.org/de/certview.html?CertificateID=6

Process Attributes (Pas) such as Process Performance, Management and Definition, with the new IT processes specified in Process Reference Model of COBIT 5 and to make a better plan for their evolution based on the assessment and on the desired level of capability. As explained before in this section, the new approach for assessment is based on evidences and it cannot be subjective (while in COBIT 4.1 Maturity Model, the assessment could be subjective since it is not based on the achievement of the processes purpose, but only on maturity attributes which are evaluated subjectively). In this way the forecast of further implementation cannot make such subjective mistakes because the assessment is based on a formal standard such as ISO/IEC 15504. Moreover, according to [10] approaches for a correct implementation (Life Cycle Approach and Road Map) are provided by ISACA which encompass the Process Capability Model for the assessment, and drive the enterprise towards an integrated implementation of the "to-be model".

Conclusions

IT governance and management is gaining more importance in generating value for stakeholders, and with the COBIT 5 Process Capability Model a new approach for managing risks and process improvements is presented. ISACA, with the COBIT framework, is trying to provide a good solution in the area of IT governance and management. With the introduction of Sarbanes-Oxley (SOX) regulation by U.S., systems for managing and controlling the IT risks were required.

In this research paper, in section 4 it was recognised COBIT 5 Process Capability Model was recognised as a good approach to:

- Assess the capability level of a process ("as-it maturity"): due to the ISO/IEC 15504 process assessment with the nine PAs and the six capability levels;
- Target a new capability level ("to-be maturity"): Based on financial analyses and opportunities that could result in improvements;
- Analyse the gap between them, structuring a plan to reach the desired level of capability for the given process.

This paper starts with a research question: "What are the improvements that COBIT 5 provides for IT governance processes?" The answer to this question was given in section 5. In particular the improvements made with the transaction from COBIT 4.1 to COBIT 5 were underlined. Indeed the COBIT 4.1 Maturity Model and the COBIT 5 Process Capability Model were compared. The result of this comparison, according to [10], [18], shows that the new approach, used in the current framework, provides advantages deriving from the adoption of ISO/IEC 15504 standard such as less resources involved in the assessment process, simplified contents, reliability and repeatability of process capability assessment activities and evaluations improved, more rigorous and formal assessment, alignment with best practices and generally accepted standards.

Moreover, COBIT 5 Process Capability Model provides a support for reusing the Maturity Attributes in the new approach, trying to help companies which have invested in the previous version of the framework [10].

Further research can focus on the development of a mapping framework for the compatibility of assessments done with COBIT 4.1 with the COBIT 5 approach. In fact the existing methods are either inefficient or they map only partially. A good approach to map these two methods would increase the compatibility of the latest version of this framework, resulting in costs savings for those companies who use COBIT 4.1.

Acknowledgement

This work is supported by the University of Applied Sciences Northwestern Switzerland (FHNW), School of Business, and by the University of Camerino, School of Science and Technology, Computer Science Division. In particular the authors thank professor P.M. Asprion for her support in this work.

References

[1] P. Weill and J. W. Ross: IT Governance: How Top Performers Manage IT Decision Rights for Superior Results, 2004, pp. 14–18.

[2] G. Hardy: Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges, Information Security Technical Report, vol. 11, no. 1, 2006, pp. 55–61.

[3] N. Kim, R.-J. Robles, S.-E. Cho, Y.-S. Lee, and T. Kim: SOX Act and IT Security Governance, in Proceedings of International Symposium on, Ubiquitous Multimedia Computing, October 13-15, 2008, pp. 218–221.

[4] ISACA: COBIT 5: Implementation, 2012, p. 2.

[5] ITGI: COBIT 4.1 Excerpt, 2007, p. 9.

[6] E. Guldentops, W. Van Grembergen, and S. De Haes: Control and governance maturity survey: establishing a reference benchmark and a self assessment tool, Information Systems Control Journal, vol. 6, 2002, pp. 32–35.

[7] E. Guldentops and S. De Haes: COBIT 3rd Edition Usage Survey: Growing Acceptance of COBIT, Information Systems Control Journal, vol. 6, 2002, pp. 25–31.

[8] ISACA: COBIT Five: Implementation, 2012.

[9] ISACA: COBIT 5, C5 Workgroup Member, 2012, p. 29.

[10] ISACA: COBIT Five: A Business Framework for the Governance and Management of Enterprise IT, 2012, pp. 41–45.

[11] ISACA: History of ISACA. [Online]. Available: http://www.isaca.org/About-ISACA/History/Pages/default.aspx

[12] A. Kadam: The Evolution of COBIT, CSI Communications, 2012, pp. 21–22.

[13] ITGI: CobiT Mapping: Overview of International IT Guidance, 2nd Edition, 2006, pp. 8–15.

[14] ITGI: COBIT Mapping: Mapping ISO/IEC 17799:2005 with COBIT 4.0, 2006, p. 6.

[15] ITGI: Cobit 4. 1, 2007, p. 9.

[16] ITGI: Cobit 4.1, 2007, p. 18.

[17] ITGI: Cobit 4.1, 2007, p. 59.

[18] ISACA: COBIT Assessment Programme Frequently Asked Questions (FAQs). [Online]. Available: http://www.isaca.org/Knowledge Center/cobit/Pages/COBIT-Assessment-Programme-FAQs.aspx.