UNIVERSIDADE FEDERAL DO ESTADO DO RIO DE JANEIRO
CENTRO DE CIÊNCIAS EXATAS E TECNOLOGIA
PROGRAMA DE PÓS-GRADUAÇÃO EM INFORMÁTICA

PSECO-IM: AN APPROACH FOR INCIDENT MANAGEMENT TO SUPPORT GOVERNANCE IN PROPRIETARY SOFTWARE ECOSYSTEMS

Luiz Alexandre Martins da Costa

Orientador

Dr. Rodrigo Pereira dos Santos

Co-orientador

Dr. Awdren de Lima Fontão

RIO DE JANEIRO, RJ - BRASIL
SETEMBRO DE 2021

PSECO-IM: AN APPROACH FOR INCIDENT MANAGEMENT TO SUPPORT GOVERNANCE IN PROPRIETARY SOFTWARE ECOSYSTEMS

LUIZ ALEXANDRE MARTINS DA COSTA

DISSERTAÇÃO APRESENTADA COMO REQUISITO PARCIAL PARA OBTENÇÃO DO TÍTULO DE MESTRE PELO PROGRAMA DE PÓS-GRADUAÇÃO EM INFORMÁTICA DA UNIVERSIDADE FEDERAL DO ESTADO DO RIO DE JANEIRO (UNIRIO). APROVADA PELA COMISSÃO EXAMINADORA ABAIXO ASSINADA.

Aprovada por:

Rodrigo Pereira dos Santos, D.Sc. — UNIRIO

Awdren de Lima Fontão

Awdren de Lima Fontão, D.Sc. — UFMS

Gleison dos Santos Souza

Gleison dos Santos Souza, D.Sc. — UNIRIO

Carina Alves

Carina Frota Alves, Ph.D. — UFPE

RIO DE JANEIRO, RJ - BRASIL
SETEMBRO DE 2021

Catalogação informatizada pelo(a) autor(a)

C837

Costa, Luiz Alexandre Martins da
PSECO-IM: An Approach for Incident Management to Support Governance in Proprietary Software Ecosystems / Luiz Alexandre Martins da Costa. -- Rio de Janeiro, 2021.
2017 f.

Orientador: Rodrigo Pereira dos Santos.
Coorientador: Awdren de Lima Fontão.
Dissertação (Mestrado) - Universidade Federal do Estado do Rio de Janeiro, Programa de Pós-Graduação em Informática, 2021.

1. Software Ecosystems. 2. Governance. 3. Incident Management. I. Santos, Rodrigo Pereira dos, orient. II. Fontão, Awdren de Lima, coorient. III. Título.

To God, my dear wife, my children and my parents.

A Deus, minha querida esposa, meus filhos e meus pais.

Acknowledgements

First, I thank God for granting me health and wisdom to always follow and for providing me with light, energy, courage, and persistence.

To my wife Angela, for her patience, support, understanding, and encouragement, and to my children, Luana and Paulo Victor, blessings in our lives. I am eternally grateful for everything that I am, for what we have achieved together, and for the happiness I have.

To my parents, Luiz Antonio and Valdete (*in memoriam*), are examples of character, kindness, affection, and especially for the words of encouragement, faith, and courage. To all my family and friends, for the positive vibes and for always cheering and believing in me, even when we had a good part of our social time reduced in favor of this goal.

To my advisor, Rodrigo Pereira dos Santos, fundamental for my development, for the opportunity, guidance, advice, motivation, patience, understanding, and for inspiring and guiding me in this project.

To my co-advisor, Awdren Fontão, dear and great friend. Thank you for the dedication that made you, at various times, put aside your moments of rest to help me and guide me. Thank you for the shared experience of writing articles and supporting the research carried out throughout this work.

I would like to thank UNIRIO professors Claudia Cappelli and Leonardo Azevedo for the precious classes in the beginning of this journey. I appreciate all Complex Systems Engineering Laboratory for helping me to grow and for the friendship, in special, Marcio Imamura, Luciana Carvalho, Nadja Piedade, Juliana Fernandes, and Felipe Cordeiro.

Finally, special thanks to my colleague Gilson Fonseca, responsible for wise words in hard times, and CAPES for financial support during my research.

Costa, Luiz Alexandre **PSECO-IM: Uma Abordagem de Gestão de Incidentes para Apoiar a Governança em Ecossistemas de Software Proprietário**. UNIRIO, 2021. 217 páginas. Dissertação de Mestrado. Programa de Pós-Graduação em Informática.

RESUMO

As organizações que produzem sistemas de software trabalham de forma cooperativa e competitiva para oferecer apoio a novos produtos e satisfazer as necessidades dos clientes. Neste cenário, mais atenção está sendo dada à conectividade e dependência nos relacionamentos entre vários atores (fornecedores de software, desenvolvedores internos e externos e gerentes) que constroem uma rede de criação de valor chamada Ecossistema de Software (ECOS). Como um tipo do ECOS, o ECOS proprietário diz respeito a dados e conhecimento concentrados em uma plataforma proprietária com contribuições protegidas por propriedade intelectual. A plataforma tecnológica que apoia as iniciativas de negócios em um ECOS proprietário é construída usando diferentes tecnologias combinadas com dezenas de pontos de integração, emergindo uma rede de dependências e complexidades arquitetônicas. Nesse contexto, alguns estudos mostram que a indisponibilidade de sistemas (incidentes) na plataforma causa grandes transtornos de imagem e financeiros para as organizações. Para mitigar os riscos de incidentes, a equipe de gestão de TI utilizar alguns mecanismos de governança para sustentar a plataforma tecnológica. Este trabalho tem como objetivo desenvolver e avaliar uma abordagem (PSECO-IM) baseada em processo para gerenciamento de incidentes visando apoiar a equipe de gestão de TI na governança da arquitetura da plataforma tecnológica em um ECOS proprietário. Primeiro, conduzimos uma revisão ad hoc para estudar a literatura sobre ECOS e alguns desafios de pesquisa. Em seguida, um estudo exploratório nos forneceu uma melhor compreensão das políticas e diretrizes de gerenciamento de ativos de software em um ECOS proprietário. A fim de atualizar os mecanismos de governança aplicados em ECOS proprietário, realizamos um estudo longitudinal da literatura. A partir dos resultados dos estudos anteriores, conduzimos um estudo de caso participativo para discutir as estratégias de governança praticadas no ECOS proprietário de uma organização. Além disso, executamos um estudo de revisões rápidas (rapid review) envolvendo profissionais da indústria para endereçar problemas práticos em gestão de incidentes. Ao longo desses estudos, descobrimos que a gestão de incidentes é uma área importante para a governança de um ECOS proprietário. Por fim, construímos uma ferramenta de apoio relevante para a tomada de decisão pela equipe de gestão com base no nível de confiança da plataforma.

Palavras-chave: Ecossistemas de Software, Ecossistemas de Software Proprietário, Governança, Gestão de Incidentes, ITIL.

Costa, Luiz Alexandre **PSECO-IM: An Approach for Incident Management to Support Governance in Proprietary Software Ecosystems**. UNIRIO, 2021. 217 pages. Master's Thesis. Graduate Program in Informatics.

ABSTRACT

Organizations that produce software systems work cooperatively and competitively to support new products and satisfy customer needs. In this scenario, more attention is being paid to connectivity and dependency in relationships among several actors (e.g., software providers, internal and external developers, and IT managers) that build the network value creation called Software Ecosystem (SECO). As a type of SECO, proprietary SECO concerns data and knowledge concentrated on a proprietary software platform with contributions protected by intellectual property. The technological platform that supports the business initiatives in a proprietary SECO is built using different technologies combined with dozens of integration points, emerging a network of dependencies and architectural complexities. In this context, some studies show that the unavailability of systems (incidents) causes major image and financial upheavals for organizations. In order to mitigate the risks of incidents, the IT management team should address strategies based on governance mechanisms to sustain the technological platform in the proprietary SECO. This work aims to develop and evaluate a process-based approach (PSECO-IM) for incident management to support the IT management team in the governance of a technology platform architecture in a proprietary SECO. First, we conducted an ad hoc literature review to study the literature on SECO and some research challenges. Next, an exploratory study gave us a better understanding of software asset management policies and guidelines in a proprietary SECO. In order to update proprietary SECO governance mechanisms, we performed a longitudinal literature study. Based on the results of previous studies, we conducted a participative case study to discuss the governance strategies practiced in the proprietary SECO of a organization. Moreover, we run a rapid review study involving industry practitioners to address practical problems in incident management. Throughout these studies, we found that incident management is an important area for proprietary SECO governance. Finally, we developed a support tool with relevance to the decision-making of the IT management team based on the confidence level of the platform.

Keywords: Software Ecosystems, Proprietary Software Ecosystems, Governance, Incident Management, ITIL.

Contents

List of Figures

List of Tables

Abbreviations

API	Application Programming Interface
BPMN	Business Process Model and Notation
DSR	Design Science Research
ERP	Enterprise Resource Planning
GQM	Goal-Question-Metric
IM	Incident Management
IS	Information Systems
ISO	International Organization for Standardization
ISV	Independent Software Vendor
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITSM	Information Technology Service Management
LOC	Lines of Code
MPS	Melhoria de Processo de Software (Software Process Improvement)
OSSECO	Open Source Software Ecosystem
PSECO	Proprietary Software Ecosystem
RQ	Research Question
SECO	Software Ecosystem
SLA	Service Level Agreement
SQ	Sub-Question
SSN	Software Supply Network

1. Introduction

This chapter aims to present the context, motivation, and problem addressed in this research. In addition, we explain the research goals and the methodology adopted to achieve them, as well as the research structure.

1.1 Context

At the end of the 20th century, information technology became a fundamental tool for any organization. In order to ensure return on investments, organizations sought greater competitiveness, reducing the cycle involving the development of products and services. To achieve these results, the search for total quality and data reengineering were widely used tools, such as ERP (Enterprise Resource Planning) systems (MUTSAERS; VAN DER ZEE; GIERTZ, 1998).

Organizations work cooperatively and competitively to support new products, satisfy customer needs, and eventually incorporate the next round of innovations. So, increasing attention is being paid to connectivity and dependency in relationships between organizations (ARNDT; DIBBERN, 2006). In this context, there are several actors involved (e.g., suppliers, distributors, outsourcing companies, software providers, developers, and managers) that affect and are affected by the value creation network (IANSITI; LEVIEN, 2004b), for example SAP SE[1].

From this perspective, researchers created a concept to be analyzed in the software industry called software ecosystems (SECO). According to Jansen *et al.* (JANSEN; BRINKKEMPER; FINKELSTEIN, 2009), SECO is a set of actors functioning as a unit

[1] The name is an initialism of the company's original German name: Systemanalyse Programmentwicklung, which translates to System Analysis Program Development. Currently, the company's legal corporate name is SAP SE — SE stands for *Societas Europaea*, a public company registered in accordance with the European Union corporate law.

and interacting in a shared market for software and services, centered on a common technological platform. A proprietary SECO is characterized by the overcrowding of several products, technologies, and architectures of other ecosystems. An organization that is responsible for maintaining it is called keystone (MANIKAS; HANSEN, 2013b). A keystone also must establish governance policies as a critical strategy for ensuring a sustainable platform (TIWANA; KONSYNSKI; BUSH, 2010). A sustainable approach refers to how the platform can resist natural changes, for example, business evolution and technology obsolescence (DHUNGANA et al., 2010).

1.2 Motivation

According to the definition of SECO governance (ANGEREN; ALVES; JANSEN, 2016), the use of strategic procedures and processes is a way of controlling, maintaining, or changing the ecosystem towards a sustainable approach. The challenge of maintaining a sustainable platform have become a priority for large organizations based on the survey performed by Gartner Group[2]. The products, applications, and services that make up the architecture of the proprietary SECO platform are built using various technologies combined with dozens of integration points, creating a network of dependencies and complexities. Complex systems may be documented in detail, but can still behave unpredictably (GRIEVES; VICKERS, 2017).

The unavailability of systems and the unpredictable behavior are concerns that cause major image and financial upheavals for a keystone. Sustaining the technological platform of the proprietary SECO requires addressing governance mechanisms related to internal and external developers, IT service providers, and IT managers to mitigate the risks of disruptions (DHUNGANA et al., 2010). Some concerns go beyond the technical solutions, such as business and social challenges (SADI; YU, 2015), to cite a few, revenue increase, knowledge management, software asset management, and process optimization for productivity gains.

In a business environment, IT plays an important role in the performance of the proprietary SECO, especially when it provides a flow of information that adds value without weakening organizational efficiency (BROWN, 2003). Based on this premise, a structured way of dealing with those challenges to support the governance mechanisms of the technological platform related to the proprietary SECO is through Information Technology Service Management (ITSM), from the business strategic plan until the incidents man-

[2] Gartner is the world's leading research and advisory company

agement. According to ITIL (Information Technology Infrastructure Library) framework, a set of good practices for ITSM, an incident is an unplanned interruption of an IT service (IDEN; EIKEBROKK, 2013). An incident management process is a set of procedures and actions taken to respond to and resolve the incidents: how incidents are detected and communicated, who is responsible, what tools are used, and what steps are taken to resolve the incident (IDEN; EIKEBROKK, 2013). Therefore, it is an integrated efficient way for the use of processes, people, and tools/technologies to promote the strategic alignment between the technological platform of the proprietary SECO and the organization business model (IDEN; EIKEBROKK, 2013).

1.3 Problem

A factor influencing the synergy between the business strategy alignment and sustaining the technology platform of the proprietary SECO is market pressure for a state-of-the-art solution for every business need. It causes organizations to work at a highly accelerated pace, passing this anxiety to IT project team, which must deliver results in an increasingly short time (KAPPELMAN; MCKEEMAN; ZHANG, 2006).

As a consequence of the growing number of demands added to the lack of flexible processes, some problems emerged, such as: there is not enough time to make a complete requirements specification; time estimates are imprecise; communication failures among clients, IT software providers, developers, and IT managers; late projects; over budget due to rework on software artifacts; and deadlines are prioritized over the quality of the software. The result is a software project delivered with low quality, producing incidents in the productive environment of the organization.

This scenario contributes to the construction of an environment that is complex and vulnerable to failures in proprietary SECO, leaving developers and managers ahead of some challenges, such as: i) building software applications able to achieve success while maintaining the stability of the technological platform; ii) managing proprietary SECO governance relating to the technological platform architecture with several actors; and iii) monitoring the technological platform architecture of the proprietary SECO in order to ensure the quality of software applications provided to end-users.

We cannot guarantee that the approved applications in this scenario have the expected quality. Therefore, the risk of applications deployment in the production environment may cause instability in the technological platform, damaging the relationships of SECO actors. This scenario may create incidents and trigger factors that directly affect the satisfaction of the end-user and the image of the organization (CREEDEN et al., 2013).

Moreover, the absence of a concrete and reliable knowledge database for decision-making hampers the keystone's management team from driving governance strategies to evaluate the replacement of software assets in the technology platform. According to the study of Manikas and Hansen (MANIKAS; HANSEN, 2013b), there is not much research to understand the mentioned behavior in the context of proprietary SECO, also due to the difficulty of access to data from these environments and considering the protection of data and intellectual property are ways used by keystone to obtain a competitive advantage.

1.4 Research question

To meet the problem and motivation contexts, we formulated the main research question for this study: **"How can an incident management approach support technology platform governance in a proprietary SECO?"**. As a way to answer the main research question presented above, the following sub-questions were defined:

- SQ1 - What factors can influence incident management in proprietary ECOS?
- SQ2 - What indicators and metrics for incident management can support governance in organizations?
- SQ3 - How are SECO software asset governance mechanisms implemented in a proprietary SECO?
- SQ4 - How are SECO governance strategies and health metrics implemented in a proprietary SECO?
- SQ5 - How to reduce incident backlog on a technological platform of the proprietary SECO?
- SQ6 - What are the characteristics of a process-based approach for incident management to support governance applied in a proprietary SECO?
- SQ7 - How the particularities of an incident management process to support governance are characterized in a proprietary SECO?
- SQ8 - How is a process-based approach for incident management to support governance implemented in a proprietary SECO?

Each research sub-question is revisited as chapters of this Master's thesis are presented. The main question is also answered through an assessment of a process-based for incident management and a tool to support the management team in the governance of the technology platform in a proprietary SECO.

1.5 Objective

This work aims to develop and evaluate a process-based approach (PSECO-IM) for incident management to support the IT management team in the governance of the technology platform architecture of a proprietary SECO. Governance frameworks are characterized by the use of strategic procedures, models and processes to guide the proprietary SECO (JANSEN; CUSUMANO, 2013). There are different strategies to cope with issues regarding SECO governance.

