Gaia Maturity Model to Deploy IT Services Continuity

Completed Research

Wagner Hiroshi Ueno
State University of Londrina
Londrina, Brazil
wagner.ueno@sistemafiep.org.br

Rodolfo Miranda de Barros
State University of Londrina
Londrina, Brazil
rodolfo@uel.br

Jacques Duílio Brancher
State University of Londrina
Londrina, Brazil
jacques@uel.br

Abstract

Nowadays, information technology companies – micro and small enterprises – represent the majority of organizations in Brazil. However, these companies are not prepared for business continuity management, which could lead to their mortality when problems such as disasters and disruption of system services occur. Deploying IT Services Continuity Management as a planning tool would be the solution. This case study shows the improvement of a technology company after the implementation of Gaia Maturity model for IT Services Continuity Management.

Keywords

Planning; management; maturity; companies.

Introduction

Even today, some managers see the IT Services Continuity Management (ITSCM) as a needless investment, for which the allocation of resources is the bare minimum. According to (Bon 2005), however, statistics show IT disasters are more common than we imagine. Causes can vary from a wide range of events, such as lightning strikes, fire accidents, floods, burglary, vandalism, energy shortcuts, or even terrorism. A Business Continuity Plan could save many corporations affected either by environmental forces or internal business-related problems.

Businesses are increasingly becoming more dependent on Information Technology, so the impact of IT Services unavailability is drastically high. If the availability or performance of a service is reduced, users face challenges in performing regular work activities. That is, the dependence on IT will continuously increase users, managers and CEOs expectations and requests. In order to guarantee the continuity of operation, corporations must estimate the impact of IT Services loss and develop a Continuity Plan.

In order to develop this idea, this paper is divided as follows: section II presents theoretical background on the two main topics of this study – namely IT services continuity management, and maturity models – also approaching related works. Section III includes both the research methodology and the methodology used in the model development process. In section IV, the questionnaire applied is presented along with the results collected. At last, section V summarizes the conclusions and future work.

Literature Review and Related Work

This section presents a literature review over the development topics, conducted in three major databases: Science Direct, IEEE Explore, and ACM Digital Library. In addition to the exploration of databases, this work also intends to study the state-of-the-art situation of IT Services Continuity Management. Related

work found over the literature body is also presented.

IT Services Continuity Management

The main objective of IT Services Continuity Management (ITSCM) is to support the Business Continuity Management (BCM) process, by making sure IT services and resources will be operational according with the recovery objectives established in the business agreement. Such services and resources include systems, networks, applications, databases, telecommunications (Soula 2013).

ITSCM aims to:

- Determine a collection of continuity and recovery plans;
- Conduct frequent Business Impact Analysis;
- Estimate business risks and projections;
- Support and guide IT and business decisions regarding continuity and recovery issues;
- Make sure continuity procedures are aligned in order to meet or surpass particular continuity objectives established in the business agreement;
- Evaluate the impact of changes over continuity and recovery plans;
- Deploy high-performance actions in order to increase service availability;
- Negotiate with third-party IT servers the recovery level needed to support continuity plans.

Related Work

In addition to the literature review, a search on available related work was also performed, as explained in the last paragraph of this item. The search reveals that this study is pioneer in the development of a framework for a maturity model using IT services continuity management. There are, however, some non-specific studies approaching the use of IT services continuity management aiming at knowledge storage.
Such studies converge to the main application of this framework, developed to assist information storage and management for companies interested in knowledge management. An example of a work applying this technique, that is, the generation of knowledge from practice in specific situations, is presented in (Mesquita 2013). This approach enables low-risk development processes, in order to reach established goals.
Compared with the CMMI (Capability Maturity Model Integration) and the Softex's Reference Model for Services (MR-MPS-SV), the Gaia Maturity Model to Deploy IT Services is divided in maturity levels, and its implementation process is designed to fit the needs of micro and small businesses – which is precisely the case of the 21 companies included in this study. In this sense, this model has proven to be efficient because data collected with the survey suggested that these companies are placed in a very low (or almost null) maturity level. Also, the model focuses on specialized training in the services offered by the companies, in order to reach a high-level performance concerning the services availability. Thus, the 5 maturity levels aim to provide companies with capacity and availability in implementing the processes efficiently.

Research Methodology

In order to emphasize the importance of defining and monitoring a research methodology for scientific production, this paper describes a ready-to-use research model, as well as a methodology specifically structured for the development of the maturity model.

