Proceedings of the Federated Conference on Computer Science and Information Systems pp. 961–964 DOI: 10.15439/2017F410 ISSN 2300-5963 ACSIS, Vol. 11

IT Governance Program and Improvements in Brazilian Small Business: Viability and Case Study

Daniel A. M. Aguillar, Isabel Murakami, Pedro Manso Junior
Instituto de Pesquisas Tecnológicas de São Paulo – IPT
Av. Almeida Prado, 532 - Butantã, São Paulo – SP - Brazil
Email: danielaguillar@yahoo.com.br,
iaadefm@hotmail.com, pedro.manso@uol.com.br

Plinio Thomaz Aquino Jr.
Centro Universitário FEI
Fundação Educacional Inaciana Pe. Saboia de Medeiros
Av. Humberto A. Castelo Branco, 3972 - 09850-901
São Bernardo Campo - SP – Brazil
E-mail: plinio.aquino@fei.edu.br

Abstract—Small companies have the potential to be agile, flexible and informal because they are usually formed by few members. This usually creates more synergy among these professionals because they tend to have more than a single role inside the company. With such role versatility, it is understandable that those professionals have to multitask/split their working hours among different kinds of demands: that may cause difficulties in planning, development, verification and improvement of internal processes. This article brings a case study where the COBIT 5.0 toolkit (Process Assessment Model) was used to identify internal processes that needed improvement within the studied company. In order to improve the selected processes, ABNT NBR ISO/IEC 12207 was tailored concerning the company's needs. Additionally, it was applied the PDCA cycle of continuous improvement and it was also proposed the adoption of an agile method, SCRUM, to integrate internal activities and processes.

I. Introduction

THIS article presents a viability case study for the application of an Information Technology (IT) corporative governance program in a small software development company. [2] shows metrics about Apps development projects – about 56% concluded within agreed deadlines and 68% within agreed budget. In order to meet deadlines and have better budget control, IT area must be efficient, aligned with business goals, and solutions must not only meet quality requirements but also have low cost and adaptability[19][2]. IT alignment with business goals can be achieved adopting a Governance model. COBIT (Control Objectives for Information and Related Technology) is a De-fact standard used to provide IT area with a governance model and it helps understanding and managing its associated risks [17]. IT efficiency can be improved with well-defined processes and standardization, using ISO/IEC 12207[8], the international standard for software life cycle processes[19]. Process should be easily adaptable as business' needs change. The adoption of agile development is increasing due to the need of fast adaption to changes. The most used agile method nowadays is Scrum [17][18][23]. Considering the Governance context (COBIT), the development model (ISO/IEC 12207) and SCRUM method, this article aims to investigate the application viability of COBIT, ISO/IEC 12207 and SCRUM in the context of a small company (up to 9 people, statistic average in Brazil) [1]. COBIT, ISO/IEC 12207 and SCRUM should be tailored considering a small company's resources limitation, where it is common to find human resources assuming multiple roles while working on different projects at the same time. The small IT Brazilian company analyzed in this case study, identified as "studied company" had reported the following main problems: rework due to scope change, consecutive delays due to lack of stakeholders' commitment, stakeholder's change and/or multiple stakeholders with inadequate communication. If not well managed, such problems can imply in financial loss, lack of productivity, frequent re-negotiations, and negative impact in other projects and human resources reallocation. Therefore, affecting commercial, development, creation and quality assurance areas – company's key areas.

II. Research goal

The goal of this study is to assess the application viability of COBIT 5.0 and consequent verification, analysis and proposition of improvements in a small companies' context, providing a viability analysis of the challenges and benefits observed when applying COBIT, ISO/IEC 12207 and SCRUM in a small company context. The primary analysis will be done with COBIT toolkit version 5.0. The application of this framework aims to verify which are the main processes influenced by the cited problems – knowing such processes will enable the application, within the right adherence level, of standards and/or techniques based in good practices of IT governance and software engineering.