It is necessary to analyze the governance mechanisms used to establish the level of control, monitoring, decision rights, and scope that have become important managerial aspects for the technology platform of the proprietary SECO (TIWANA; KONSYNSKI; BUSH, 2010). The problem addressed in this research refers to sustaining and monitoring the technological platform of a proprietary SECO using governance mechanisms related to incident management. Section 1.4 provided the body of knowledge around the main research question.

Our research goal is not to be limited by a specific proprietary SECO environment. The benefits are available to IT managers to address a broad range of governance issues in different domains, such as financial, energy, food, and telecommunication industries. **Specific goals** further determine the ideas of our research. We aim to achieve the following intermediate results as specific goals to address the problems described above:

- Defining a body of knowledge on the relevance of software asset governance mechanisms in proprietary SECO;
- Understanding how governance mechanisms are realized by actors in a proprietary SECO;
- Defining a body of knowledge on incident management in proprietary SECO;
- Establishing an approach to incident management process in proprietary SECO considering the elements: keystone, internal and external developers, IT service provider, and IT managers;

- Developing a support tool that instantiates the proposed process comprising the goals presented above; and

- Identifying and defining monitoring metrics for diagnosing the technological platform architecture aiming to support the IT management team in a proprietary SECO.

1.6 Research methodology

We ground our work on methods from Empirical Software Engineering (WOHLIN; RUNESON; HÖST, et al., 2012) and was inspired by **Design Science Research (DSR)** due to the need to build an artifact to solve a problem in the real world (HEVNER, 2007). Our work is composed of three phases: ***conception***, ***implementation***, and ***evaluation***. This research followed the methodology shown in Figure 1.1. The ***conception*** phase is the initial phase of this research project and involves the intellectual process of developing a research idea into a realistic and appropriate research design. Exploratory study, literature studies, and survey research are methods that sustained this phase. The ***implementation*** phase involves applying research results into practice. The definition and implementation of process-based approach for incident management to support governance in a proprietary SECO and a focus group sustained this phase. Finally, the ***evaluation*** phase represents the visions and perspectives of practitioners and is focused on evaluating the process-based approach relating to adequacy, control, understanding, and generality perceptions. The tool was evaluated concerning utility and ease-of-use perceptions. Participative case study and some adjustments were performed to ensure that the objectives were met during this phase. Each step from Figure 1.1 is described as follows:

- **Ad hoc Literature Review:** this method is an informal approach to understand the main concepts of a research line and identify a gap not yet covered on a research topic. Generally, the actions taken are not documented. We studied the literature on SECO and some research challenges were identified, mainly covering the following topics: SECO governance mechanisms, SECO health, SECO characteristics and classification, and SECO incident management process. This preliminary step helped us to understand the context of SECO and the concepts regarding SECO governance *(Chapter 2 , Section 2.2)*;

- **Exploratory Study:** from literature studies on SECO, we investigated the governance mechanisms of software assets in a proprietary SECO of an insurance industry organization. Some lessons were observed from the results. This step helped us to refine the research protocols regarding governance and incident management in proprietary SECO (KITCHENHAM; CHARTERS, 2007) *(Chapter 3).* The study results were published in the main track of the XVI Brazilian Symposium on Information Systems (SBSI) (COSTA; FONTÃO; SANTOS, 2020a), provided a publication partnership in the V Workshop on Social, Human and Economic Aspects of Software (WASHES) (IMAMURA et al., 2020), and strengthened the research theme when it was published at the XIII Workshop on Theses and Dissertations in Information Systems (WTDSI) (COSTA; FONTÃO; SANTOS, 2020b);

- **Longitudinal Literature Study:** the study was performed on SECO, extending an existing study of Alves *et al.* (ALVES; OLIVEIRA; JANSEN, 2017) that covered 2006 to 2015 in order to provide an update on SECO governance mechanisms and SECO health metrics. We analyze SECO classifications, evaluate the evolution of proprietary SECO, and investigate the SECO incident management process aligned with the organization's strategies *(Chapter 2, Section 2.3).* The study results were published in the main track of the XVII Brazilian Symposium on Information Systems (SBSI) (COSTA; FONTÃO; SANTOS, 2021b);

- **Participative Case Study (1):** in this step, a study was conducted to discuss the governance strategies practiced in the proprietary SECO of an organization. The participants also proposed new governance strategies based on the governance mechanisms and health metrics of Alves *et al.* (ALVES; OLIVEIRA; JANSEN, 2017) in the context of proprietary SECO *(Chapter 4).* The study results were published for a Special Issue on Collaboration and Innovation Dynamics in Software Ecosystems at IEEE Transactions on Engineering Management Journal (COSTA; FONTÃO; SANTOS, 2021d);

- **Rapid Review Study:** based on discussions of the participative case study, this method was performed to provide a body of knowledge bounded to practical problems, to investigate keystone's issues to handle incident management, and to explore the keystone's strategies to model incident management process *(Chapter 2, Section 2.4).* The study results were submitted to the Information and Management Journal (COSTA; FONTÃO; SANTOS, 2021c);

- **Approach for SECO Incident Management Process:** this study presents an incident management approach (PSECO-IM) to be explored within the existing relationships in the proprietary SECO, where we have a central organization with concerns on different platforms, mixed technologies, internal and external developers, different IT software providers, organization IT managers, and the emergence of new software projects frequently. In addition, a tool to support the decision-making of the IT management team was developed *(Chapter 5)*. The study results are in the final stage of submission at Information Systems Journal (COSTA; FONTÃO; SANTOS, 2021a);

- **Focus Group:** this method was applied to assess the effectiveness of the PSECO-IM approach for incident management to support governance in the proprietary SECO based on the experts' opinions *(Chapter 6, Section 6.3)*;

- **Participative Case Study (2):** this study aimed to evaluate the PSECO-IM approach's contributions to incident management in the proprietary SECO and the support tool to help the IT management team in the governance of a technology platform architecture. The approach was evaluated in an insurance industry organization as part of the case study. We grounded this study based on experts' opinions *(Chapter 6, Section 6.4)*; and

- **Refinement:** after the results of the participative case study step, a refinement step is indicated in order to act on the adjustments identified from the study. The PSECO-IM approach was refined and the tool's functionalities modified according to the practitioners' needs involved in the previous step *(Chapter 6, Section 6.4.6.5)*.

In summary, Figure 1.1 shows the chain of studies performed as follows: i) the context and the concepts regarding SECO governance were studied in the ad hoc literature review and provided us with input for the exploratory study. With the outcomes, we noticed the relevance of governance mechanisms in the proprietary SECO. The new results motivated us to verify in the literature the issues related to the governance of proprietary SECO through a longitudinal literature study. This longitudinal literature study allowed us to build an artifact with a set of governance mechanisms and health metrics used later in a participative case study. From the discussions about new governance strategies that emerged in the participative case study, we realized the need to understand the perceptions, methods, and technologies that were being used in incident management with practitioners through a rapid review; ii) the results generated in all these studies served as input for the conception of the PSECO-IM approach to the incident management process and the construction of a tool to instantiate a part of that process. Next, an assessment of the approach was carried out by experts through a focus group; and iii) another participative case study was performed to evaluate the PSECO-IM approach to incident management in the proprietary SECO and the support tool. The approach and the tool help the IT management team in the governance of a technology platform architecture. A refinement step with practitioners was added to improve the research results.

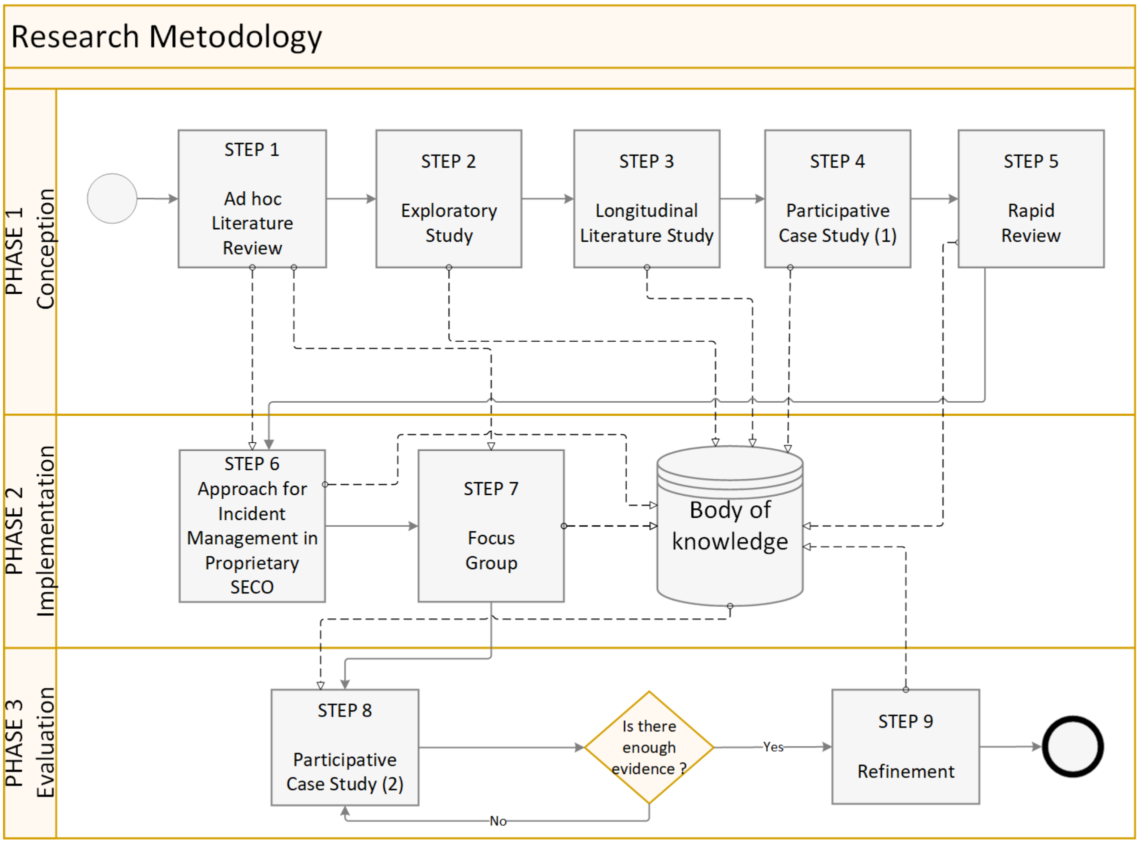


Figure 1.1: Research methodology.

1.7 Master's thesis structure

This Master's thesis is organized in seven chapters. In **Chapter 1**, the context of this work was presented, as well as the motivation and problem addressed by this research. Objectives were defined and the research methodology to reach those objectives were explained. The organization of this work follows the structure below:

Chapter 2 presents a discussion on the main topics of this research that serve as background to develop an approach for supporting the problems described in Chapter 1. This chapter explores the planning, execution, and analysis of the longitudinal literature and rapid review studies. The longitudinal literature study aims to provide an update on SECO governance mechanisms, SECO health metrics, SECO classifications, and analyze the evolution of proprietary SECO. The results are an updated perspective based on seven research questions, as well as a refined perspective on proprietary SECO and an initial understanding of the incident management process in this context. The rapid review study aims to provide a deeper understanding of the activities and strategies of incident management based on four research questions. Our results reveal some strategic drivers, indicators, and metrics for incidents handling in organizations.

Chapter 3 describes the exploratory study where it was possible to better understand the software asset management policies and guidelines as critical aspects for maintaining a sustainable proprietary SECO. The results of the analysis of the investigation on asset governance mechanisms in a proprietary SECO were performed using: i) survey research to collect insights on some governance mechanisms; ii) interviews with a group of managers to analyze the most relevant governance mechanisms; and iii) correlation analysis from the managers' opinions.

Chapter 4 presents a discussion on governance mechanisms in the context of a proprietary SECO of a large international insurance organization through a participative case study. Moreover, to cite a few, we gathered information on the governance in practice, and defined strategies to implement governance mechanisms measured by health metrics using the following methods: i) observation - to analyze the behavior of the participants in the face of problematic situations; ii) interviews - to collect participants' information on the adoption of governance mechanisms; and iii) opinion survey - to verify the level of participants' perception about the new strategies related to proprietary SECO governance mechanisms. Based on the results, we derived practical implications to provide a research agenda for the academic and practitioners.

Chapter 5 presents the conception of an approach for incident management to support governance in a proprietary SECO (PSECO-IM) aiming to identify incidents from recent project deployments following the ITIL guidelines and a tool to support the decision-making of the IT management team as a way to contribute to the elements of proprietary SECO.

Chapter 6 describes the results of the evaluation of the process-based approach and the support tool proposed in Chapter 5. This chapter also collects suggestions for improvements to the tool's functionalities and usability, as well as the governance strategies arising from the dashboard diagnosis provided by the tool.

Chapter 7 concludes this Master's thesis with some final remarks. Contributions to the academic community and to IT practitioners are discussed, as well as the research limitations and opportunities for future work.

2. Background

In order to address the research objective presented in Chapter 1, some concepts were identified relevant to this research, such as Software Ecosystems, Health and Governance in Software Ecosystems, Information Technology Service Management, and Information Technology Infrastructure Library. In this chapter, such concepts related to the development of an approach to support IT management team, the background that supports this work, and two secondary studies applied to the construction of a body of knowledge are presented.

2.1 Introduction

The development of a single software product has been replaced by a strategy where multiple software are integrated through a common technological platform (SANTOS, 2016), creating a collaborative environment known as Software ECOsystem (SECO). When the ecosystem is centered in a closed environment in which several platforms relate to each other, it is known as a proprietary SECO (MANIKAS; HANSEN, 2013b), such as SAP (Systems Applications and Products in data processing).

SAP ecosystem is composed of several actors, to cite a few, global delivery partners, service providers, resellers, independent software vendors, third-party developers, and customers. Its proprietary SECO depends on partners for customer success, who have: i) an understanding of the needs of customers, SAP products, and the ability to bring them together effectively, ii) built additional capabilities and solutions, and iii) integrated all of these elements along with customer legacy IT systems (CECCAGNOLI et al., 2012).

In this context, concerns are focused on information and knowledge concentrated on a proprietary software platform and the contributions are protected by intellectual property. This is also pointed out in the *Grand Research Challenges in Information Systems*

(BOSCARIOLI; ARAUJO; MACIEL, 2017), more specifically on how to build technological platforms to deal with a new generation of information systems concerning technical complexity and social diversity.

Maintaining the platforms based on technological excellence to mitigate the risks of incidents (i.e., unplanned service interruption) can be an opportunity to solve challenges that are beyond technical problems, i.e., involving business activities and social concerns (SADI; YU, 2015). The keystone (organization that maintains a SECO) is responsible for keeping the proprietary SECO platform that is characterized by comprising several products, technologies, and architectures. The keystone must establish governance policies as a critical strategy for ensuring a sustainable platform. A sustainable approach refers to how the platform can resist natural changes, for example, business evolution and technology obsolescence (DHUNGANA et al., 2010).

The advancement of business needs for more confidence solutions and outdated technologies may be incident triggering factors and pose a threat to the platform continuity. In this scenario, governance frameworks emerged, aiming to promote robust management practices to enhance the keystone's business planning and reinforce the structure of the IT area, making it an area with a strategic function, such as the management of ongoing arrangements with service providers and software/hardware vendors. The governance frameworks are models comprising good practices that recommends how IT projects, incident management processes and other demands should be managed (SELIG, 2008). These frameworks serve to guide the work, setting standards and guidelines so that IT became a strategic area within the company. In the SECO context, the governance frameworks can be characterized by the use of strategic procedures, models and processes (JANSEN; CUSUMANO, 2013).

The correct implementation of governance mechanisms can promote a sustainable and healthy ecosystem and an ineffective governance can result in a declining growth of the ecosystem (WAREHAM; FOX; CANO GINER, 2014). According to Manikas and Hansen (MANIKAS; HANSEN, 2013a), SECO heath is defined as the ability to provide durably growing opportunities for its members and for those who depend on it. SECO health is measured from operational indicators related to governance mechanisms. The Epic Games and Apple case illustrates how the choice of certain governance methods can directly influence the SECO health. The business battle between Epic Games, responsible for the biggest phenomenon of multiplayer games (Fortnite), and Apple, the only company in the world with more than US$2 trillion in market value became a great example how different strategies and tactics can address situations on how ecosystem is managed. In short, Epic actively violated an Apple App Store rule and Apple removed Fortnite from

Apple Store in retaliation (BOSTOEN; MÂNDRESCU, 2020).