Research Methodology Model

The research methodology used is based on a model provided by the GAIA Software Lab, housed at the Computer Department of the State University of Londrina.
GAIA's model consists of three major topics: (1) Theoretical Analysis, (2) Development, and (3) Validation. The first stage – (1) Theoretical Analysis – includes three main activities: State-of-the-art Analysis, Theoretical Foundation, and Comparative Analysis. The "State-of-the-art Analysis", which is performed by searching databases, aims to provide resources for the second and the third macro-activities – "Theoretical Foundation" and "Comparative Analysis". The first stage of the methodology is completed after performing all 3 steps.
In the second stage – (2) Development –, a first pass version of the framework is developed in the beginning

of the process. After that, development progresses to the "Selection of Indicators for Analysis and Validation" and the "Selection of Case Studies". These two steps are in-between activities in the Development and the Validation stages, since they share activities and outcomes with both parts.
Then, the model progresses to stage 3 (Validation), where the "Data Collection during Implementation" and the "Results Analysis" are performed. Finally, the cycle goes back to stage 2, in order to perform the last step – "Framework Development (Consolidated Version)". This methodology is proven to be especially efficient in projects related to the development of maturity models through a framework.
Based on the described methodology – which was also applied in this study – a methodology specifically structured for maturity models through the IT Services Continuity Management (ITSCM) was developed, as presented in Section B.

Research Methodology Developed for the IT Services Continuity Management (ITSCM) Model

This methodology is based on (Horita and Barros 2012), and is also divided in three major topics, namely: (1) Initial Analysis, (2) Development, and (3) Validation, including seven steps for the framework development process. Among them, two steps are in the Initial Analysis, four steps are in the Development and two final steps are in the Validation stage, as shown in Figure 2.

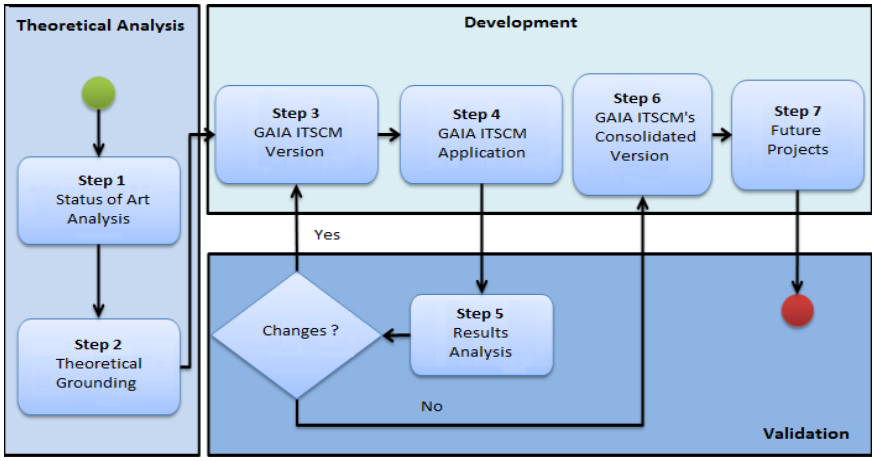

Figure 2 – Research methodology for a framework aimed at Maturity Models using IT Services Continuity Management (ITSCM). Source: adapted from (Horita and Barros 2012).

According to Figure 2, the first stage – Theoretical Analysis – consists of two steps: Step 1 – State-of-the-art Analysis and Step 2 – Theoretical Foundation. In the first step the model is structured. In this case, the following databases were used for structuring: Science Direct, IEEE Explore, Scopus, and ACM Library. This step should guide the search for related and/or complementary work in the literature body.
The second stage presented in Figure 2 is the Development. This stage includes four steps. Step 3 – GAIA ITSCM Version, aims at the establishment of maturity levels, services, and the diagnostic assessment questionnaire application, whilst Step 4 – GAIA ITSCM Application, according to (Horita and Barros 2012), includes: (1) case study planning, (2) data collection preparation, (3) data collection, (4) data analysis, and (5) reports.
Before the second stage ends, the model starts the third stage – Validation. This is where Step 5 – Results Analysis takes place, by comparing results collected so far with the model development, until it becomes able to perform all required procedures for deployment. The flow returns to Step 6 – GAIA ITSCM Final Version in Stage 2, where a final version of the model is developed. Finally, Step 7 – Future Work ends the framework cycle with the description of desired future work to be conducted upon the research.

Questionnaire Application and Results

A research was conducted in 21 Information Technology companies located in the North, Northwest, West and Southwest Paraná (Brazilian province), with the application of a diagnostic assessment questionnaire (DAQ), as presented in Figure 3.