III. Expected contributions and Method

It is possible to cite as expected contributions of this study internal processes and governance improvement, and the fact that this study is related to a less studied domain: small companies – Showing the application viability of such practices in this context. The method used in this study has the following activities: (1) Collection of information and problematic situations; (2) Analysis of collected data; (3) Application of COBIT 5.0 framework; (4) Bibliographic

IEEE Catalog Number: CFP1785N-ART ©2017, PTI

survey for possible solutions; (5) Analysis and proposition of hypothetical solution; and (6) Development of paper that documents adopted procedures and obtained conclusions.

IV. Related Work

Several researchers have investigated the harmonization of Governance models with agile models of development. [16] used concepts of COBIT, PRINCE2 and SCRUM to propose the addition of security tests requirements and penetrations tests into the agile development lifecycle. [14] proposed a software acquisition model aligned with COBIT, ITIL, PDCA concepts for continuous improvement, adding concepts as daily meetings from Scrum and portfolio management from SAFe. [22] observed the migration of a company to agile models from Waterfall, while complying with COBIT – listing challenges and adopted solutions, while losing the big picture in design, a problem solved with the addition of a zero sprint step following a formal approval process. Similarly to such studies, this work has combined COBIT, PDCA and SCRUM, however using a different approach, adding COBIT to identify which processes should be improved on a context of small to medium enterprises, using ISO 12207 for the full software development life cycle and PDCA for continuous improvement. In order to combine Governance control over the agile model, researchers had worked on mapping COBIT process with SCRUM activities. [7] mapped COBIT controls with the development processes of understanding requirements, designing, building, testing and implementing solutions to make agile projects comply with Sarbanes Oxley regulatory requirements. [24] validated their proposed model AGIT (AGIle software developmenT), which includes measurement of Scrum-based software development, with information systems auditing criteria, as described in COBIT. [4] observed the impact of applying control over the project context and over the team communication either using formal control, based on performance evaluation strategy and Informal control, based on social and people strategies. [3] researched metrics that could provide IT management with information regarding progress of scrum-based software development process not harming SCRUM's agility. This work has also mapped COBIT process with the ISO/IEC 12207 processes and SCRUM model.

V. Case study

A. Problems analysis – causes and effects

It was necessary to collect information and understand the processual problems shown by this company in order to enable its analysis and consequent improvements/solutions proposition. The method used to analyze all problems consisted of:

1. Brainstorm: Informal meetings with the board of directors (2 members responsible for the management of the Marketing, Sales, Operations, Finances) and the technical team (3 members that work assuming multiple roles during software's lifecycle) in order to detect the main problems affecting company's management and operations;

2. Data Collection analysis: All the main topics discussed during the brainstorm were analyzed and the main problematic situations detected were:

A: Rework due to scope change;

B: Delays due to lack of stakeholder's commitment;

C: Stakeholders change and/or multiple stakeholders;

D: Money loss due to delays in projects and company's unavailability to work in new projects;

E: Lack of productivity due to extra work caused by unexpected scope changes;

F: Frequent renegotiations due to inadequate process and communication, and scope change;

G: Negative impact in other projects;

H: Human resources reallocation.

3. Brainstorm: Meetings with the board of directors to identify the possible root causes and the effects of each problematic situation detected;

4. Cause-effect matrix: Problematic situations were classified into causes or effects of other problems and distributed in a cause-effect matrix. The following matrix shows causes (C) and their effects (E):

Table I. Cause-effect matrix[1]

CAUSE EFFECT	A-2	B-2	C-2	D-2	E-2	F-2	G-2	H-2	TOTAL CAUSES
A-1	-	E	E	C	C	C	C	C	**5**
B-1	C	-	E	C	C	C	C	C	**6**
C-1	C	C	-	C	C	C	C	C	**7**
D-1	E	E	E	-	C	E	E	C	2
E-1	E	E	E	E	-	E	E	E	0
F-1	E	E	E	C	C	-	C	C	4
G-1	E	E	E	C	C	E	-	C	3
H-1	E	E	E	E	C	E	E	-	1

[1] Read the matrix as follows: e.g. A-1 is cause/effect of B-2. Grey cells represent the selected main causes.