This chapter is organized as follows: Section 2.2 presents the basic concepts in our research context; Section 2.3 describes the research method of the longitudinal literature study; Section 2.4 describes the research method of the rapid review study; and Section 2.5 summarizes the findings from this chapter.

2.2 Basic concepts

2.2.1 Software ecosystems

According to Bosch (BOSCH, 2009), software ecosystems (SECO) is a set of software solutions that enable, support and automate the activities and transactions among actors and the organizations that provide these solutions in an associated social or business ecosystem. It consists of a software platform, a set of internal and external developers and a community of experts serving the needs of a community of users aiming to build solutions that add value. Figure 2.1 shows the actors involved in the context of SECO.

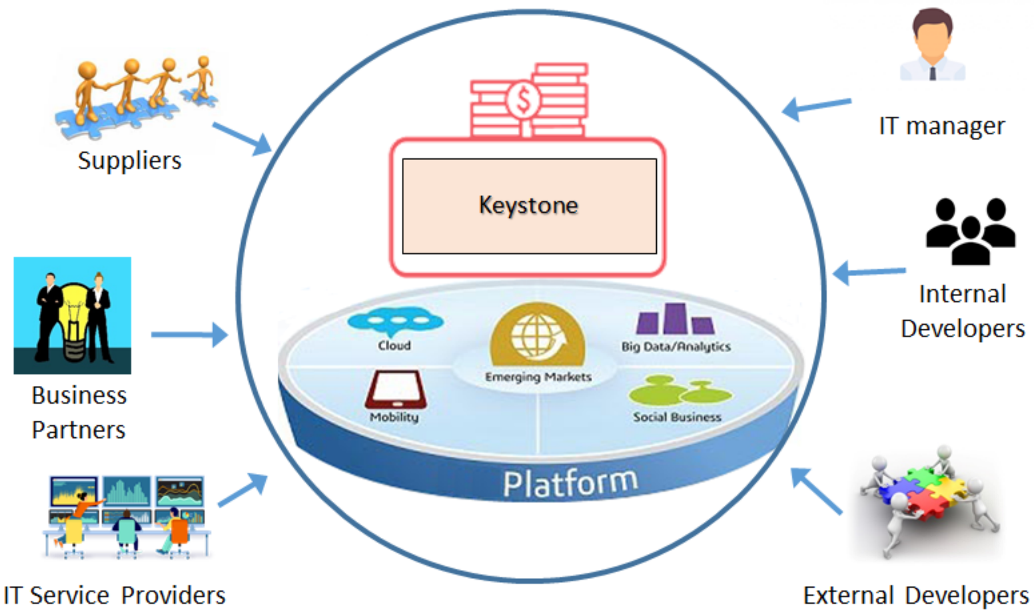


Figure 2.1: SECO actors.

A SECO classification approached from a value creation perspective (MANIKAS; HANSEN, 2013b) can be: **i) proprietary**: where the source code and other artifacts produced are protected by confidentiality agreements, as they are the products that would yield revenues to the ecosystem, e.g., platform as a service and e-commerce ecosystems; **ii) open**: where the actors do not participate to obtain direct revenues from their activity in the ecosystem, e.g., Eclipse Foundation and Apache Foundation; and **iii) hybrid**: which supports proprietary and open source contributions, e.g., iOS SECO may use proprietary strategies as app store and the source code repository to drive policies in the technological platform, and open source strategies for community engagement as tools, submission, and publication contributions.

SECO are complex environments composed by diverse actors interacting in a distributed software development environment, with a platform, where these actors give technological support to the established environment (SANTOS; WERNER, 2011). The SECO governance requires a careful balance of control and autonomy given to players and becomes a managerial aspect for proprietary platform owners and open source communities (ALVES; OLIVEIRA; JANSEN, 2017). Moreover, the governance mechanisms can be managerial tools used by SECO actors aimed at influencing an ecosystem's health (ALVES; OLIVEIRA; JANSEN, 2017).

2.2.2 Health and governance in software ecosystems

Iansiti and Levien introduced the concept of ecosystems' health in (IANSITI; LEVIEN, 2004a). As a definition, SECO health is the ability to provide durably growing opportunities for its members and for those who depend on it. This conception was built from analyzing three aspects based on the biological ecosystems: robustness, productivity, and niche creation (IANSITI; LEVIEN, 2004a). The need to measure the SECO health can help to find errors and point out the need for changes in some decision-making. For the keystone, the concrete information of the health indicators provides more correct decisions and more peace of mind to make the necessary adjustments.

For each aspect, a variety of metrics to measure the health status with the indicators that can be divided into groups to reflect the business conditions of a SECO was presented (IANSITI; LEVIEN, 2004a): **i) robustness**: represents the ability of the ecosystem to face and survive radical changes; **ii) productivity**: is the capacity of an ecosystem to convert and transform inputs into new products and new features; and **iii) niche creation**: is the ability of an ecosystem to support the variety and diversity of different organizations creating valuable resources.

Selecting ecosystem governance strategies that contribute towards ecosystem health is a challenge (BAARS; JANSEN, 2012) due to the requirements of keeping a careful balance between control and autonomy given to ecosystem actors. SECO governance guidelines can contribute to achieve the organization's strategic goals through managerial decision-making based on data related to operational metrics and indicators.

In this research, we use as a basis the integrated definition for SECO governance proposed by Alves *et al.* (ALVES; OLIVEIRA; JANSEN, 2017) as: "*all processes by which a player creates value, coordinates relationships, and defines controls*". It indicates that ecosystem governance influences the health and sustainability of ecosystems (HARTIGH; TOL; VISSCHER, 2006) (JANSEN; BRINKKEMPER; SOUER, et al., 2012) (JANSEN; CUSUMANO, 2013) (MONTEITH; MCGREGOR; INGRAM, 2014) (ANGEREN; ALVES; JANSEN, 2016). This means that governance strategies and managerial decisions taken by keystones will affect the healthy evolution of the entire ecosystem. The health metrics can also provide operational indicators on how a SECO is governed.

There are three main categories of governance mechanisms (ALVES; OLIVEIRA; JANSEN, 2017): **i) value creation** that generates and distributes value; **ii) coordination of players** that maintains consistency and integration of activities, relationships and ecosystem structures; and **iii) organizational control and openness** that manages the tension between open and closed models.

2.2.3 Reference artifacts

We proposed two reference artifacts for better understanding the SECO governance mechanisms. The first document is a mind map (Section 2.2.3.1) and the second one refers to a glossary (Section 2.2.3.2). Based on Alves *et al.* (ALVES; OLIVEIRA; JANSEN, 2017), both artifacts provide parameters that help to obtain an overview of a domain, guiding a starting point to ensure the consistency and applicability of the study. We followed and synthesized the governance mechanisms of Alves *et al.* (ALVES; OLIVEIRA; JANSEN, 2017) as an inspiration for the models presented in this study.

2.2.3.1 Building the mind map document

Figure 2.2 shows the governance mechanisms mind map diagram. The mechanisms are refered as *"(Mxx)"* where *"M"* is the governance mechanism and *"xx"* is the ID. The main reason for choosing such a research tool was the potential type of diagram focused on the management of information, knowledge and intellectual capital, for understanding and solving problems, in memorization and learning, and helping in the business strategic management of a company (NOVAK; CAÑAS, 2006). In addition to the mind map, we detail a glossary document with a conceptual description of each governance mechanism.

The mind map was built based on the three main categories of governance mechanisms proposed by Alves *et al.* (ALVES; OLIVEIRA; JANSEN, 2017). The orange color ellipses correspond to the value creation category, the pink color ones to the coordination of players category, and the green color ones to organizational openness and control category. To facilitate the comprehension of each governance mechanism, we also provided a glossary detailed in Section 2.2.3.2 that contains the meaning of each one.

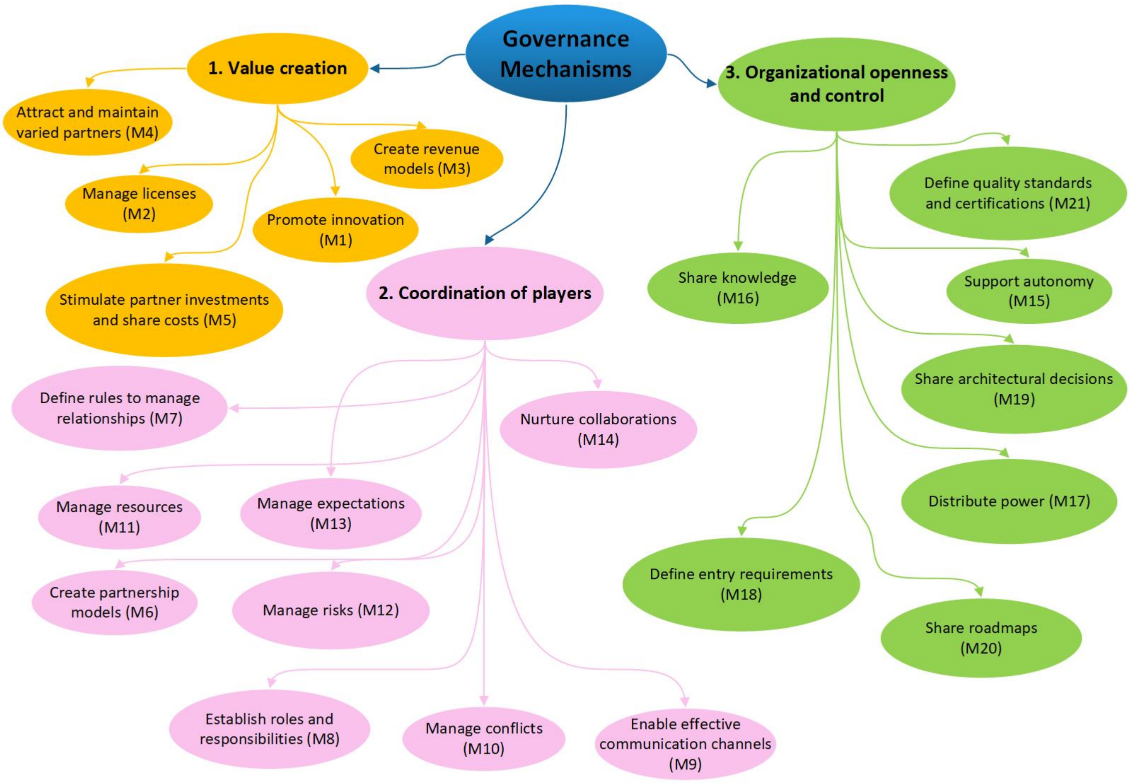

Governance Mechanisms
1. Value creation
Attract and maintain varied partners (M4)
Create revenue models (M3)
Manage licenses (M2)
Promote innovation (M1)
Stimulate partner investments and share costs (M5)
2. Coordination of players
Define rules to manage relationships (M7)
Nurture collaborations (M14)
Manage resources (M11)
Manage expectations (M13)
Create partnership models (M6)
Manage risks (M12)
Establish roles and responsibilities (M8)
Manage conflicts (M10)
Enable effective communication channels (M9)
3. Organizational openness and control
Define quality standards and certifications (M21)
Share knowledge (M16)
Support autonomy (M15)
Share architectural decisions (M19)
Distribute power (M17)
Define entry requirements (M18)
Share roadmaps (M20)

Figure 2.2: Mind map of the three main categories of SECO governance mechanisms (ALVES; OLIVEIRA; JANSEN, 2017).

2.2.3.2 Defining the glossary document

In general, a glossary contains explanations of concepts relevant to a certain field of study or action. As such, the term is related to the notion of ontology. We introduced the glossary document as follow:

- **Software Ecosystem** (acronym SECO) is a set of actors acting as a unit and interacting in a shared market for software and services, centered on a common platform (BRINKKEMPER; VAN SOEST; JANSEN, 2009).

- **SECO Governance** are procedures and processes by which a company controls, changes or maintains the current and future position in a SECO at different levels of scope (JANSEN; CUSUMANO, 2013).

- **SECO Governance Mechanisms** are managerial tools (e.g., team monitoring, 360-degree assessment, creation of certification programs) used by managers, developers and stakeholders aimed to influence the SECO health. In other words, we boost the set of mechanisms to offer mutual benefits to everyone using a technological platform, increasing the community of users and developers for longer periods and with the ability to survive changes, such as new technologies or new products. Alves *et al.* (ALVES; OLIVEIRA; JANSEN, 2017) proposed three main categories of governance mechanisms:

1. **Value Creation** - the mechanisms are generally proposed and fed by the organization that owns the technological platform, generating and distributing value to the entire ecosystem, sensitive to partners and customers.
   (a) **Promote innovation (M1)**: promote initiatives with partners and software suppliers to improve innovation processes, and can provide extended value to the customer in the future;
   (b) **Manage licenses (M2)**: create new value propositions that generate new revenue streams. For example, developer software/services licenses that provide warranties regarding support for intellectual property;
   (c) **Create revenue models (M3)**: discuss different ways to generate revenue, as there may be different models for different situations, for example, direct sales of plug-ins and new communication channels to build customer relationships;
   (d) **Attract and maintain varied partners (M4)**: create strategies so that developers and suppliers are attracted to the platform, willing to obtain financial advantages and form business relationships; and
   (e) **Stimulate partner investments and share costs (M5)**: encourage partners to invest in services with manufacturers, enabling another channel for the customer, which could motivate cost sharing with the manufacturer itself.
2. **Coordination of players** - this category focuses on aspects of governance coordination aimed at maintaining consistency and integration of ecosystem activities, relationships and structures, both for customers and partners.
   (a) **Create partnership models (M6)**: building partnerships with customers, suppliers and a third party community to allow the creation of final products;
   (b) **Define rules to manage relationships (M7)**: rethinking how the organization can deal with alliances, offering stakeholders new possibilities for building relationships;
   (c) **Establish roles and responsibilities (M8)**: establishing regulations, processes and measures to coordinate all activities and, being able to dif-

ferentiate the roles of partners, the organization will be able to maintain interaction at manageable levels;

   (d) **Enable effective communication channels (M9)**: defining an effective strategy and process to manage communication between partners, through the improvement of communication channels;

   (e) **Manage conflicts (M10)**: creating by the organization an incentive structure to attract partners and manage possible conflicts between them;

   (f) **Manage resources (M11)**: managing the balance of resources between the development of specific customization requested by customers and the evolution of the product according to their own roadmap, that is, a planning view of the product improvements;

   (g) **Manage risks (M12)**: managing risks in decision making among maintenance and software evolution is an important issue to be addressed, for example, the constant updating of a product can represent a risk for the systems running;

   (h) **Manage expectations (M13)**: defining objectives, expectations, requirements and interests of each stakeholder. The organization must implement negotiation strategies among the different participants within the ecosystem; and

   (i) **Nurture collaborations (M14)**: encouraging collaborative and complementary relationships with suppliers and customers is an important strategy for the organization's survival, being a competitive advantage in the market.

3. **Organizational Openness and Control** - this category focuses on strategic openness and control decisions. These mechanisms capture the tension between open and closed organizational models and represent how control will be retained by the organization and how autonomy will be given to stakeholders.

   (a) **Support autonomy (M15)**: Companies must share their internal plans and customer groups with partners, but they do not want to reduce their autonomy;

   (b) **Share knowledge (M16)**: Companies have challenges in how to distribute knowledge correctly with easy access to all members. These partnerships enable the sharing of knowledge and technology, increasing the potential for innovation and making the company an attractive partner;

   (c) **Distribute power (M17)**: The organization needs to demonstrate deliberate forms of power when negotiating requirements. This scenario allows suppliers to engage in a battle for power and control over the product's most valuable resources;

(d) **Define entry requirements (M18)**: The organization needs to define strategies so that stakeholders can overcome entry barriers related to financial issues and the need to dedicate a considerable amount of resources, for example, different pricing schemes, complete package offers with add-ons available at no additional cost of use and providing a basic level of functionality free of charge;

(e) **Share architectural decisions (M19)**: the organization adopts several architectural practices that contribute to maintaining the products performance and health, e.g., SDKs, APIs, tools, IDEs and any other resources of the central platform;

(f) **Share roadmaps (M20)**: the organization needs to disclose which launches are planned and how the products will evolve to understand stakeholders. These roadmaps establish an evolution products commitment and can be used as a basis for negotiating future contracts; and

(g) **Define quality standards and certifications (M21)**: defining a certification program allows the organization to raise quality standards and establish certain partners as highly valuable to the ecosystem.

- **SECO Governance Strategies** refer to management techniques, assessment, and a set of tools designed to help keystones make high-level strategic decisions (IANSITI; LEVIEN, 2004b).