This questionnaire is based on the Gartner Group Inc. study, which aims to portray the organization's perspective over the business continuity management. It was responded by IT managers and CEOs of all the 21 companies. The complete presentation of results is compiled in (Briganó 2014).
The questionnaire provided an overview of the company, regarding IT governance and emphasizing the IT services continuity management.

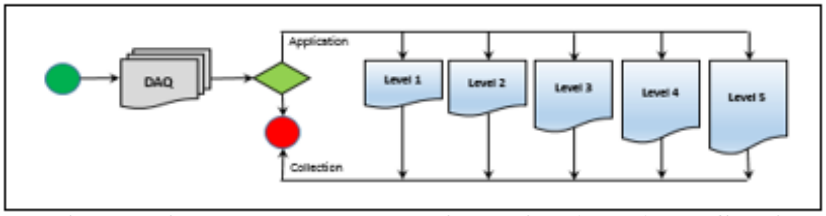

Figure 3 – Diagnostic Assessment Questionnaire (DAQ) application process

Research Questionnaire Results

As presented in Figures 4, 5 and 6, results indicate that the companies do not have a security plan to protect against disasters caused by terrorism, fortuity, force majeure reasons, or system failure. Security plans implementation rate is under 30% in these companies.
Figure 4 presents the compliance rate (total of all samples divided by the total number of companies) in each one of the 7 axes. In turn, figure 6 presents the individual results collected from the 21 companies surveyed.

Compliance rate by axis

Axis	Compliance rate
Governance	29,50%
Scope	29,97%
Investment	33,20%
Organizational Program	29,90%
IT DRM	29,30%
Processes and Control	28,55%
Training / Simulation	30,40%

Figure 4 – Table with results divided by axes

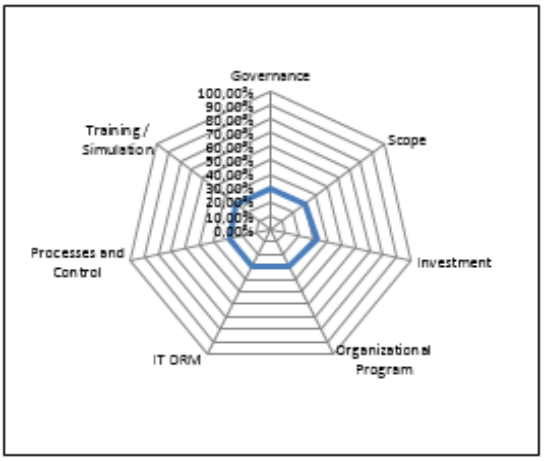

Figure 5 – Representative chart with results divided by axes

Governance appears with 29.50% of compliance rate in the survey conducted with companies. It indicates how often top-level administration is updated about the business continuity management and about the recovery objectives that support new corporative ventures. It also describes how often an internal balance is performed in order to effectively implement and maintain the BCM routine.

Scope is rated with only 29.97% of compliance. It is responsible for the definition of a group of metrics the organizations should have in order to measure the business continuity management routine.
It also determines span limits for service recovery in critical situations.
Besides that, it establishes metrics for risk management and business continuity that must be reported to managers.

Investment reports 33.20% of compliance rate. This indicates where managers place investment related to business continuity management and disaster recovery. It should ideally be connected to long-term strategic objectives and particular business agreements. Business continuity management projects must be revised (if needed) in order to guarantee budget requirements compliance.

Organizational program appears with a rate of 29.90%. This topic requires the business continuity management and the disaster recovery management to be aligned with a global corporative program. Business continuity management objectives should also be in line with the business strategy.

IT DRM (Disaster Recovery) rate is 29.30%. Service levels for disaster recovery management are established by the key-business requirements. It also integrates business continuity management with disaster recovery, besides performing continuous validation of risk evaluation and business impact analysis.

Processes and control are reported to have 28.55% of compliance rate. Recovery time objectives (RTO) and recovery point objectives (RPO) must be aligned with the actual recovery time. Maximum Acceptable Outage (MAO) and minimum business continuity must be clearly defined both for products and services. There must be a software/system to control and manage the status and maturity of the business continuity management plan. It also must include a crisis/accidents management tool in order to manage disaster responses.

Training/simulation rate of compliance is 30.40%. This is consistently achieved through planned simulation or actual recovery scenarios, by performing service level recovery and availability in critical situations.