After building the cause-effect matrix, an established criterion was applied to allow the identification of the main causes among all problems. The criterion was: the problematic situation should cause at least 70% of problems. The goal was to define root problems/major causes: "A", "B" and "C" were found as such. The actual development model is based on the waterfall model. The process is defined as follows: initial scope analysis and alignment between it's internal manager and stakeholder; characterization of necessary documentation, development, tests and delivery - in modular increments. When a module is delivered, the stakeholder might not be the same who did the initial request, his need might have changed or due the lack of alignment during the module development, it might not be what he was expecting (problematic situations "B" and "C"). This will cause the problematic situation "A".

Additionally, whenever an alignment is needed, meetings are scheduled without any pre-determined periodicity as there are no formalized alignment milestones. Considering the need to generate more commitment from stakeholders, the previously proposed adoption of an agile method can be cogitated as an essential part of the solution. This may help focusing on scope's alignment and delivery validations due to frequent alignment during development process.

B. COBIT 5.0 framework application

This framework was conceived for technology information management. Its application involves business requirements analysis considering: effectiveness, efficiency, integrity, availability, compliance and trustability. Its results bring a panoramic view on the general maturity level of the company's IT area, helping to understand what needs to be done to reach higher levels.

COBIT 5.0 framework was applied addressing the previously cited problems - the assessment was done for every process described in the framework. It stablishes 6 maturity levels, on a 0 to 5 scale.

There was an initial process of governance being executed to ensure the governance setting and maintenance (EDM01 – Rated: Level 1), but it was not being properly managed/maintained - resulting in a lower maturity level.

Value optimization governance (EDM02 – Rated: Level 3) was being managed and had a defined process, but needed well-defined quality attributes to measure its effectiveness.

Risk optimization governance (EDM03 – Rated: Level 2) was being managed at the start and end of projects, but lacked management and measurements during its life cycle.

The budget and costs management process (APO06 – Rated: Level 4) establishes measuring points during the process, to provide costs monitoring and control for the full life cycle of the project.

The positive aspect regarding quality management governance (APO11 – Rated: Level 3) lies in the establishment of more rigorous processes during software development (direct or indirectly).

A bigger level of quality control should be assured by verifying, validating and making revisions in partnership with stakeholders. This would mitigate uncovered problems in quality metrics that were found during COBIT's application.

Risk management governance (APO12 – Rated: Level 2) should be continuous, during the entire project's life cycle. There is a stablished process, but it's not managed. Each risk must be analyzed and proper actions should be taken (avoiding, assuming, reducing or transferring risk) and documented.

Requirement's definition governance (BAI02 – Rated: Level 2) can be improved by using a well-defined acquisition process, suggesting a process to the acquirer (if he does not have it already). Other project's phases will also suffer impact such as: provision, development, maintenance, documentation, quality assurance, verification, validation, joint review and management.

Upon the establishment of a clearer and more well-defined process, operations management governance (DSS01 – Rated: Level 3) can be more complete, by controlling and monitoring more crucial aspects about projects. To improve these processes - requirements, risks and costs must be traceable and documented. To reach this goal, it was suggested the adoption of an ALM (Application Life Cycle Management) tool that automatically registers these steps. A small company's team cannot spend time with bureaucracy that can be automated.

VI. Analysis and solution hypothesis

Many studies were considered [4][5][6][20][21] for the choice and proposition of a viable solution for the studied company. It was found as a viable solution the definition of an adherence level to the ISO/IEC 12207 standard[8]; the incorporation of SCRUM [9][10][13][15] and the implementation of continuous improvement cycle with PDCA [11][12]. Cycle-based processes, based in a study that shows how to apply ISO/IEC 12207 with SCRUM and Agile Methods [15]. Please, view Appendix for full details in this section.

VII. Research and solution proposition: ISO/IEC 12207, PDCA Cycle and SCRUM

As a technical standard reference, it was adopted the ISO/IEC 12207 [8]. The decision for SCRUM was taken based on study [6]. To reach an agile process, it was also recommended to follow the Agile manifesto and its key principles[9].

In order to properly adapt the ISO/IEC 12207 [8], it was used some criteria that is fully explained in the full article. ISO/IEC 12207[8] sub-processes were selected considering the previously mentioned criteria and adaptations were made to it, relating to it SCRUM activities and the affected COBIT processes. Please, view Appendix for full details in this section.