- **SECO Metrics** provide operational indicators of how SECO is governed and data on keystones' standard business processes (ALVES; OLIVEIRA; JANSEN, 2017).

- **SECO Indicators** are measurable values that show how the SECO is achieving business objectives (ALVES; OLIVEIRA; JANSEN, 2017).

The application of governance mechanisms is essential for achieving the balance between the SECO actors and the technological platform (ALVES; OLIVEIRA; JANSEN, 2017). The technological platform is maintained by sustaining a set of technologies supported by keystone's developers and the SECO's applications with their supporting technologies are maintained by keystone's IT management team (JANSEN; CUSUMANO, 2013). However, the IT management decisions become more complex as third parties have greater influence in the keystone and their boundaries are not well defined due to relationships with external actors and developers (BOUCHARAS; JANSEN; BRINKKEMPER, 2009). To support good IT decisions, the market has directed efforts on frameworks, such as ITIL (Information Technology Infrastructure Library), COBIT (Control Objectives for Information Technologies), CMMI (Capability Maturity Model Integration), and PMBOK (Project Management Body of Knowledge) that reflect the practice of governance and has sought quality standards through international norms and standards, such as ISO/IEC 20000, 27002, and 38500.

2.2.4 Information Technology Service Management and Information Technology Infrastructure Library

Information Technology Service Management (ITSM) are the activities performed by an organization to design, plan, deliver, operate and control Information Technology (IT) services offered to customers (SELIG, 2008). ITSM consists of meeting the needs of stakeholders in a structured and agile way, analyzing the impact of these services and whether they are within the strategy created by organization (GALUP et al., 2009). Some traditional IT management frameworks (e.g., ITIL, COBIT, CMMI, and PMBOK) have reached a high degree of maturity making the transition to a ITSM model. Tools and models contribute to control the risks and information flows associated with the conduct of business processes in organizations (RAMLAOUI; SEMMA, 2014). While ITSM is a professional discipline that concerns itself with the effective design, deployment, and management of IT services, ITIL is a framework that IT professionals can use to implement best practices for ITSM and move towards a more effective IT organization (IDEN; EIKEBROKK, 2013).

For a proprietary SECO, ITSM is the set of processes that encompass the planning, execution and monitoring of the IT architecture of the technological platform. ITSM aims to ensure that ecosystem actors have access to quality services and that these services meet business needs. To do so, it is necessary to invest in people, processes and technology. If the organizations have difficulties when analyzing investments with tangible returns, intangible investments become even more complex as is the case with IT assets. IT assets are artifacts produced/acquired and stored by an organization (ADAMS; GOVEKAR, 2012). Showing the relationship between IT and return on investment is a challenge. Implementing ITSM is one of the structured ways to deal with the challenge from the strategic plan to incident management. According to ITIL - one of the ITSM most recognized frameworks (MCNAUGHTON; RAY; LEWIS, 2010) -, an IT service is a means of delivering value to organization clients (internal and external), facilitating the achievement of the results and avoiding specific costs and risks.

ITIL was originally created by the CCTA (Central Computer and Telecommunications Agency) under the auspices of the British government, and is a registered trademark of the UK Government's Office of Government Commerce (usually known as OGC). ITIL is a collection of best practices in ITSM in order to monitor, measure and improve the IT services (ADDY, 2007). The ITIL library comprises five distinct volumes: ITIL Service Strategy; ITIL Service Design; ITIL Service Transition; ITIL Service Operation; and ITIL Continual Service Improvement. Complementing the theoretical foundation, Incident Management (IM) is part of the Service Operation area, as shown in Figure 2.3. The theoretical lens of this work is focused in the context of proprietary SECO.

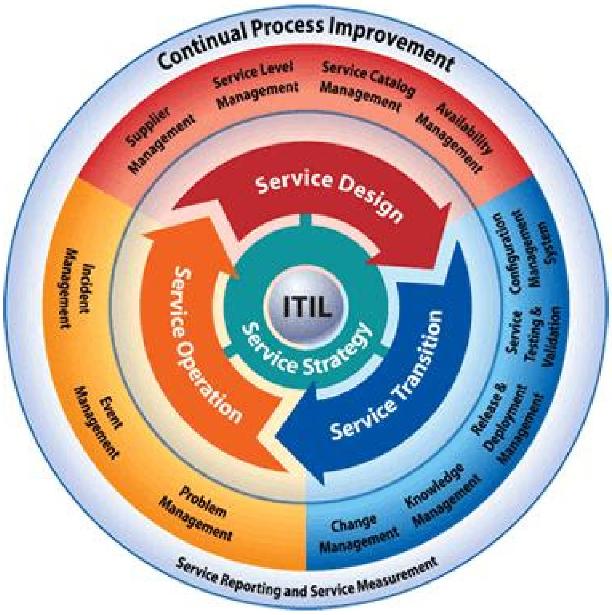


Figure 2.3: ITIL Service Operation (ADDY, 2007).

The objective of ITIL Service Operation is to make sure that IT services are delivered effectively and efficiently (ADDY, 2007). The primary goal of IM is to solve the incident as quickly as possible and return the IT service to normal operation. An incident, by ITIL definition, is an unplanned interruption or reduction in the quality of an IT service. IM process must manage the lifecycle of all incidents (ADDY, 2007).

There is a difference between ITIL and ISO/IEC 20000, 25000, and 27000. ITIL is a set of best practices created by technology industries worldwide and packaged in a library or framework, which does not necessarily need to be followed or implemented. ISO/IEC 20000[1] is the first international standard for service management and has a different focus.

[1] ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission) form the specialized system for worldwide standardization. Download at `https://www.iso.org/obp/ui/#iso:std:iso-iec:20000:-1:ed-3:v1:en`

It is a standard that needs to be followed and implemented. ISO/IEC 20000 is all based on ITIL (SAHIBUDIN; SHARIFI; AYAT, 2008). Before the emergence of any standard, we have to discover the best practices, so that an organization that wants to be certified in ISO/IEC 20000 needs to follow the standards and implements the best practices, whereas organizations that only want to improve the processes can go straight to implement best practices and then, succeed (SAHIBUDIN; SHARIFI; AYAT, 2008).

2.3 Longitudinal literature study

The challenge of selecting SECO governance strategies that contributes to the ecosystem health motivated Alves *et al.* (ALVES; OLIVEIRA; JANSEN, 2017) to conduct a systematic literature review (SLR). The authors provided an overview of SECO governance definitions and mechanisms, as well as SECO health definitions and metrics, covering literature from 2006 to 2015. To allow researchers to be able to detect any changes in specific research subjects that may occur over a while (ZAPF; DORMANN; FRESE, 1996), we propose a longitudinal literature study.

The longitudinal literature study focused on proprietary SECO governance and health was reported covering from 2016 to 2020, updating and refining the previous study of Alves *et al.* (ALVES; OLIVEIRA; JANSEN, 2017). An investigation was performed on SECO governance and health mechanisms for the proprietary SECO context. We provided an update based on examining how proprietary SECO aspects have evolved in the past five years, motivated by an exploratory study in an insurance industry organization (COSTA; FONTÃO; SANTOS, 2020a). The results of this study were published at an information systems conference (COSTA; FONTÃO; SANTOS, 2021b). This section details the research method, results and discussion.

2.3.1 Research method

We based our research protocol on Alves *et al.* (ALVES; OLIVEIRA; JANSEN, 2017) study and designed according to the guidelines for secondary studies of Kitchenham and Charters (KITCHENHAM; CHARTERS, 2007). When new evidence is added as part of updating an SLR, different findings and conclusions from those reported initially may be identified. Therefore, updating SLR may contribute to different purposes. For example, (i) providing a continuous update of the state-of-the-art on a research topic; and (ii) identifying how a particular research topic is evolving (MENDES et al., 2020). Based on these arguments, our SLR is characterized as a longitudinal study.

2.3.1.1 Research questions

We define the research questions (RQ) and the procedures to answer them. RQ1 to RQ4 came from the work of Alves *et al.* (ALVES; OLIVEIRA; JANSEN, 2017) are shown in Table 2.1. RQ5 to RQ7 refer to new SECO aspects concerning proprietary SECO are shown in Table 2.2.

Table 2.1: Goals and procedures to support answers from RQ1 to RQ4.

RQ	Goals	Procedures
1. How is governance characterized in SECO literature?	Discussing available definitions for SECO governance proposed in primary studies.	We searched the term "governance" in the primary studies and check if the study defined governance in SECO context. Subsequently, we extracted the definitions and discussed the concepts of governance.
2. What are the mechanisms proposed to govern SECO?	Classifying the studies propose in literature to govern SECO in three main categories of governance mechanisms (ALVES; OLIVEIRA; JANSEN, 2017).	We used thematic analysis as synthesis method, following the recommended steps proposed in (CRUZES; DYBA, 2011). We identified the relevant codes and merged them into key themes as performed by Alves *et al.* (ALVES; OLIVEIRA; JANSEN, 2017), counted how many times they appeared in the studies, and finally compared with the previous study classification.
3. How is health characterized in SECO literature?	Finding definitions about SECO health in the studies.	We searched the term "health" in the primary studies and collected data for each study including relevant information about the ecosystem.
4. What are the metrics proposed to assess the SECO health?	Classifying health metrics using productivity, robustness and niche creation definitions (IANSITI; LEVIEN, 2004a)(IANSITI; LEVIEN, 2004b)(IANSITI; RICHARDS, 2006).	We classified health metrics, counted how many times they appeared in the studies, and compared with the previous study classification.

2.3.1.2 Search process

The automatic search was the same as original SLR and was executed on the following databases: ACM Digital Library, IEEE Xplore Digital Library, Science Direct, and SpringerLink. We used the search string: *"software ecosystem" OR "software ecosystems" OR "platform ecosystem" OR "platform ecosystems"*. The extraction of data from the studies were carried out by two researchers with extensive experience in Empirical Software Engineering. Several discussion meetings were held to clarify doubts that required double-checking the results. A third researcher with expertise in executing systematic reviews, validated the final set of studies. The filtering process is detailed below.

Table 2.2: Goals and procedures to support answers from RQ5 to RQ7.

RQ	Goals	Procedures
5. What kind of SECO is covered in the study: open, proprietary or hybrid?	Understanding how studies are being conducted according to the type of SECO (MANIKAS; HANSEN, 2013b).	Each study was classified according to the type of SECO it was mostly targeting.
6. If the study deals with proprietary SECO, what are the peculiarities of this scenario?	Defining characteristics of governance mechanisms adopted by proprietary SECO.	For each study classified as a proprietary SECO, we described the related scenarios and their peculiarities.
7. Is there any approach for incident management related to SECO governance?	Understanding how this theme is being addressed within SECO.	We observed if the different published studies can provide us information whether and how incident management is treated in SECO governance.

2.3.1.3 Inclusion and exclusion criteria

We adopted the following inclusion criteria to select studies: (i) studies written in English, and (ii) studies that answer at least one RQ. The exclusion criteria adopted in this study were: (i) secondary studies (e.g., systematic mapping studies and SLR); (ii) technical reports, abstracts, and whitepapers; and (iii) duplicate reports of the same study.

The literature collection started with 667 studies retrieved from the digital libraries. The search was conducted in January 2020 and the compiled results were finished in July 2020. We did restrict the year range in our search, considering the goal of the longitudinal literature study. Initially, we removed studies that satisfied our exclusion criteria, reaching 422 studies. Next, we excluded studies based on titles and abstracts that did not satisfy our inclusion criteria, obtaining 104 studies. In the following, we read the full texts, reaching 36 primary studies that were likely to answer at least one RQ. Finally, a quality assessment (BRHEL et al., 2015) (ALVES; OLIVEIRA; JANSEN, 2017) was performed and we included 20 studies for data extraction. Studies S90 to S109 were found in our work after the first SLR period, as shown in Appendix A. Studies S1 to S89 were indicated in the SLR of Alves *et al.* (ALVES; OLIVEIRA; JANSEN, 2017). The steps of the longitudinal study are shown in Figure 2.4.

2.3.2 Results

2.3.2.1 RQ1: How is governance characterized in SECO literature?

Alves *et al.* (ALVES; OLIVEIRA; JANSEN, 2017) identified that the concept of governance is consolidated in the SECO literature and proposed an integrated definition for

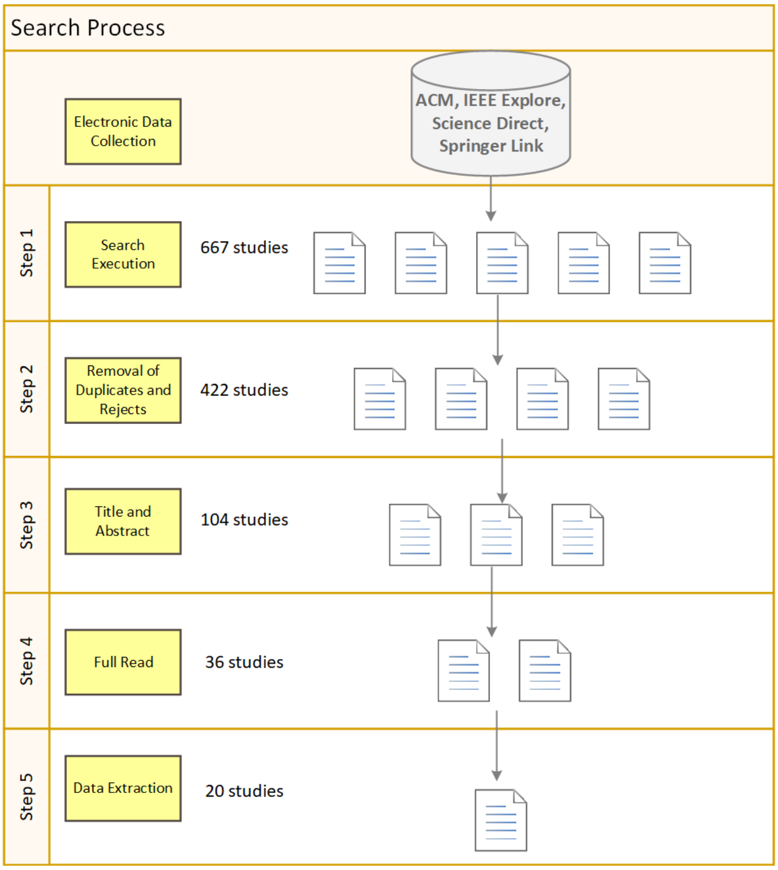


Figure 2.4: Selection and data extraction steps of the longitudinal study.

SECO governance: *processes by which a player creates value, coordinates relationships, and defines of controls*. In our work, we described SECO governance features covered in some studies. Lehtinen *et al.* [S90] are focused on megaprojects governance where several actors, such as developers, clients, and project managers, are looking for common and individual goals while delivering and exchanging values with each other.

The alignment of governance policies with detailed SECO objectives facilitates the management of the complexity of internal and external relationships ensuring the success and viability of megaprojects. Alves *et al.* [S91] discuss that keystone controls the SECO by governance mechanisms, such as establishing entry requirements, stimulating investments by partners, and sharing knowledge. Such mechanisms are vital to guarantee a strategic position in the market, becoming a challenge to survival, as it will be one of the conditions for the company to prosper or die. Pernpeintner [S93] argues that the control can be imposed by a keystone that acts as a governing entity and reinforces compliance with certain rules or can emerge from the interaction of the components themselves.

Fontão *et al.* [S95, S99] address the governance from developer experience perspective. In a mobile SECO (MSECO), keystones need to attract and engage external developers to meet users' demands. So it is necessary to evaluate the experiences of the developers during their involvement in training as a strategy to request developers to contribute to the quantitative and qualitative expansion of MSECO. The authors also used the concept of Alves *et al.* (ALVES; OLIVEIRA; JANSEN, 2017) to define the SECO governance mechanisms as management tools that aim to influence SECO health.

Regarding the study of Bogart *et al.* [S105], there is no clear definition of governance. However, the study describes procedures and processes aligning actions with the organization's strategies for greater productivity and optimization resources. This proposal is directly aligned with the SECO governance definition proposed by Baars and Jansen [S4] as "procedures and processes by which a company controls, changes or maintains its current and future position in SECO on all different scope levels".

Amorim *et al.* [S106] present an initial investigation on how open source software (OSS) ecosystems face different architectural challenges to expand software projects to external businesses, requiring multi-organizational governance to develop the software platform. Saarni and Kauppinen [S107] investigate activities and challenges in the planning phase of a Finnish SECO. The authors defined a governance model with the following tasks: defining the roles and responsibilities of the actors, defining decision-making practices, and creating a rule book. Fontão *et al.* [S109] investigated the importance of defining developers' governance guidelines for monitoring their behavior and experience. This study mentioned the work of Manikas *et al.* (MANIKAS; HANSEN, 2013b) arguing that decisions related to governance can influence SECO health and can result in promoting the success or contributing to the failure.