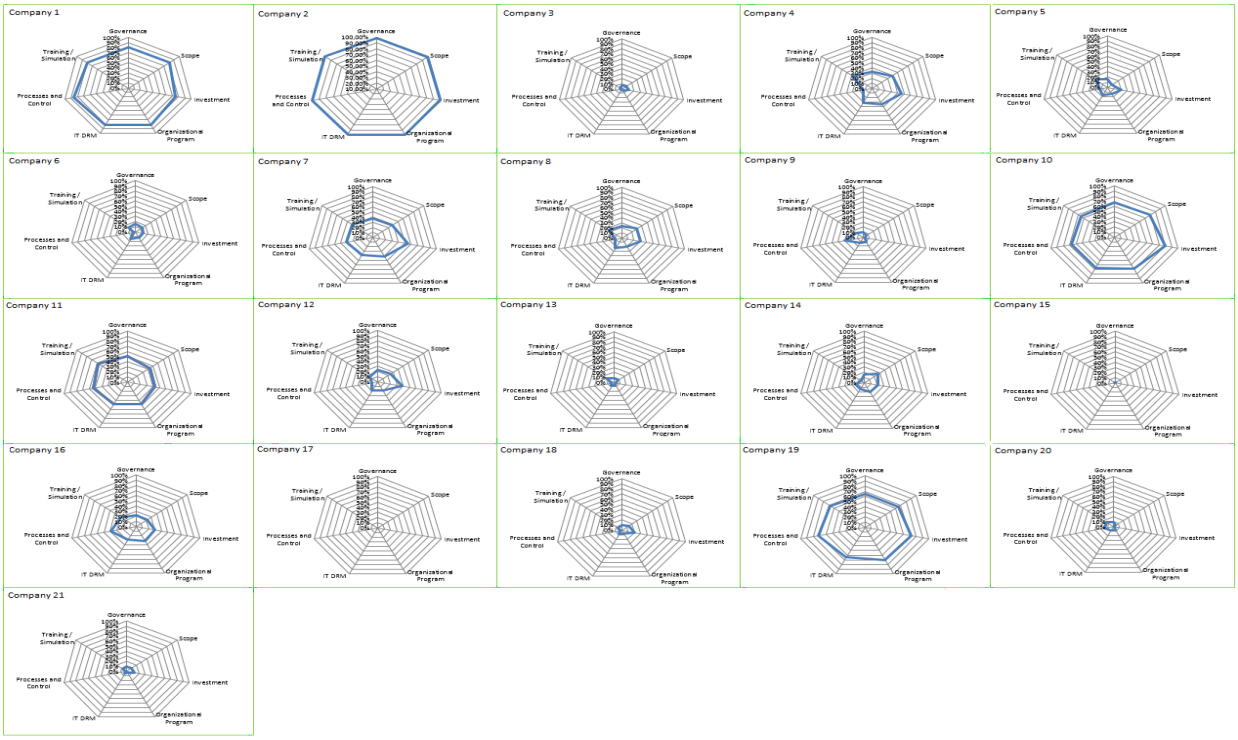

Figure 6 – Results collected from 21 companies with the application of the Diagnostic Assessment Questionnaire (DAQ)

Maturity Levels

Maturity levels were defined for the Gaia Maturity Model to Deploy IT Services Continuity, based on the works of (Taconi et al. 2013 and Taconi 2014). They are presented in Figure 7:

Figure 7 – Gaia Maturity Levels to the Deployment of IT Services Continuity

Level 1 – No Management: in the beginning of this level, there are several recovery procedures provided by the IT Department. It is impossible, however, to either name and quantify them, or identify their functionalities, people in charge, and whether they are provided by the internal team or third-party partners. The focus in this level must be to identify and quantify the collection of continuity and recovery plans provided by the IT staff. The compliance rate accepted in this maturity level varies from 0% to 19.9%;

Level 2 – Partially Managed: continuity and recovery plans are identified, but they are not recorded or documented, thus restricting the access to information such as their availability and objectives. In this level, the main goal is to deploy and document the variety of continuity and recovery plans for IT services. The compliance rate accepted in this maturity level varies from 20% to 39.9%;

Level 3 – Fairly managed: the collection of continuity and recovery plans for IT services are stored in a database, but there is no description of requirements, settings, people in charge, support and users. The objective in this level is to identify the aforementioned aspects in relation to continuity and recovery. This level also requires the definition of expected results – considering the IT staff capabilities – description of requirements, settings, and contacts of people in charge of recovery activities. The compliance rate accepted in this maturity level varies from 40% to 59.9%;

Level 4 – Managed and audited: the collection of continuity and recovery plans for IT services are stored in a database, along with the attributes description, but there is no update policy, information on the latest updates, or an IT services continuity policy to be controlled by the IT Department. In this level, it is requested that companies properly document changes in the continuity and recovery plans. Besides that, every new plan must be registered in the IT database prior to being provided for use. The compliance rate accepted in this maturity level varies from 60% to 79.9%;

Level 5 – Continuous Improvement: the collection of continuity and recovery plans for IT services are stored and constantly updated. New plans are registered in the system prior to launching. The development of a new policy is needed for approval, verification and updating of existing plans – such as improvements to be performed. The compliance rate accepted in this maturity level varies from 80% to 100%.