VIII. Conclusion

In this case study of a small company, it was applied the COBIT 5.0 framework in order to identify which IT goals impacting processes needed improvement.

After improving selected processes, ISO/IEC 12207 was adapted according to the company's needs, and it was also suggested the adoption of PDCA cycle for continuous improvement along with SCRUM to organize company's development process.

The application of COBIT 5.0 in this company was complex, because small companies usually don't have specific departments to manage their internal processes. Every roles and attributions, in general, are treated by a reduced amount or people, that accumulate roles, mixing activities in different processes.

It was also noticed that some activities and processes such as the monitoring of costs and risks (during the project's life cycle) were not being formally executed.

Although the company was aware of the consequences and impacts of scope changes in the project, there were no formalized processes to tackle this problem in order to standardize decisions in such scenarios. During the development of this case study it was verified that COBIT 5.0 governance framework when applied in a small company's context, might be challenging, because it requires some adaptions (given the deepness of its analysis) such as: lowering of its high complexity (may be hard to understand and use it), having enough time and human resources on getting it to a reduced scope (for analysis) and bringing together the high volume of information/necessary resources for a precise diagnostic.

It's possible to imply that these might be challenging situations, because in a small company context, there is a reduced amount of people to execute certain tasks, and they end up accumulating responsibilities regarding some processes, that may have different maturity levels.

This research's goals can be defined as attained: It was verified as viable the diagnostic of a small company's IT governance using COBIT, identifying processes that impacted strategic goals and proposing solutions as the definition of formalized processes, based on ISO/IEC 12207. The PDCA cycle along with SCRUM contributed to the improvement process and it will be useful enabling the company to adopt a continuous delivery tactics, gaining more competitiveness in the market.

This study was limited to processes related to software engineering in ISO/IEC 12207 and IT governance impacting solutions were proposed. These propositions of improvement on processes involved the establishment of a set of controls and processes with positive impacts in company's management, helping it achieving higher maturity levels.

Concluding, an objective and selective process view is obtained by the application of COBIT framework and it's possible to adopt standards and patterns in a tailored level of adherence and complexity within processes, enabling better processes and reduction of efforts/costs – mainly in the studied context.

APPENDIX

This paper and the study that was made is extensive. Due to paper's space restraints, the full paper was published in the following internet address for further reading with more details regarding problem analysis, solution hypothesis and paper's contributions:

http://www.fei.edu.br/~plinio.aquino/cobit_scrum/

ACKNOWLEDGMENT

Special thanks to professors Antonio Rigo, PhD. and Gianni Ricciardi, MSc. that conducted the IT governance classes and helped providing important information and insights on IT governance for this article. We thank FAPESP (São Paulo Research Foundation) for financial support.

REFERENCES

[1] SEBRAE, "Micro e Pequenas Empresas em Número." Available at: http://www.sebraesp.com.br/index.php/234-uncategorised/institucional/pesquisas-sobre-micro-e-pequenas-empresas-paulistas/micro-e-pequenas-empresas-em-numeros

[2] J. K. Guevara, L. Hall and E. Stegman, "IT Key Metrics Data 2014: Key Applications Multiyear." Gartner. December 16th, 2013.

[3] G. Concas, M. Marchesi, G. Destefanis, R. Tonelli. "An empirical study of software metrics for assessing the phases of an agile project." International Journal of Software Engineering and Knowledge Engineering 22, no. 04 (2012): 525-548. DOI: 10.1142/S0218194012500131

[4] J. S. Persson, L. Mathiassen, I. Aaen. "Agile distributed software development: enacting control through media and context." Information Systems Journal 22, no. 6 (2012): 411-433.Persson, Mathiassen and Aaen (2012). DOI:10.1111/j.1365-2575.2011.00390.x <link: dx.doi.org/10.1142/S0218194012500131>

[5] Standish Group International Inc., "Extreme Chaos Report", 2001. Available at: https://courses.cs.ut.ee/MTAT.03.243/2013_spring/uploads/Main/standish.pdf