Therefore, nine studies [S90, S91, S93, S95, S99, S105, S106, S107, S109] highlighted that the notion of SECO governance is related to the concepts of health. In other words, there is an influence on the strategies and decision-making carried out by the keystones, and SECO governance guidelines can be analyzed using health metrics.

2.3.2.2 RQ2: What are the mechanisms proposed to govern SECO?

We classified governance mechanisms in the same three categories proposed by Alves *et al.* (ALVES; OLIVEIRA; JANSEN, 2017): i) value creation; ii) coordination of players; and iii) organizational openness and control. Then, we compare (in percentage terms) the most cited mechanisms in the new studies with the most cited ones by Alves *et al.* (ALVES; OLIVEIRA; JANSEN, 2017).

We verified that the recent results differed from those found previously. In both studies, the most cited mechanisms were: *attract and maintain partners* corresponding to 31% (ALVES; OLIVEIRA; JANSEN, 2017) and 55% (ours) of the studies in the value creation category, and *share knowledge* corresponding to 22% (ALVES; OLIVEIRA; JANSEN, 2017) and 45% (ours) in the organizational openness and control category. However, in the coordination of players category, we had a changing: the most cited mechanism is *nurture collaborations* corresponding to 50% (ours) instead of *define rules to manage relationships*, 19% and *establish roles and responsibilities*, 19% (ALVES; OLIVEIRA; JANSEN, 2017). Figure 2.5 shows the percentage of citations for each mechanism in the context of each study.

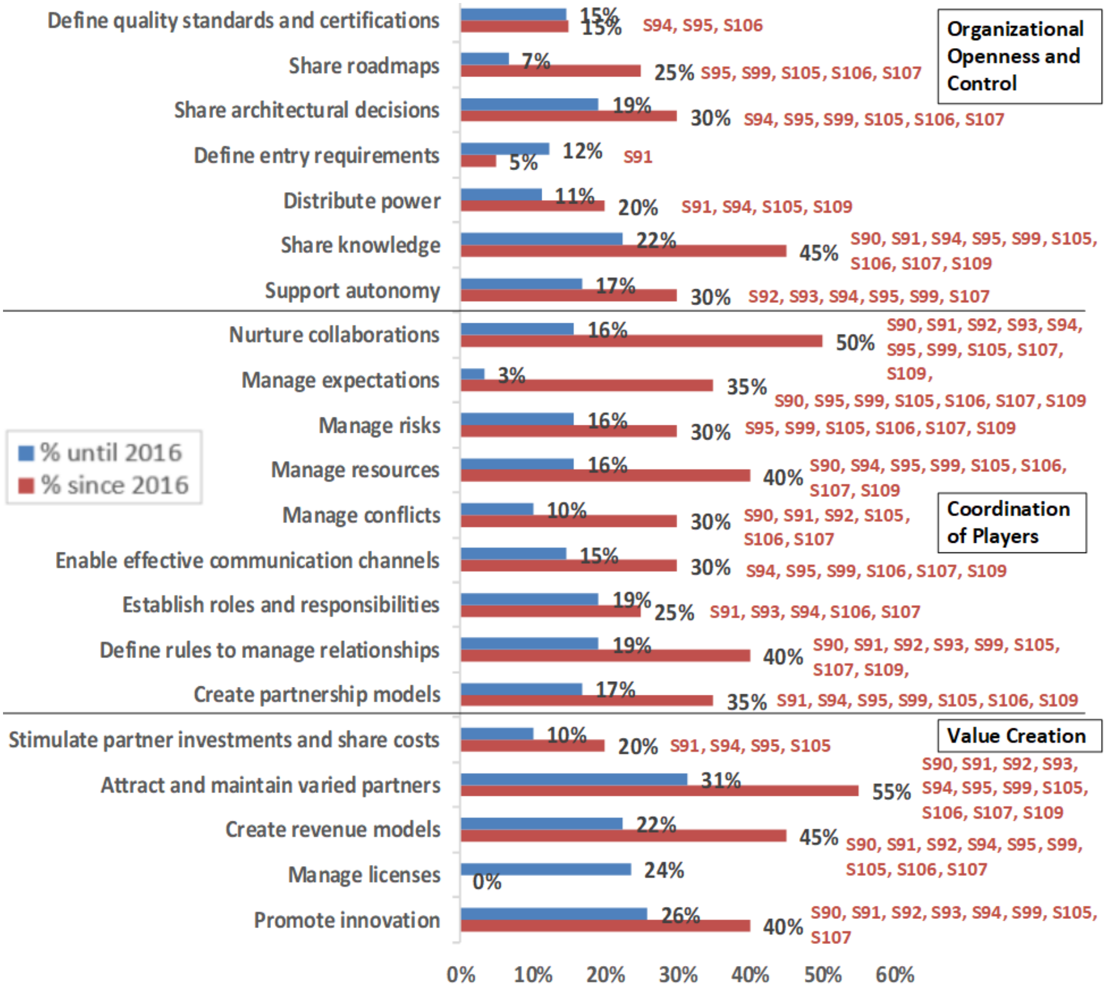


Figure 2.5: Governance mechanisms update.

2.3.2.3 RQ3: How is health characterized in SECO literature?

Iansiti and Levien introduced the concept of ecosystems' health (IANSITI; LEVIEN, 2004a) using the concept of Business Ecosystems. The authors analysed how the network structures could be more effective and how such effectiveness could be measured. Health is a term originally formulated in the field of natural ecosystems and many authors use analogies from Biology to explain that the health of business networks depends on relationships among ecosystem actors, similarly as in nature.

An indication of how health definition changes is the number of citations. In terms of quantity, we found the definition *can be measured as productivity, robustness and niche creation* remains the most cited, corresponding 50% of our studies. However, we noticed an upward trend in the definition *the ability to provide durably growing opportunities for its members and for those who depend on it*, being the highest percentage increase in our research, corresponding to 30%. Figure 2.6 shows the percentage of citations for each health definition.

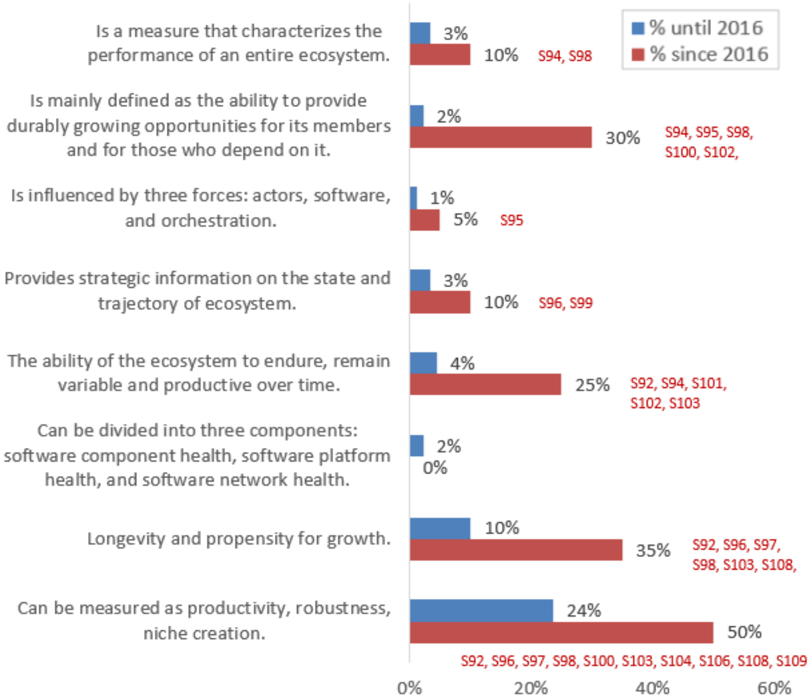


Figure 2.6: Ecosystem health definitions.

2.3.2.4 RQ4: What are the metrics proposed to assess the SECO health?

The SECO health is closely connected with the performance of each participant as well as the whole ecosystem. A healthy SECO provides durably growing opportunities for its members and for those who depend on it (IANSITI; LEVIEN, 2004a). This definition was built from the analysis of three aspects based on the biological ecosystem's symbolism (i.e., robustness, productivity, and niche creation).

Robustness represents the ability of the ecosystem to face and survive perturbations and disruptions. The ecosystem must confront and overcome difficulties from environmental changes. Productivity is the capacity of the ecosystem to rapidly transform inputs into new products and capabilities. Niche creation is the ability to support the variety and diversity of several types of organizations working with high productivity and also adding value to the ecosystem. For each aspect of ecosystems' health, Iansiti and Levien presented a variety of metrics to measure the health status (IANSITI; LEVIEN, 2004a).

Defining and controlling the SECO health are important factors and such control can be accomplished by defining metrics and evaluating them as well. The previous SLR (ALVES; OLIVEIRA; JANSEN, 2017) presents a classification of health metrics proposed by the primary studies and the metrics were identified and classified into the three health indicators (productivity, robustness, and niche creation). In our procedure for synthesizing evidence, we started filling the table with items that were explicitly cited as health metrics by primary studies, or we included data that were closely related to the health metrics.

Wang *et al.* [S92] propose a new type of evaluation that could be applied to the health of OSSE (Open Source Software Ecosystem). The study considers three aspects: commercial, product, and collaboration quality. An evaluation framework for OSSE was built. In addition to the basic information of developers, it is noticed that users should also be investigated for identifying some indicators.

The studies dealing with cryptocurrency ecosystems [S96, S97] identified a new metric on the productivity aspect: the number of forks. Forks happen when a developer starts an independent project based on the code of an existing project, without discontinuing the first one. Forks are considered good for the health of the cryptocurrency ecosystem, as they represent the updates or changes that a cryptocurrency's code receives.

We evaluate and compare the metrics pointed out as the highest number of citations in our study. Regarding productivity, the metric with the highest percentage of citation in the study of Alves *et al.* (ALVES; OLIVEIRA; JANSEN, 2017) was *Active contributors/developers* corresponding to 20% of studies. This trend remained in our research: this metric was mentioned in 70% of the selected studies, as shown in Figure 2.7.

Regarding robustness, we observed a change in the ranking of citations of metrics. In the study of Alves *et al.* (ALVES; OLIVEIRA; JANSEN, 2017), the most cited health metric were *Connectedness* and *Number of partners/Community building* corresponding each one to 15% of the studies. However, in our research, the highest citation was *Community building/Partnership model*, corresponding to 50% of the studies, as shown in Figure 2.7.

Finally, regarding niche creation, we also verified the ranking of citations of metrics. In the study of Alves *et al.* (ALVES; OLIVEIRA; JANSEN, 2017), the health metric *Openness/transparency level* was the champion, corresponding to 21% of the studies. However, in our research, this metric is in fourth place and the metric *Variety* gained importance corresponding to 65% of the studies, as shown in Figure 2.7.

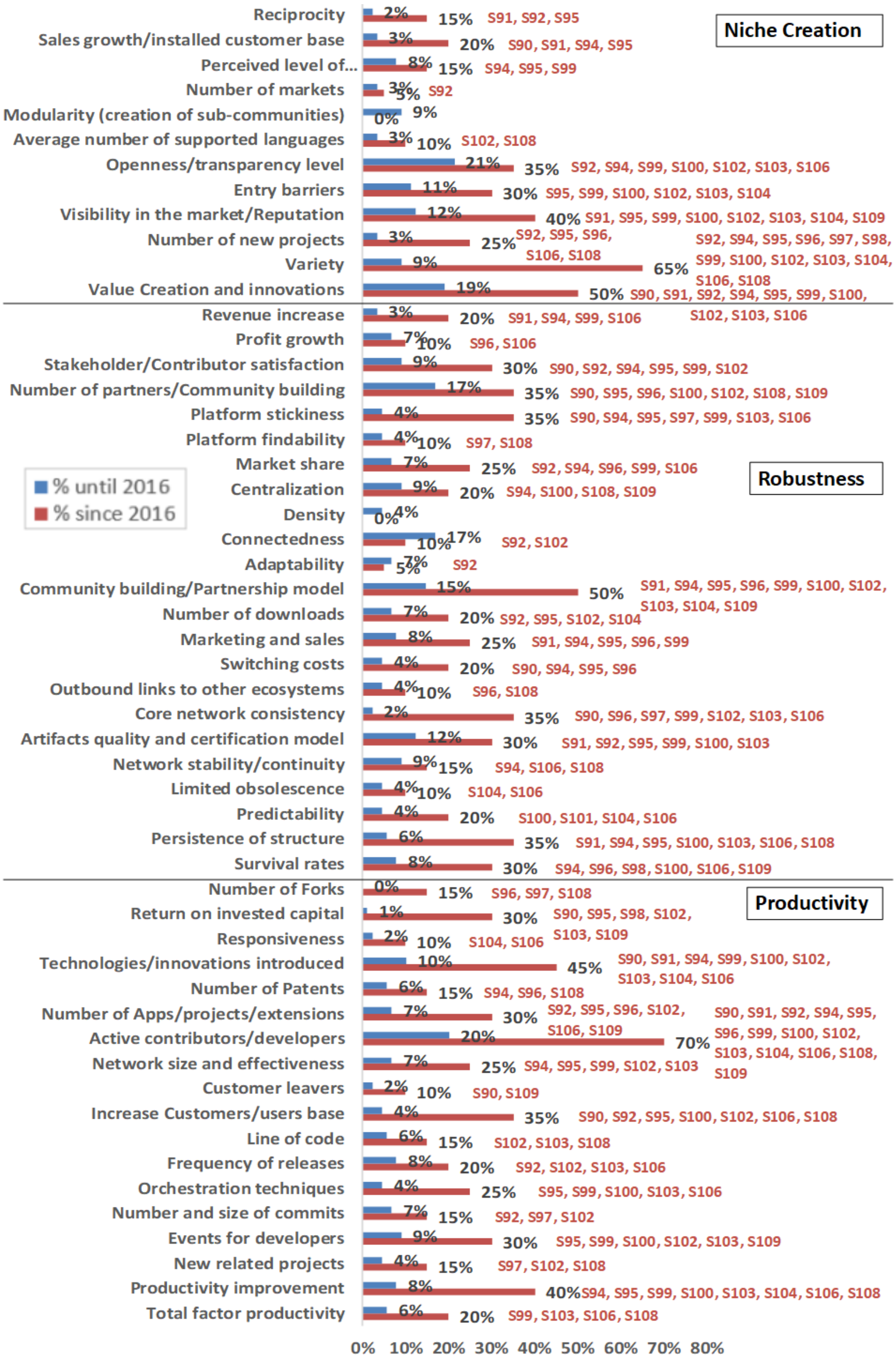


Figure 2.7: Productivity, Robustness and Niche Creation health metrics update.

2.3.2.5 RQ5: What kind of SECO is covered in the study: open source, proprietary or hybrid?

We used SECO classification approached by Manikas and Hansen in a which a proprietary ecosystem has the source code and other artifacts protected, as they are the products that would yield revenues to the ecosystem, while new actors would probably have to be certified in some way to participate in the ecosystem (MANIKAS; HANSEN, 2013b).

In a traditional free open source software (FOSS) ecosystem, the actors do not necessarily participate to obtain direct revenues from their activity in the ecosystem, while it is often much easier for an actor to participate in a FOSS than a proprietary SECO (MANIKAS; HANSEN, 2013b). A hybrid SECO supports proprietary and open source contributions and will be the majority.

According to the study of Manikas and Hansen (MANIKAS; HANSEN, 2013b), there is not much research in proprietary SECO, also due to the difficulty of access to data from these environments. Our work covered all the studies, including the SLR of Alves *et al.* (ALVES; OLIVEIRA; JANSEN, 2017). Figure 2.8 shows these results and indicates that the least amount of research takes place in proprietary SECO in both works.