The progression of the Gaia Maturity 5-level model to Deploy IT Services Continuity is presented in the following sub-items. They also describe specific required actions in order to move from one level to another. The explanation of Gaia Maturity Model to Deploy IT Services Continuity, divided in axes, is provided below:

Maturity Levels to Deploy Governance

According to Figure 8, Governance is – in the first level – disconnected from top-level administration. In the second level, the IT Services Continuity program is aligned with management requirements, including the definition of recovery objectives. Level 3 adds the performing of an internal balance in order to implement and maintain the program. Level 4 encourages alignment with clients and services providers regarding recovery and availability of minimum requirements. In order to progress to the fifth level, the organization is requested to control and continuously improve the IT Services Continuity Management program.

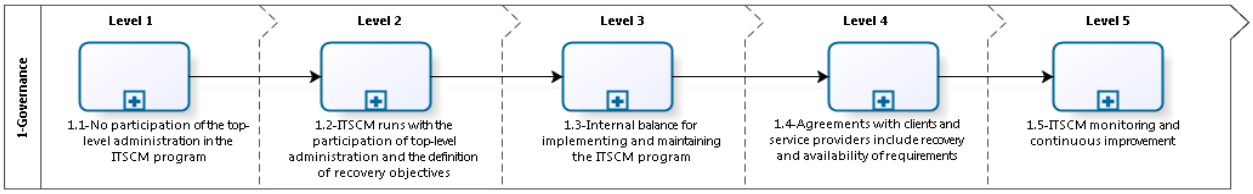

Figure 8 – Maturity Levels to Deploy Governance

Maturity Levels to Deploy Scope

As presented in Figure 9, the Scope initially does not provide metrics for the IT Services Continuity Management. As it progresses to level 2, primary minimal metrics are defined for the Continuity Management. In level 3, there is – in addition to defined metrics – the establishment of services recovery time. Level 4 intends to validate defined metrics together with the top-level administration staff. Progression to level 5 depends on the monitoring and updating of metrics for the management of IT services.

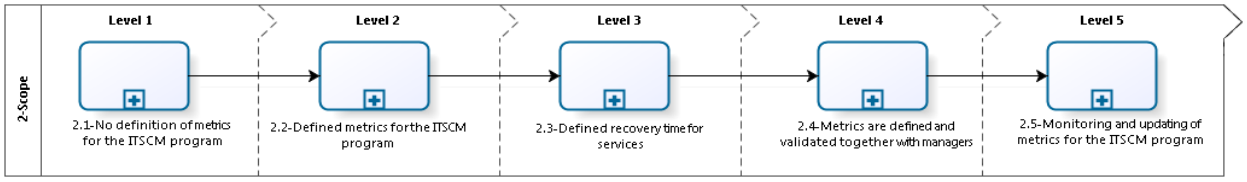

Figure 9 – Maturity Levels to Deploy Scope

Maturity Levels to Deploy Investment

According to Figure 10, the top-level administration is unaware of the IT Services Continuity project in the beginning of level 1. In level 2, managers define investments required for the IT Services Continuity. Level 3 connects IT Services Continuity objectives with organizational long-term strategic objectives. Level 4, in turn, links IT investments with the long-term strategic objectives. Finally, in level 5, projects are constantly revised in order to reach compliance with the financial planning.