[6] F. McGovern, "Managing Software Projects with Business-Based Requirements." IEEE Software. IEEE Computer Society. IT Professional, Volume:4, Issue:5. 2002. Available at: http://ieeexplore.ieee.org/xpl/abstractAuthors.jsp?arnumber=1041174 - DOI: 10.1109/MITP.2002.1041174

[7] S. Gupta. "SOX Compliant Agile Processes." In Agile, 2008. AGILE'08. Conference, pp. 140-143. IEEE, 2008.Gupta (2008). DOI 10.1109/Agile.2008.48

[8] ABNT – ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. "NBR ISO/IEC 12207 – Tecnologia de informação - Processos de ciclo de vida de software." Rio de Janeiro: ABNT, 1998, 35 p. Available at: http://aulasprof.6te.net/Arquivos_Aulas/06-qualidade_Soft/ABNT_NBR_ISO_12207.pdf

[9] M. Fowler, et al, "Manifesto for agile software development" Available at: http://agilemanifesto.org

[10] SCRUMSTUDY. "A Guide to the SCRUM Body of Knowledge - SBOK GUIDE". Phoenix, Arizona, USA: VMEdu, Inc., 2013.

[11] Quality Assurance Mentor. "*PDCA Cycle.*" Available at: http://www.quality-assurance-mentor.com/software-quality-assurance.html

[12] Reserva em revista. "Ciclo PDCA." Available at: http://necs.preservaambiental.com/ciclo-pdca-abordagem-de-processo-e-escopo-do-sistema-de-gestao-ambiental/

[13] C. Larman "Agile & Iterative Development: A Manager's Guide." Addison-Wesley Professional. ISBN 0-13-111155-8. 2004.

[14] M. S. Silva. "GAIA Modelo de maturidade para aquisição de software". Universidade Estadual de Londrina, Paraná, Brazil. 2016.

[15] Irrazabal, et al, "Applying ISO/IEC 12207:2008 with Scrum and Agile Methods", Universidad Rey Juan Carlos, Madrid, España. 2011.

[16] M. Tomanek, T. Klima. "Penetration Testing in Agile Software Development Projects." arXiv preprint arXiv:1504.00942 (2015). DOI:10.5121/ijcis.2015.5101

[17] N. Ozkan. "Risks, Challenges and Issues in a Possible Scrum and COBIT Marriage." In *Software Engineering Conference (APSEC), 2015 Asia-Pacific*, pp. 111-118. IEEE, 2015. - DOI: 10.1109/APSEC.2015.29

[18] P. Bunyakiati and P. Surachaikulwattana. "Fit between Agile practices and organizational cultures." In *Computer Science and Software Engineering (JCSSE), 2016 13th International Joint Conference on*, pp. 1-6. IEEE, 2016. - DOI: 10.1109/JCSSE.2016.7748915

[19] **C. Christof**, and K. Shankar. "Industry Trends 2017." *IEEE Software* 34, no. 2 (2017): 112-116. - DOI: 10.1109/MS.2017.55

[20] Standish Group International Inc., "THE CHAOS MANIFESTO", 2012. Available at: https://cs.calvin.edu/courses/cs/262/kvlinden/resources/CHAOSManifesto2012.pdf

[21] S. Hastie, S. Wojewoda, "Standish Group 2015 Chaos Report - Q&A with Jennifer Lynch". Oct 04, 2015. Available at: https://www.infoq.com/articles/standish-chaos-2015

[22] N. Ozkan, A. Tarhan, C. Kucuk. "Scrum at Scale in a COBIT Compliant Environment: The Case of Turkiye Finans IT." (2017).Ozkhan, Tarhan e Kucuk (2017)

[23] A. G. Vallerão, L. K. Roses. "Monitoramento e controle de projetos de desenvolvimento de Software com o Scrum: avaliação da Produção Científica." Revista de Gestão e Projetos 4, no. 2 (2013): 100. DOI: 10.5585/gep.v4i2.154

[24] V. Mahnic, N. Zabkar. "Using COBIT indicators for measuring scrum-based software development." Wseas transactions on computers 7, no. 10 (2008): 1605-1617.Mahnic, Zabkar (2008)