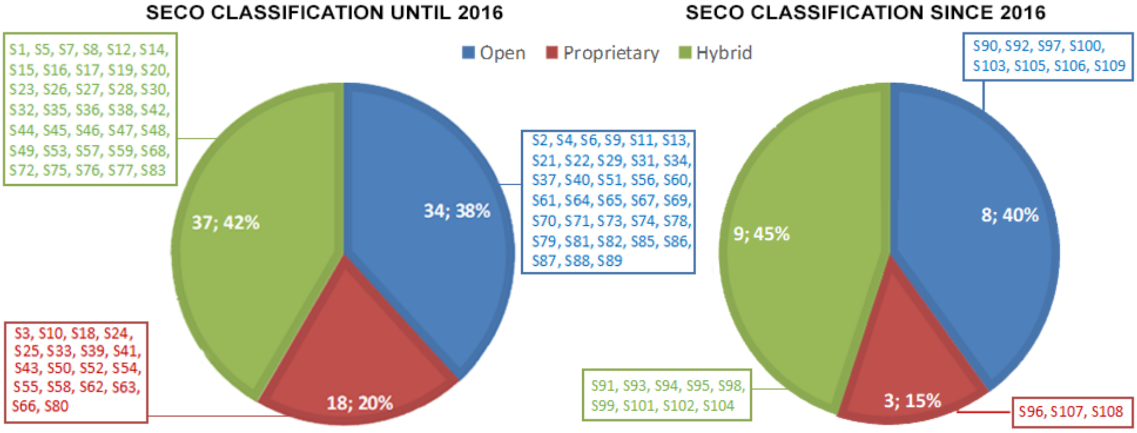


Figure 2.8: Comparison between SECO classification studies from Alves *et al.* (ALVES; OLIVEIRA; JANSEN, 2017) and our work.

2.3.2.6 RQ6: If the study deals with proprietary SECO, what are the peculiarities of this scenario?

The business structure defines the SECO characteristics that make it possible to identify some means of creating value. Proprietary SECO has less research due to the protection of data in this type of ecosystem. While in FOSS ecosystems the contributions are open and public with recognition through knowledge or personal satisfaction, in proprietary SECO the recognition is done through financial compensation and is protected by intellectual property processes. We examined peculiarities in all selected studies.

Axelsson *et al.* [S3] provided a characterization of the mechanisms that need to be present for the success of federated embedded systems (FES). Dittrich [S11] presented a health measurement instrument for business ecosystems in the Dutch IT industry. Gawer and Henderson [S18] explored Intel's strategy about complementary markets for microprocessors highlighting the organizational structure and its processes.

Huang *et al.* [S24] investigated whether intellectual property rights are effective in encouraging an independent software vendor to become certified into proprietary software platforms. Iansiti and Levien [S25] explored some reasons for Microsoft and WalMart's excellence in modern business. The authors claim that these networks of companies formed ecosystems with different actors, including suppliers, distributors, third parties, product manufacturers, technology suppliers, among others. Such ecosystems are still poorly understood and managed, requiring further research.

Jansen [S33] presented the challenges and efforts of technology companies when opening their products to promote an active developer around a common technology platform. In this study, a case study of a leading communication technology company that opened its platform across eleven product lines was investigated. In turn, Manikas *et al.* [S39] discussed the governance challenges of healthcare applications citing as an example the Happtique company, a virtual market and a distribution platform that took the task of providing certifications for medical fitness applications.

Monteith *et al.* [S41] evaluated a conceptual ecosystem health framework in the context of a research consortium that manages the production of network analysis tools, called Cytoscape Consortium. Schultis *et al.* [S50] presented a detailed case study on the collaboration and architecture challenges in two large-scale software projects at Siemens, which involved a set of internal organizational units with independent profit centers. The authors defined these systems as an Internal SECO (ISECO).

Van Angeren *et al.* [S54] investigated the inter-organizational relationships between commercial platform application developers through a comparative study of four ecosystems: Google Apps, Microsoft Office365, Google Chrome, and Internet Explorer. Viljainen and Kauppinen [S58] investigated management practices that support software integrators in SECO platforms in the telecom industry. Wnuk *et al.* [S62] addressed the hardware-dependent SECO governance applied by Axis, a producer of network video and surveillance cameras.

Ben Hadj Salem Mhamdia [S66] proposed an assessment of five dimensions of SECO health in a Tunisian company: robustness, productivity, interoperability, satisfaction, and creativity of stakeholders (customers and employees). Lucassen *et al.* [S80] also presented a method to measure the SECO health with eight different Platform as a Service (PaaS) providers. Boshuis *et al.* [S96] and Berkhout *et al.* [S108] addressed research topics related to the effects of business strategies on the SECO cryptocurrencies health: Ripple, Ethereum, Litecoin, IOTA, and Zcash. Finally, Saarni and Kauppinen [S107] aimed to investigate activities and challenges in the planning phase of a Finnish SECO.

2.3.2.7 RQ7: Is there any approach for incident management related to SECO governance?

Our research aimed to identify whether the selected studies dealt with SECO incident management. We did not identify any study that directly addressed it, which leads us to conclude that this is a subject that is still little explored in the SECO literature. Among our findings, we highlight some studies that came closest to understanding this question but did not deal directly with the topic.

Wang *et al.* [S92] and Boshuis *et al.* [S96] compare the SECO health metrics with the ecological ecosystems. Both ecosystems have participants who are collaborating and competing with each other for finite resources that can cause other participants to be included or excluded from the ecosystem. However, a participant may decide to enter, exit, or even destroy the ecosystem, whereas participants are an involuntary part in a natural ecosystem.

These authors state that a healthy ecological ecosystem must be stable and sustainable. The stable characteristic means a perception linked to the fact that it simply “works as it should” with predictable behavior, causing no problems for users. This perception is obtained from those who use the system. Regarding the sustainable characteristic in SECO, studies address the longevity of information and systems focusing on mitigation actions, disruptive techniques, and controls to deal with technological and socioeconomic changes, particularly obsolescence threats.

2.3.3 Discussion

2.3.3.1 Governance definitions

Examining the results of the analysis, we noticed that the concept of governance is gaining importance in SECO literature as pointed out by Alves *et al.* (ALVES; OLIVEIRA; JANSEN, 2017). Governance definitions are also found in studies with terms related to management and orchestration, but no specific one for proprietary SECO.

The term governance is directly linked to strategy. Once knowing the SECO strategy, it will be possible to define a set of practices to guide managers in decision making, reaching these objectives. This concept was created to elaborate and plan objectives in order to give competitive advantages to keystones in a SECO. However, in the selected studies, a field that has not been covered refers to the organization strategies and decision making in SECO or the main IT governance frameworks. These strategies must be considered as confidential and security assets that should not be publicly exposed.

Existing frameworks for traditional IT management have reached a high degree of maturity. Tools and models such as ITIL, COBIT, CMMI, and PMBOK contribute to control the risks and information flows associated with the conduct of business processes in organizations (RAMLAOUI; SEMMA, 2014). So, based on the SECO governance definition proposed by Alves *et al.* (ALVES; OLIVEIRA; JANSEN, 2017) and the previous analysis of RQ1, we advance on a proprietary SECO governance definition: *"set of practices and guidelines conducted by the keystones aiming to protect intellectual property while supporting the actors in generating revenue for the ecosystem through strategic business decisions"*.

2.3.3.2 Governance maturity and evolution

Based on RQ2, in the value creation category in which mechanisms are generally proposed by the keystone, generating and distributing value to the entire ecosystem (including partners and customers), more than half of the new studies mention the governance mechanism *attract and maintain diverse partners*. So, it is the most cited mechanism of all categories, with 11 occurrences.

Value creation can be attractive for developers and suppliers willing to obtain financial advantages and to form commercial suppliers. Its importance is due to discussions on how the value will be shared between the several parties involved. It is an important principle that participation must be attractive to those involved to sustain an ecosystem (WILLIAMSON; DE MEYER, 2012).

We observe in the category of coordination of players that the governance mechanism *nurture collaborations* had a percentage increase of 34% of citations. As mentioned before, this category is responsible for aspects of coordination and integration of activities, planning, and ecosystem structures, both for customers and partners. It was the biggest increase in citations found among all the mechanisms of our research.

A strategy for the keystone survival is to encourage collaborative and complementary relationships with suppliers and customers so that it becomes a competitive advantage in the market. It is one of the reasons why this governance mechanism stands out. Collaboration is the starting point for bringing together the skills of actors in an ecosystem. Maintaining a healthy partnership is the key to winning a successful association and avoiding undesirable risks, as a way to resist market uncertainties (IANSITI; RICHARDS, 2006).

In the organizational openness and control category, the governance mechanism *share knowledge* remained prominent compared to the previous work (ALVES; OLIVEIRA; JANSEN, 2017), with an increase of 23% in citations. The keystone has challenges in how to distribute knowledge correctly with easy access to all members. These partnerships enable the sharing of knowledge and technology, increasing innovation and making the company an attractive partner. The interaction among partners raises the need for knowledge management to support efficient propagation of information.

2.3.3.3 Health metrics maturity and evolution

Iansiti and Levien introduced the concept of ecosystems' health and drew an analogy with biological ecosystems. They argued that SECO health should be assessed based on three indicators: robustness, productivity, and niche creation (IANSITI; LEVIEN, 2004a). For the SECO keystones, the concrete information of the health indicators provides more correct decisions and more peace of mind to make the necessary adjustments. Iansiti and Levien presented a variety of metrics for each aspect of ecosystems' health (IANSITI; LEVIEN, 2004a). The indicators can be divided into groups that reflect SECO business conditions.

Based on the previous analysis of RQ4, in which robustness represents the ecosystem's ability to face and survive to radical changes, the most prominent governance mechanism is the *community building/partnership model*. Investing in building communities focused on your products and services is one way to engage a group of people. Keystones must offer and promote a creative space for building connections between actors with common interests in SECO while identifying the needs of these actors to propose efficient solutions for all involved.

Thus, creating a community, attracting new people, promoting dialogues, increasing engagement, producing content, encouraging collaboration, and strengthening ties between its members has become an even greater challenge for platform leadership. There is a need to build a space that allows these interactions and that helps to establish partnerships between developers and other actors. The network of relationships of a SECO must be strong. This scenario increases the opportunities for collaboration and facilitates partnerships between the ecosystem actors, including IT managers, developers, contributors, and other stakeholders who form an important indicator of ecosystem health. If this indicator is not satisfactory, SECO may be close to ending.

Regarding productivity, in which an ecosystem converts and transforms inputs into new products and new capabilities, an indicator that has become important to measure the ecosystem health is the *active contributors/developers*. An active developer is defined as a developer who has committed one or more lines of code to the respective repositories within the last two years. The more active collaborators/developers consuming and using the technological platform, the greater the collaboration within the community, the more people analyze and test each part of the software, aiming to guarantee higher quality for the platform as a whole. The number of active developers shows how dependent an ecosystem is on individual developers and how it is being recognized in the market.

The developers form groups of people with common goals who come together with the intention of sharing ideas, scheduling meetings, and discussing new technology trends. These actions increase an ecosystem's ability to produce meaningful results and improve its reputation. By increasing the community, the updates and new versions of the software assets (applications, services, and documentation) that make up this technological platform maintained by keystone will always be released. This means that there will be patches available for eventual failures and updates with improvements to the system. In this context, Fontão *et al.* [S95] consider that developer governance is a research topic to be investigated, approaching how keystones should maintain Developer Relations teams working closely with developers and supporting them in their activities and contributions.

Finally, niche creation, focusing on the ability of an ecosystem to support the variety and diversity of different organizations creating valuable resources, an indicator of relevance is the *variety*. One of the challenges faced by the keystone is to be able to attract and maintain a variety and diversity of applications in SECO. The ecosystem should provide the structure for creating new features over time, increasing the diversity among SECO members products.

2.3.3.4 Incident management

The unavailability of some software assets (i.e., service or component) that comprise a SECO platform is a factor that affects the organization's credibility and reputation - but it can be avoided. Therefore, the causes of unavailability must be a constant concern of the IT management team. Such incidents (i.e., unplanned interruptions of software assets) can compromise companies, whether in the brand or financially (CREEDEN et al., 2013).

Incident management is an activity whose main objective is to restore the normal service operation as quickly as possible, minimizing losses to the business operation and thus ensuring the best level of service and availability (CUSICK; MA, 2010). SECO may face difficulties in the lack or deficiency of an incident management process, causing an imbalance in internal and external relationships (LUCIANO; TESTA; AZEVEDO BRAGANÇA, 2012). Managing IT services, from the strategic plan to incident management on the technology platform, is a challenge that a keystone must face and we have not verified any study that addressed practices, processes, or tools to deal with this theme.

Based on the previous analysis of RQ7, we have identified that this research field is not covered in the body of the SECO literature. In the SECO scenario, an IT service is a means of enabling the co-creation of value between actors in the ecosystem, including IT managers, developers, customers, and the organization as a whole. This concept is proposed by ITIL (Information Technology Infrastructure Library), one of the most recognized frameworks on IT service management in the world (MCNAUGHTON; RAY; LEWIS, 2010). This framework establishes a set of best practices that must be adapted to the context and maturity of each keystone and could be adopted in a SECO.

2.3.4 Threats to validity

As limitations of this study, we extended a previous SLR and considered the same protocol. The results may be affected by the researcher bias in the study selection. Another identified threat is the classification schema and the way we established relations between them. To avoid bias, we follow some procedures indicated by Petersen *et al.* (PETERSEN; VAKKALANKA; KUZNIARZ, 2015). However, other reviews can have other classification schema and ways to group and analyze the studies.

To mitigate the both risks that may have affected the results, when there was doubt about the inclusion of any governance mechanism or health metric, there was a debate with other experienced researchers on performing mapping studies, so that we reached a common understanding. Although a broad inspection could be performed, different reviews have already pointed the lack of work on proprietary SECO (ALVES; OLIVEIRA; JANSEN, 2017) (MANIKAS; HANSEN, 2013b). To ensure a consensus on the comprehension of the selection criteria, the study protocol was also discussed among researchers.

As internal threats, we can consider the subjective decisions that might have occurred during primary studies selection and data extraction. Some relevant studies may not be selected as primary studies. In order to minimize this threat, we follow a study plan guided by inclusion and exclusion criteria. The longitudinal literature protocol was reviewed by researchers with large experience in Empirical Software Engineering and in planning/executing of systematic reviews.

2.3.5 Conclusion

This section presented a longitudinal literature study on SECO governance. We extended the previous SLR performed by Alves *et al.* (ALVES; OLIVEIRA; JANSEN, 2017) and included the related literature from 2016 to 2020 with three main objectives: i) providing an update on the SECO governance mechanisms and SECO health metrics; ii) analyzing the evolution of proprietary SECO; and iii) exploring the SECO incident management process. 667 studies were retrieved between 2016 and 2020, from which 20 were selected after applying the review procedures. The set also comprised 89 studies from the previous SLR.

Considering the governance mechanisms identified in the value creation, coordination of players, and organizational openness and control categories, we realized a trend of change. The governance mechanism *nurture collaborations* belonging to the coordination of players category had the highest percentage increase considering the number of citations from the studies. In other categories, the governance mechanisms *attract and maintain varied partners* and *share knowledge* remained the most relevant. Concerning incident management, a keystone must face the challenge of how to reduce the fragility of the technology platform.

Exclusively for the context of proprietary SECO, the governance mechanism *promote innovation* was the most prominent and is convergent with general findings of Alves *et al.* (ALVES; OLIVEIRA; JANSEN, 2017). To provide an additional body of knowledge to proprietary SECO governance bound to practical contexts, we performed a rapid review study as described in Section 2.4.

2.4 Rapid review study

Choosing the right ecosystem strategies and governance mechanisms is a life-or-death decision for keystone organizations and it is not an easy task (HARTIGH; TOL; VISSCHER, 2006). The efficient development of governance mechanisms can result in a sustainable and healthy ecosystem. On the other hand, the absence of these mechanisms may lead to failure (HARTIGH; TOL; VISSCHER, 2006).

An investigation was conducted into the challenges of finding a way to structure the incident management strategies used in an organization's day-to-day activities to guarantee the business and process evolution in the proprietary SECO context. This study had the collaboration of a large international organization's practitioners. We performed a rapid review study of handling the incident management to identify factors, drivers, benefits, and challenges. 293 studies were retrieved, from which 23 were selected after applying the review procedures. The results of this study were submitted to an international software engineering journal (COSTA; FONTÃO; SANTOS, 2021c). This section details the research method, results and discussion.

2.4.1 Research method

Rapid Reviews (RR) are practice-oriented secondary studies (WATT et al., 2008) (HABY et al., 2016) (POLISENA et al., 2015) (TRICCO; LANGLOIS, et al., 2017). The main goal of a RR is to provide evidence to support decision-making towards the solution, or removing issues that practitioners face in practice - in our study, incident management in Information Systems area covering proprietary SECO. To support this goal and to meet practice time constraints, RR should deliver evidence in shorter time frames, when compared to Systematic Reviews (SR), which often take months to years (TRICCO; ANTONY, et al., 2015). In order to make RR compliant, some steps of SR are omitted or simplified. We used a similar protocol designed according to the guidelines of Kitchenham and Charters (KITCHENHAM; CHARTERS, 2007).