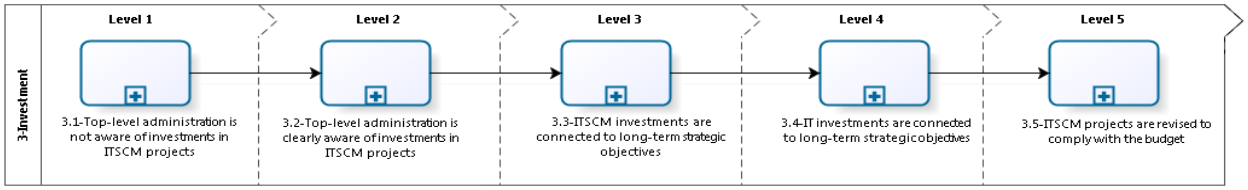

Figure 10 – Maturity Levels to Deploy Investment

Maturity Levels to Deploy Organizational Program

The maturity levels for Organizational Program are presented in Figure 11. At first, the Organizational Program is completely disconnected from the Organizational Policy. In level 2, the organizational program is defined accordingly with the company policy, but its focus is restricted to the organization major strategic activities. In level 3, the company shares information on the IT services continuity management and the disaster recovery with all employees. Level 4 integrates the IT services continuity management with the disaster recovery management. In order to progress, the fifth level requires the complete integration between critical situations plans and the disaster recovery, along with the definition of minimal levels for the IT Services Continuity.

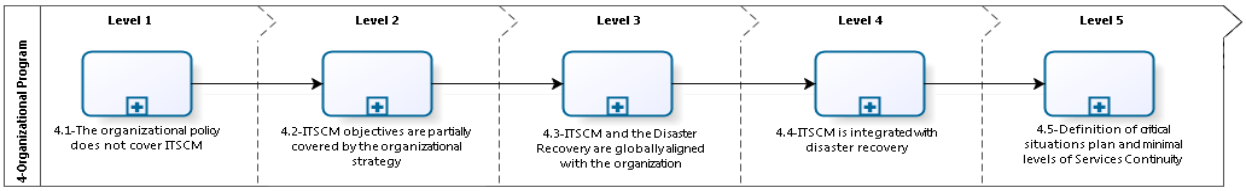

Figure 11 – Maturity Levels to Deploy Organizational Program

Maturity Levels to Deploy IT DRM

In the first level, the IT Disaster Recovery Management (IT DRM) – according to Figure 12 – identifies which risks and impacts directly influences the company services. Level 2, in turn, includes the criteria definition for classification of risks, as well as the impact evaluation in case of services outage. In level 3, the main objective is to develop an action plan to minimize such risks. In level 4, the focus is on sharing

information and updating about the documentation process. Finally, level 5 requires the implementation of a risks monitoring process.

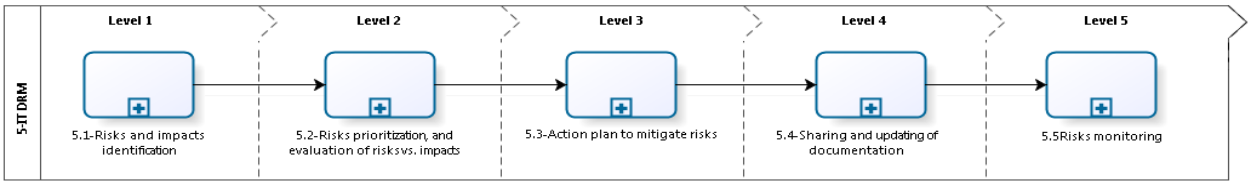

Figure 12 – Maturity Levels to Deploy IT DRM

Maturity Levels to Deploy Processes and Control

Recovery processes are present but not properly defined in the first level of the Processes and Control axis – Figure 13. In level 2, the competencies of the people in charge of recovery activities are defined and evaluated during performance. Level 3 requires the definition of recovery procedures (Time, Point, and Maximum Acceptable Outage). In order to reach the fourth level, a tool to manage this process must be implemented. At last, level 5 requires the monitoring of processes and the definition of a continuous improvement plan.

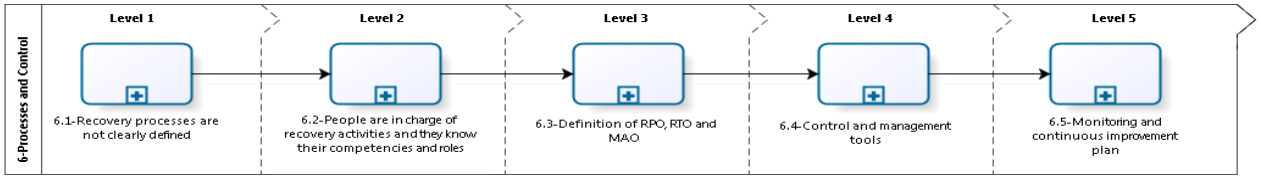

Figure 13 – Maturity Levels to Deploy Processes and Control

Maturity Levels to Deploy Training / Simulation

According to Figure 14, the first level of Training/Simulation starts with no training and simulations defined for services recovery. In level 2, training and simulated recovery activities are included for all staff members. In level 3, training is customized – roles and specific activities in the service recovery process are defined. Training and simulation activities are planned in level 4, and results show individual performance of the staff members. Finally, level 5 is related to the IT services continuity management awareness program, which is frequently revised and updated, if necessary.

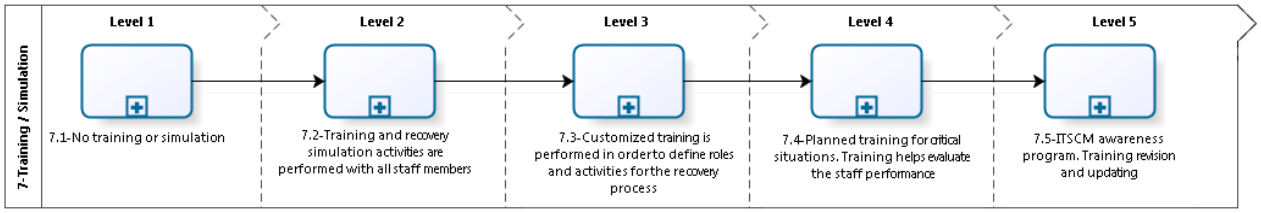

Figure 14 – Maturity Levels to Deploy Training and Simulation

Case study of one of the companies that responded the diagnostic assessment questionnaire, after the Gaia Maturity Model application

The case study analyzes one of the companies that responded the Diagnostic Assessment Questionnaire (DAQ). It is a technology company that works as a third-party datacenter provider.
The implementation stage of Gaia Maturity Model to Deploy IT Services Continuity Management lasted 3 months. During this time, several control activities and procedures were implemented in order to help achieving the objectives.
The control activities and documentation developed along the process include: Organizational Policy with services continuity protocols, risk management diagram, services recovery times, and the specialized training for the staff in charge of each service.
Figures 15 and 16 show the company metrics before (Q1) and after (Q2) the Gaia Maturity Model to Deploy

IT Services Continuity Management implementation.

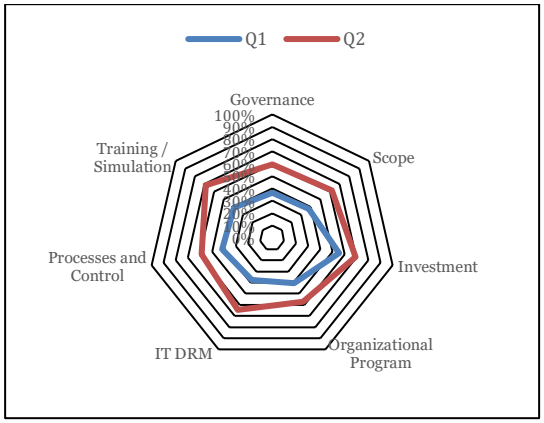

Figure 15 – Chart comparing the company progression.

As presented in Figure 16, there was an expressive improvement in all 7 areas. Growth represented more than 50% in comparison with results collected prior to the Gaia Maturity Model to Deploy IT Services Continuity Management implementation.

Axis	Q1	Q2
Governance	37%	60%
Scope	38%	62%
Investment	56%	69%
Organizational Program	41%	57%
IT DRM	37%	65%
Processes and Control	41%	59%
Training / Simulation	40%	69%
Average	41%	63%

Figure 16 – Table comparing the company progression.

In order to improve Governance capabilities, the IT services continuity management was deployed after discussion with the top-level administration. Recovery objectives were defined, and services were listed according to the priority. An internal balance was performed with the results achieved.
Scope was improved by defining Services Continuity metrics, which were aligned with services levels and recovery time operations. Such metrics support decision-making in occasional recovery scenarios.
In addition to involving the top-level administration, the Investment was connected with IT services continuity objectives and with long-term strategic objectives.
In relation to the Organizational Program, a major concern was to align the IT services continuity with the disaster recovery procedures defined in the Organizational Policy, as well as sharing information and involving all the staff members.
In order to improve Disaster Recovery (IT DRM), risks were identified and classified through the definition of criteria for risks and impact analysis. That resulted in the development of an action plan to reduce risks.
Regarding Processes and Control, roles were clearly defined for staff members, as well as recovery objectives (RTO, RPO, and Maximum Acceptable Outage).
Finally, Training and Simulation activities for service recovery were defined and planned. Customized training sessions were designed, including specific roles and recovery activities.
After the implementation and operation of the model, and taking in consideration the results collected, it is possible to notice an expressive and consistent improvement in relation to the assessed topics.