The demand for RR emerged from the alignment of the researcher's work based on a practical problem: the traditional IT processes of an organization tend to move slowly to prevent instabilities from disrupting the company's productive activities (HOCHSTEIN; ZARNEKOW; BRENNER, 2005). To get a competitive advantage over competitors, the organizations need to invest in governance strategies addressing knowledge management, software assets quality, and innovative solutions. To succeed in this initiative, the transition to a service management model framework that is concerned with the development of people, processes, and technology, such as ITIL, needed to be investigated.

2.4.1.1 Research questions

In order to investigate the keystone issues related to incident management and define strategies for modeling the incident management process, we defined four research questions (RQ), more specifically concerning factors, drivers, benefits, and challenges. To answer all the RQ, we performed the procedures shown in Table 2.3. As a protocol of RR, RQ was defined in close collaboration with practitioners and moderated by the researcher.

Table 2.3: Goals and procedures to support the rapid review study.

RQ	Goals	Procedures
1. What are the factors that influence incident management?	Discussing available viewpoints and dimensions for incident management proposed by primary studies.	According to the approach performed by the researcher, we identified which dimensions were contemplated in the study. Subsequently, we extracted the definitions and discussed the concepts of incident management.
2. What are the strategies (processes, tools, methods, frameworks) to improve incident management?	Classifying the studies propose by literature to identify standards, techniques, technologies, tools, methods, and requirements.	We identified the relevant strategies and merged them into key themes and count the number of times they appeared in the studies.
3. What are the benefits of incident management for an organization?	Finding related advantages about incident managment	We extracted the benefits and collected information for each study including relevant cases about the incident management.
4. What are the difficulties and challenges caused by the absence of incident management elements in the technological platform for the management team?	Relating difficulties linked to technical solutions for incident management	We extracted obstacles and challenges for technical solutions involving incident management.

2.4.1.2 Search process

We conducted a similar SR protocol and the procedures were performed as described in Section 2.4.1.3. Following the RR methodological characteristics (CARTAXO; PINTO; SOARES, 2020), we abbreviate the search for primary studies and conduct the RR under the agreed time frame. We used only the Scopus[2] search engine with no date filter. It searches in many of the most relevant digital libraries. We tested many different versions of the search string until we found a set that returned relevant studies. Before conducting the search, we present the possible search string to other two experienced researchers in Empirical Software Engineering, and through a feedback loop with them, we refined and defined the following search string:

[2] https://www.scopus.com/home.uri

((“software ecosystem*” OR “ecosystem*” OR “software supply network” OR “software vendor*” OR “software supply industry” OR “information system*”) AND “incident manag*”)

The extraction and analysis of data from the selected studies were carried out by two researchers. Several discussion meetings were held to clarify some doubts that required double checking the results. A third researcher validated the final set of studies.

2.4.1.3 Inclusion and exclusion criteria

We adopted the following inclusion criteria to select studies: (i) studies written in English, ii) studies must present evidence based on scientific empirical methods (e.g., interviews, surveys, case studies etc.), and (iii) studies that answer at least one RQ. The exclusion criteria adopted in this study were: (i) secondary studies (e.g., systematic mapping studies and systematic reviews), and (ii) duplicate reports of the same study.

As first step, the literature collection started with 293 studies retrieved from the Scopus digital library. Scopus digital library was chosen due to the scope of its search engine being able to cover a wide range of research studies (KITCHENHAM; BRERETON, 2013). The automatic search was conducted between March and April, 2020. In the second step, we removed studies that satisfied our exclusion criteria, reaching 287 studies. In the third step, we excluded studies based on titles and abstract that did not satisfy our inclusion criteria, obtaining 255 studies. In the fourth step, we read the full text of the studies and removed those that could not answer at least one RQ, obtaining 32 studies. Finally, a quality assessment (BRHEL et al., 2015) of each study was conducted and we selected 23 studies for data extraction. We present the complete list of selected studies enumerated from R1 to R23 in Appendix B. The selection and data extraction steps of the rapid review were shown in Fig 2.9.

2.4.2 Results

Research questions in RR are as important as in SR (KITCHENHAM; CHARTERS, 2007). However, there is a subtle difference. While SR research questions are intended to identify research gaps and provide broader insights to the research community, RR research questions are more restricted, aimed at providing limited answers to the practical context in which they are embedded (CARTAXO; PINTO; SOARES, 2020).

Therefore, once RR research questions are defined, all effort is towards answering them. In RR, results are considered useful when they help practitioners to solve or miti-

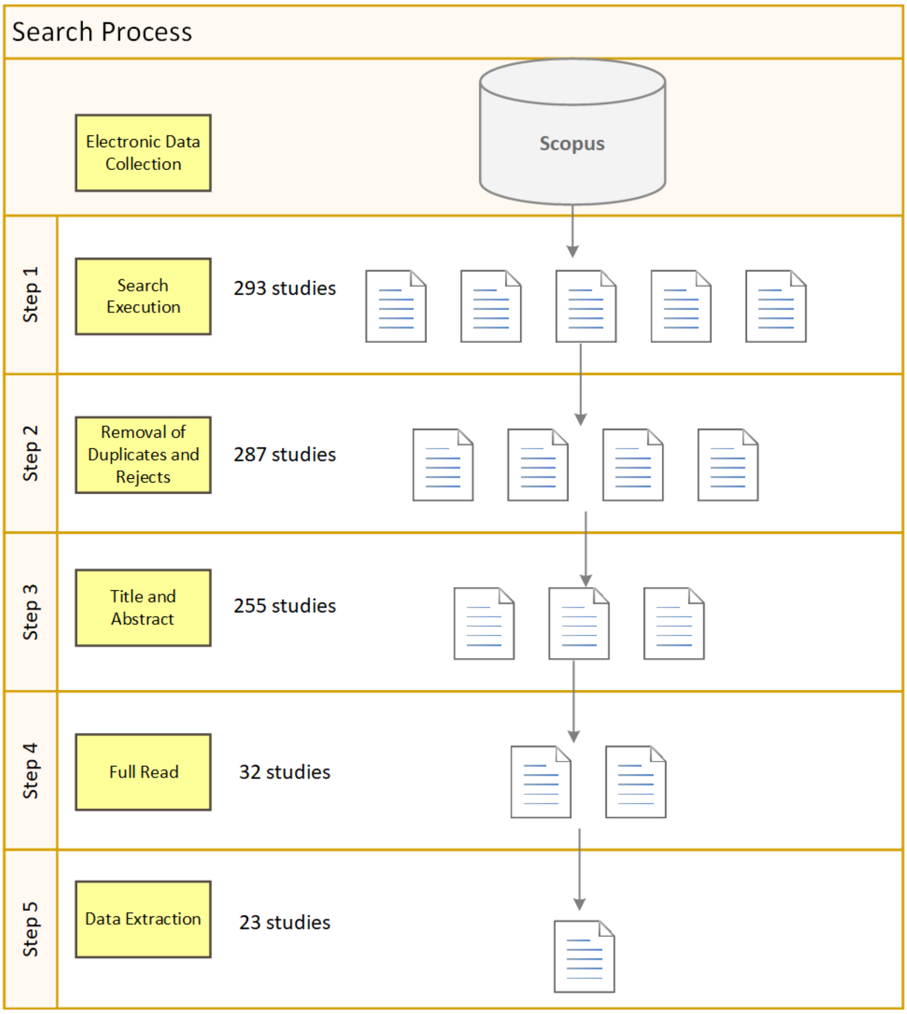


Figure 2.9: Selection and data extraction steps of the rapid review.

gate the practical problems (CARTAXO; PINTO; SOARES, 2020).

2.4.2.1 RQ1: What are the factors that influence incident management?

In this case, factors are constituted by a set of viewpoints that reveal the perceptions in software engineering studies regarding the dimensions of incident management (SOMMERVILLE; SAWYER, 1997). The viewpoints we have encountered are:

- **People:** perform a specific type of work for an organization;
- **Process:** actions or steps that need to happen in order to achieve a particular goal;
- **Technology:** activities and solutions provided by computer resources aimed at organizing the production and use of information.

In order to explain and illustrate the relationships, similarities and differences between dimensions of incident management approached in each study, we use the Venn diagram, as shown in Figure 2.10. Another factor of interest is the annual distribution of selected studies as shown in Table 2.4. It is possible to notice an increase in the number of studies in the last decade. This suggests a growing interest by the community in the field. Moreover, it indicates this topic is relatively recent in publications.

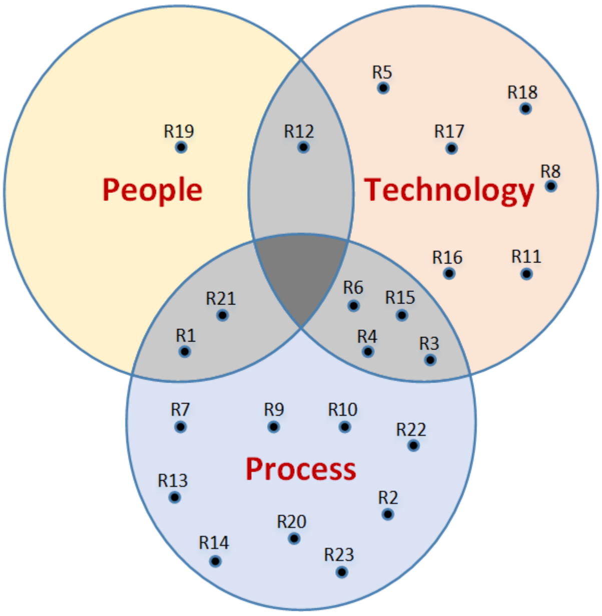


Figure 2.10: Dimensions of incident management addressed for each study.

Table 2.4: Studies published per year.

Year	Study	Total
2005	R23	1
2006	R22	1
2007	R21	1
2010	R19, R20	2
2011	R18	1
2012	R14, R15, R16, R17	4
2014	R13	1
2016	R11, R12	2
2017	R8, R9, R10	3
2018	R4, R5, R6, R7	4
2019	R1, R2, R3	3

In our study, we described features covered in some studies. Tello-Oquendo *et al.* [R1] is focused on cybersecurity incident management. An accurate definition of incident management is difficult and it can mean different things to different communities. For instance, in ITIL, incident management refers to the handling of any service disruption or interruption (VAN BON et al., 2008). In the International Standard for Information Security Incident Management (ISO/IEC 27035), it is the processes for detecting, reporting, assessing, responding to, dealing with, and learning from cybersecurity incidents

(ISO/IEC 27035). In the scope addressed in [R1], the authors considered a computer security incident as any adverse event which compromises some aspect of network security.

Amaral *et al.* [R4] noticed the processes covering ITIL framework, including incident management and monitoring indicators. One of the most relevant monitoring indicators related to this process is the completion time for incident resolution, known as "ticket completion time". According to the authors, a common reason for poor estimates is due to conduct predictions based only on a superficial understanding of the incident. In order to face this challenge, many companies are using process-aware information systems and recording events about the activities executed. The large amount of data recorded in event logs can be explored in detail through different process mining techniques, which allow to infer a more realistic process model. For example, representing the process as an Annotated Transition System (ATS) allows to estimate the process completion time based on statistics of the process model (VAN DER AALST; SCHONENBERG; SONG, 2011).

Raharjana *et al.* [R5] are focused on incidents related to IT systems in academic information systems (e.g., error when input value) or within academic scope (e.g., collision lecture schedules, damaged classroom facilities). Palilingan *et al.* [R7] also describe incidents in academic information systems that are not properly handled. Both studies claim that the most academic information systems are still focused on the main processes of universities and the incidents have not been a major concern. The studies propose the adoption of ITIL best practices to solve incidents in academic systems.

Silva *et al.* [R6] present an approach based on machine learning to automate the classification of an incident consisting on analyze descriptions written in natural language. The authors presented that incident management process requires a correct categorization to attribute incident tickets to the right resolution group aiming to have the lowest possible impact on the business. Belov *et al.* [R8] point out the effectiveness of the incident management process is determined by the speed of incidents resolution. However, the reducing the time of incidents resolution is not an easy task. It will need to consider more factors, including the queuing of incidents on the platform. The authors propose to use a management subsystem for identification and classification of incidents on the platform through a mathematical model algorithms.

Astuti *et al.* [R9] addressed the incident management hold significant role in the organization They could pose threats and risks if it is not well succeeded. Hence, identification and assessment of risks, especially risks of incident management processes, are required to avoid problem or disruption in organizational business processes and to minimize losses. The study proposes a risk mitigation analysis on incident management process in order to help strategic decisions' making.

Samopa *et al.* [R10] highlight the importance of analyzing the root cause of incidents and building a knowledge base to identify major incidents which frequently occur. The authors proposed a Work Instruction (WI) model that contains instructions on how to handle critical incidents. The result of the work is expected to be the guideline for IT Service Desk in handling the incidents. Maris *et al.* [R11] performed a case study using process mining to check if the new IT service management tool that was implemented to support the incident management resembles the ITIL processes. The goal is to create a list of relevant points of attention to make the applicability of process mining better.

Goby *et al.* [R12] investigated the benefits of business intelligence methods in order to transform implicit knowledge to explicit, accelerating business processes throughout the entire company, and retaining the knowledge of experienced employees upon retirement. The authors show how an analysis analytic can automate the assignment of Service Desk tasks, enable early warning mechanisms for incidents, and enhance knowledge sharing among Service Desk users.

Assunçao *et al.* [R14] discuss that incident management systems usually provide human resource assignment functionalities. However, the assignment poses several challenges such as, establishing priorities to tasks and defining when and how tasks are allocated to available human resources. The study [R14] evaluates the impact of task preemption on incident resolution and service level agreement (SLA) attainment.

Kundu *et al.* [R15] adressed the importance of implementing Service Level Agreements (SLA) to ensure high standards of IT service in organizations. In order to determine the current level of service, IT Sevice Desk require knowledge of the process capability of the incident management process. However, in many organizations, appropriate baseline (a clearly defined starting point for the task) of the incident management process capability do not exist. The authors point out that IT Sevice Desk are often forced to take decisions purely based on experience and subjective information in absence of any meaningful baseline capability data of the incident management process.

Tchoffa *et al.* [R17] discuss the causes of dysfunctions and problems that occur in distributed systems where they are characterized by heterogeneity and comprise several interdependent applications, whose programming is done by separate teams, without communication between them. Among the causes mentioned, the authors highlighted: i) technical (e.g., abnormal functioning of a hardware); ii) human (e.g., based on developer error code); and iii) organizational (e.g., increase of activities flow).

Bartolini *et al.* [R18] focuses on IT managers who need comprehensive decision support tools that enable them to analyze incident management operations, both at the level of the entire organization and in the single support group. The tool's challenges are: i) verifying the effectiveness of the incident resolution operational process by through indicators and metrics, and ii) obtaining an assessment architectural improvement insights.

Silva *et al.* [R19] report that the main responsible for ITIL implementation project failures is people's resistance to change. The authors suggest that organizations can have the best and most streamlined processes ever designed, but if the people do not have skills to execute them, the processes are useless, and vice-versa. Pereira *et al.* [R20] proposed a maturity model to assess an ITIL implementation. The authors addressed that the main problem resides in the fact that ITIL dictates to organizations "what should do" but is not clear about "how should do".

Muhren *et al.* [R21] performed a case study at a large European financial services provider in IT Incident Management process. The authors investigated how people involved in a process of such a mainstream organization, where reliability is of great concern, can learn from High Reliability Organizations (HRO). HRO are organizations that have histories of very safe operations although they operate in environments where accidents could have an enormous impact, such as aircraft carriers and nuclear industry. The authors also noticed that HRO invest more money in training people to recognize and respond to anomalies than other organizations. In order to reduce incidents, mainstream organizations should follow the same path.

Van Den Eede *et al.* [R22] present a dynamic model of the performance of an organization's incident management process as determined by the capability of its supporting emergency response information system. The authors propose concepts of adaptability, control, implicit knowledge and explicit knowledge in order to achieve improvement in the incident management process. However, care must be taken with the dilemma "work hard" versus "work smart".

Bandara *et al.* [R23] considered a case narrative on how a leading Australian Finance organization has utilised contemporary Business Process Management (BPM) concepts for improving the incident management processes within the whole organization. Some factors are recommended by the authors, such as: i) having a consistent process with handling incidents in all departments; ii) having a clear identification of incidents; iii) having a cleaner process flow; and iv) ensuring all information is collected at first call.