Conclusion and Future Work

IT services continuity management has increasingly become more important for the management of any company. The managing of active properties does not only provide control, but it also represents a core process inside every department, thus contributing to the success or failure of the business.

In this context, this study presented a maturity model to assist processes, so that IT services continuity management can correctively, constructively, and positively occur inside the company. This case study started with the application of a diagnostic assessment questionnaire, which places the company within one of the maturity levels. After the model implementation process, services should be in a high-performance position, supported by best practices used within each maturity level.

Therefore, the questionnaire application and the model implementation allow the identification of where the company is – in a given scenario – and where it should go next. This study also covered the company progression through all 5 maturity levels – demonstrated through the data collection and the case study. Results indicate the model is efficient and that it can positively contribute to increase the company maturity level. The model presented in this study elevates the IT services continuity management to more than just abstract theory: it becomes a feasible and convenient way to manage and support organizations.

In line with the results presented so far, future work includes the application of the model in companies with a higher maturity level (where maturity level ≥ 4), in order to verify whether the model is equally efficient and applicable to that context.

REFERENCES

Associação para Promoção da Excelência do Software Brasileiro. 2015. Guia Geral MPS de Serviços (MR-MPS-SV).

Bon, J. V. 2005. Foundations of IT Service Management, based on ITIL. Lunteren - Holanda: Van Haren Publishing,

Briganó, G.U. 2014. "Um framework para desenvolvimento de Governança de TIC", Dissertação de Mestrado em Ciência da Computação. Universidade Estadual de Londrina – UEL.

Ehsan, N.P. A., Arif, J., Mirza, E. and Ishaque, A. 2010. "CMMI / spice based process improvement", in Management of Innovations and Technology (ICMT) IEEE International Conference, 99.859-862.

Ekionea, B., Bernard, P. and Plaisent, M. 2011. "Towards a maturity model of knowledge management competences as an organisational capability", International Conference on E- Business and E-Government (ICEE).

Gaffo, F. H. and Barros R. M. de. 2012. "GAIA Risk - A Service-based Framework to Manage Project Risks", CLEI, XXXVIII Conferencia Latino america en Informatica, Medellín, Colômbia. pp.1-10.

Góes, A. S. and Barros R. M. de. 2012. "Gerenciamento do conhecimento em uma fábrica de software: um estudo de caso aplicando a ferramenta GAIA – L.A." CLEI, XXXVIII Conferencia Latino america en Informatica, Medellín, Colômbia. pp.1-9.

Horita, F. E. A. and Barros R. M. de. 2012. "GAIA Human Resources - An approach to integrate ITIL and Maturity Levels focused on improving the Human Resource Management in Software Development". 25th International Conference on Computer Applications in Industry and Engineering, New Orleans, Louisiana USA. v. 1. p. 51-56.

ISO, ISO/IEC 27005. 2008. Information Technology – Security Techniques – Information Security Risk Management.

Magalhães, I. L. and Pinheiro, W. B. 2007. "Gerenciamento de Serviços de TI na Prática", Uma abordagem com base na ITIL, Novatec Editora Ltda.

Mesquita, B. O. and Barros, R. M. de. 2013. "A model to manage the software estimation process through maturity levels and services", IADIS International Conference Information Systems, Lisboa.

Guedes, R. M. 2012. "Percepção da maturidade de gerenciamento de projetos de tecnologia de informação - um estudo comparativo entre setores do brasil", Master's thesis, Universidade de São Paulo, Brazil.

Rautenberg, S., Steil, A. V. and Todesco, J. L. 2011. "Modelo de Conhecimento para mapeamento de instrumentos da gestão do conhecimento e de agentes computacionais da engenharia do conhecimento", Perspectivas em Ciência da Informação, v.16, n.3, p.26-46.

Soula, J. M. F. 2013. "ISO/IEC 20000 Gerenciamento de Serviços de Tecnologia da Informação", Brasport Livros e Multimídia Ltda.

Taconi, L. H., Barros, R. M. de. and Zarpelão, B. M. 2013. "Proposal of a Maturity Model to Deploy a Service Catalog", 10th International Conference Applied Computing.

Taconi, L. H. 2014. "Gaia Catálogo de Serviços de TI: Um framework para construção de catálogos de serviços de Tecnologia da Informação", Dissertação de Mestrado em Ciência da Computação, Universidade Estadual de Londrina – UEL.

United Kingdow, 2011. "ITIL Continual Service Improvement", Cabinet Office.