Therefore, only a few studies [R1, R12, R19, R21] linked the factors to the people dimension. On the other hand, there is a great influence on the process dimension studies. An indication of how the popularity of a research field changes is the number of publications per year. We notice that the number of publications has been increasing since 2016 and an increasing popularity of IM field.

2.4.2.2 RQ2: What are the strategies (processes, tools, methods, frameworks) to improve incident management?

RQ2 is motivated by the need to identify processes, technologies or tools, and methods which are generally used to provide solutions in incident management. The results obtained are summarized in the Table 2.5. All studies used at least one method or process or tool related to incident management.

Table 2.5: Overview of the strategies used in each study which "M" as a method, "T" as tool, and "P" as a process.

Strategy	Type	Study
Annotated Transition System (ATS)	P	R4
Business Process Model	P	R23
COBIT framework	M	R2, R5, R9
CRISP-DM	P	R12
Decision Programming Language	M, T	R17
DERMIS framework	M	R22
Discrete-event simulator	T	R14, R16, R18
Educational organizations framework	M	R1
ITIL framework	M,P	R7, R10, R13, R19, R20, R21
Machine learning	T	R6
Mathematical model	T	R8
Monte Carlo simulation	T	R15, R17
People Capability Maturity Model	M	R19
ProM framework	M	R11
SVN, SonarQube, Jenkins, Cerberus	T	R3
Topic modeling	T	R12
Work instruction	T	R10

The study [R1] proposed an incident management framework that is adaptable to educational organizations and allows them to improve their management processes in the face of computer incidents, focusing in cybersecurity incident management. The studies

[R2, S5, S9] indicated COBIT framework as a standardized guideline to the management of handling incidents which includes issues of planning, implementing, operation, and monitoring to the whole processes of the IT.

The study [R3] describes a set of tools, such as source code repository (SVN)[3], static analysis tool (SonarQube)[4], continuous integration server (Jenkins)[5], and the in-house continuous testing tool, named as Cerberus, to allow a complete solution in order to address issues and incidents to the sustaining team. [R4] deals with process mining using Annotated Transition System (ATS) method to allow the estimation of process completion time based on statistics aggregated into the process model.

The study [R6] used machine learning tools and methods to automate the incident categorization. The studies [R7, R10, R19, R20] address the use of ITIL framework to handle incidents. These studies improved incident management processes, defined the responsibilities and implementing guidelines of roles involved, and define key performance indicators. [R8] proposed a mathematical model that was used to develop algorithms for identifying, classifying, and correlating incoming incidents. The study [R10] presents a work to identify major incidents which frequently occurred throught a developed tool to handle incidents, known as Work Instruction (WI).

In [R11], ProM[6] framework was used because of the rather large number of algorithms it provides for incident analysis and the fact that conformance checking is supported. [R12] used a combination of topic modeling (machine learning technique capable of scanning a set of documents, detecting word and phrase patterns within them) and predictive analytics applied to an large dataset of incident tickets. The authors followed the CRISP-DM[7] guidelines.

In [R14], the authors investigated the effects of different ticket dispatching policies and developed a Discrete Event Simulator (DES)[8]. Also using DES techniques, the studies [R16, R18] presents Symian, a decision support tool for the improvement of incident management performance. Symian supports IT managers to assess and improve the per-

[3] Apache Subversion, abbreviated as SVN, is a centralized version control system.

[4] Also known as Sonar. It is an open-source platform developed by SonarSource for continuous inspection of code quality to perform automatic reviews with static analysis of code to detect bugs, code smells, and security vulnerabilities.

[5] Jenkins is an open source automation server which enables developers around the world to reliably build, test, and deploy their software.

[6] Short for Process Mining framework. It is an extensible framework that supports a wide variety of process mining techniques in the form of plug-ins.

[7] Stands for Cross Industry Standard Process for Data Mining. It provides a structured approach to planning a data mining project.

[8] DES models the operation of a system as a sequence of events in time.

formance of the organization.

The study [R15] presents the details on how Monte Carlo[9] simulation was used for determination of incident management process capability. [R17] proposed a method to manage incidents in information systems using Decision Programming Language (DPL 5.0)[10] and Monte Carlo simulation. The goal of study [R19] is to reduce resistance rates by creating a framework that uses People Capability Maturity Model[11] to overcome real organizational problems faced throughout the ITIL processes implementation.

The study [R22] presents DERMIS[12] framework to improve the performance of an organization's Incident Management process as determined by the capability of its supporting emergency response information system. [R23] documented how Business Process Management (BPM) concepts were utilized to improve the IT incident management processes within the entire organization.

2.4.2.3 RQ3: What are the benefits of incident management for an organization?

Table 2.6 shows the benefits of incident management according to the outcomes of this rapid review. Most of studies drives to define categories and priorities in order to speed up diagnosis and reduce delays [R6, R7, R8, R9, R10, R12, R14, R17, R22, R23].

Several studies [R9, R10, R11, R15, R21, R22, R23] discuss the benefits of incident management to have an information center relating incidents, resolutions and impacts with rich audit reports about services delivery. Other general benefits found in studies emphasize to create dashboards to solve incidents with autonomy [R3, R4, R9, R11, R12, R13, R16, R23], better quality of service [R1, R2, R4, R5, R9, R13, R16], improving user satisfaction [R5, R6, R7, R8, R13, R16, R23], and reducing business impact [R2, R3, R4, R6, R7, R8, R9, R18, R22, R23].

The studies also highlighted the benefits: providing business information in a centrally way [R1, R2, R10, R23], restoring any IT service as quick as possible [R3, R7, R8, R10, R17, R22, R23], measuring performance using indicators [R4, R8, R11, R13, R15, R18, R23], and properly employ the sustaining team to increase productivity [R1, R2, R6, R13,

[9] Monte Carlo performs risk analysis by building models of possible results by substituting a range of values (a probability distribution) for any factor that has inherent uncertainty.

[10] An application for decision analysis created by ADA Inc. and Microsoft Corporation that allows editing decision trees as well as drawing Influence diagrams, Rainbow diagrams, Vann diagrams, and Tornado diagrams.

[11] Short names: People CMM, PCMM, or P-CMM. A maturity framework that focuses on continuously improving the management and development of the human assets of an organization.

[12] Dynamic Emergency Response Management Information System framework established by Turoff *et al.* (TUROFF et al., 2004).

R14, R15, R19, R21, R23] are factors that were taken into account.

Table 2.6: Benefits of incident management perspective.

Benefits	**Study**
Automation, efficiency and proactivity	R3, R4, R5, R7, R12, R13, R17, R18
Better quality of service through improved information management	R1, R2, R4, R5, R9, R13, R16
Better use of sustaining team by prioritizing tasks, leading to increased productivity	R1, R2, R6, R13, R14, R15, R19, R21, R23
Defining categories and priorities for incidents in order to speed up diagnosis and reduce delays	R6, R7, R8, R9, R10, R12, R14, R17, R22, R23
Having a central information base relating incidents, resolutions and impacts to the objectives established in SLA through audit reports	R9, R10, R11, R15, R21, R22, R23
Having dashboards for service desk team to resolve incidents with autonomy	R3, R4, R9, R11, R12, R13, R16, R23
Improve monitoring allowing performance measurement through indicators based on SLA	R4, R8, R11, R13, R15, R18, 23
Improving user satisfaction	R5, R6, R7, R8, R13, R16, R23
Providing business information in a centrally way	R1, R2, R10, R23
Reducing business impact	R2, R3, R4, R6, R7, R8, R9, R18, R22, 23
Restoring any IT service as quickly as possible	R3, R7, R8, R10, R17, R22, R23

2.4.2.4 RQ4: What are the difficulties and challenges caused by the absence of incident management elements in the technological platform for the management team?

From the studies reviewed, Table 2.7 presents the main challenges, limitations, and difficulties regarding the absence of incident management elements. We can observe many difficulties regarding incident handling process [R5, R6, R7, R11, R12, R14, R16, R18, R22], total service fix time [R5, R6, R7, R12, R14], mapping key performance indicators [R5, R7, R11, R16, R18], and tools for data analysis [R6, R16, R18]. The studies also highlighted as difficulties: reaction time [R5, R6, R12], communication plan failure [R6, R12, R22], tacit knowledge [R5, R12, R22], and root cause analysis [R16].

Table 2.7: Challenges and limitations of incident management perspective.

Challenges and Difficulties	Study
Adopting tools for data analysis	R6, R16, R18
Agile and efficient incident handling process	R5, R6, R7, R11, R12, R14, R16, R18, R22
Communication plan failure	R6, R12, R22
Reaction time to deal with an incident	R5, R6, R12
Root cause treatment and analysis	R16
Sustaining team tacit knowledge	R5, R12, R22
Total service fix time above the desired time	R5, R6, R7, R12, R14
Tracking all key performance indicators	R5, R7, R11, R16, R18

2.4.3 Discussion

It is no coincidence that one of the observed factors refer to the PPT (People, Process, Technology) methodology in which the three dimensions are necessary for organizational transformation and management. In order to achieve organizational efficiency, it is necessary to balance and maintain good relationships among them (PRODAN; PRODAN; PURCAREA, 2015).

ITSM aims to ensure that clients have access to quality services and these services meet business needs. For that, it is necessary to invest in people, processes and technology, known as Golden Triangle. As standalone components, people, process, and technology are necessary for organizational transformation and management. In order to achieve organizational efficiency, there is a need to balance the three and maintain good relationships among them (PEE; KANKANHALLI, 2009).

In most of selected studies, we noticed an alignment among people and process strategies concerns [R7, R10, R13, R19, R20, R21]. Finding people with the right experience, qualifications, and attitude is a necessary step in implementing ITIL guidelines in IM field. The organization should make sure the information flows between the right people in the right place and trust them to make the right decisions following guiding principles of the organization. To do so, the organization should optimize the processes (TALLA; VALVERDE, 2013).

A process is a series of actions or steps that need to happen in order to achieve a particular goal. People are ineffective without processes in place to support their decisions. In accordance with ITIL best practices, incident management is a process that aims to resume service as soon as possible, causing minimal damage to the business. Based on these needs, the process should be ordered and clear with some steps to certify, such as: i) make sure people know how they fit into the workflow; ii) make sure people do the work receive proper training on the new processes; iii) make sure organization provides proper instructions; and iv) consider how you will measure the success of a process (TALLA; VALVERDE, 2013).

However, in practice it does not happen. One of the bad governance strategy pointed out in our previous study (COSTA; FONTÃO; SANTOS, 2021d) addressed that tacit knowledge is concentrated in a few people and there is no knowledge management culture. Tacit knowledge is on the employees' mind and has been absorbed daily. If the organization does not have the development of a knowledge management culture, it can be hostage from people and software consultants knowledge. Another factor is the people resistance to share knowledge. It allows the false notion that information belongs of a single owner. As a consequence, many of the problems that arise in information systems come from incidents that are not properly handled or not adequately addressed due to the failure in the process implementation, such as clear procedures and/or failure people management that still rely on individuals who work only on the basis of previous experience.

In the third element of the Golden Triangle, technology alone does not solve problems. Many studies [R3, R6, R8, R10, R12, R14, R15, R16, R17, R18] have dedicated themselves to focusing on tools to resolve some obstacles. Technology will not make existing problems go away without the people and processes around to support it. Too often, companies make an investment in technology and try to retrofit the people and processes, but that is inverse logic. This statement was corroborated in our previous study (COSTA; FONTÃO; SANTOS, 2021d) discussing the the evaluation criteria of software vendors. It is easy to fall in love with state of art of technology and the vendors who sell it. When software vendor´s deliveries are found not to be satisfactorily suited to the organization's needs, it is too late. The real value in any technology is providing improvement to business needs and promoting user's satisfaction.

Our study also highlighted several approaches focused on methods and processes for incident management. Within this context, it is important to emphasize that the points of view evolve and are perfected over time. Therefore, we join practical experience with several literature studies and proposed a mind map diagram of incident management with the following goals, as shown in Figure 2.11: i) change in perception of impact to end user; ii) speed of request attending; and iii) value creation in the services provider of IT. The main reason for choosing such tool was the potential type of diagram focused on the management of information, knowledge and intellectual capital for understanding and solving problems (NOVAK; CAÑAS, 2006).

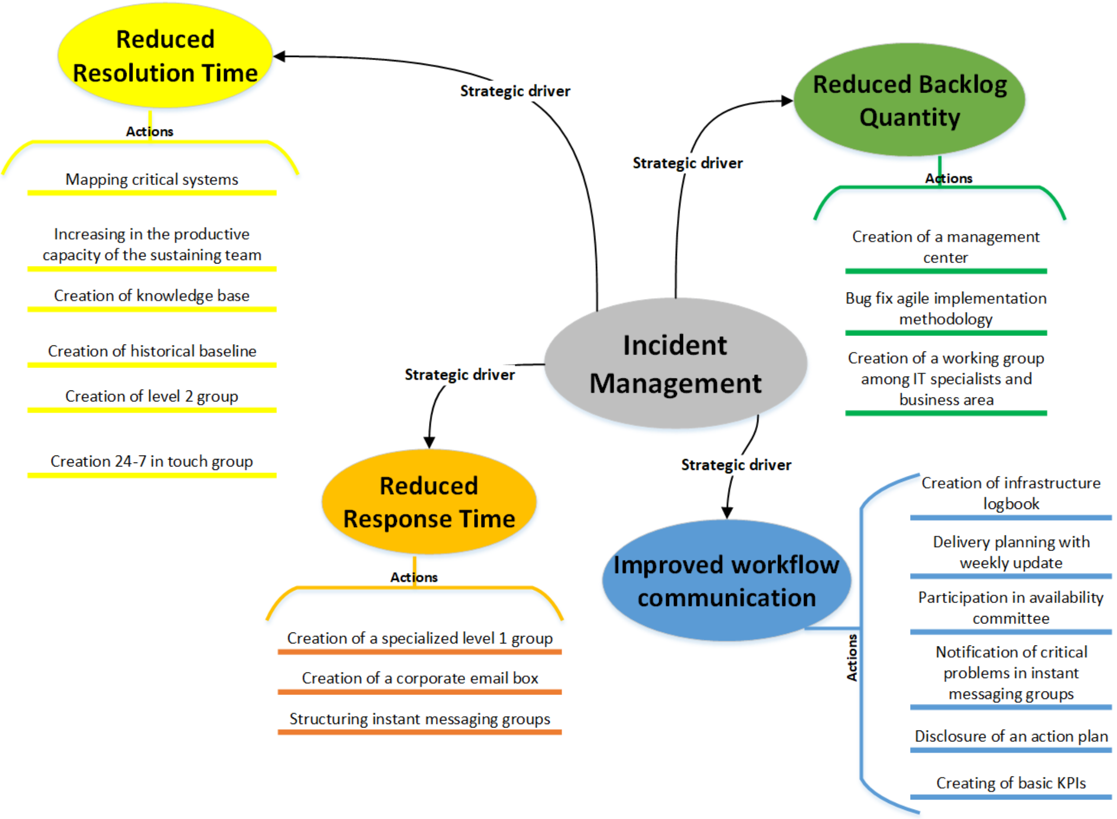

Reduced Resolution Time
Actions
Mapping critical systems
Increasing in the productive capacity of the sustaining team
Creation of knowledge base
Creation of historical baseline
Creation of level 2 group
Creation 24-7 in touch group
Strategic driver
Strategic driver
Reduced Backlog Quantity
Actions
Creation of a management center
Bug fix agile implementation methodology
Creation of a working group among IT specialists and business area
Incident Management
Strategic driver
Reduced Response Time
Actions
Creation of a specialized level 1 group
Creation of a corporate email box
Structuring instant messaging groups
Strategic driver
Improved workflow communication
Actions
Creation of infrastructure logbook
Delivery planning with weekly update
Participation in availability committee
Notification of critical problems in instant messaging groups
Disclosure of an action plan
Creating of basic KPIs

Figure 2.11: Mind map of incident management.

The four pillars known as strategic drivers define how the results will be achieved and what to govern through indicators and metrics. They establish the organizational strategy to be followed and implemented for unfolding in measurable objectives. These drivers were compiled based on practical experience in line with the rapid review selected studies. For each strategic drivers, we defined some actions to fulfil the goal.

Before detailing each of the drivers, we identified some steps for the incident management process, according to ITIL best practices:

1. *Identification* - recognition and reporting of the incident to the service desk team;
2. *Registration* - documentation of the incident reported in a ticket system or other tool used by the organization (e.g., JIRA Service Management, HP Application Lifecycle Management);
3. *Categorization* - classification of the incident according to type and specificity;
4. *Prioritization* - classification of the incident according to urgency of attendance;
5. *Initial diagnosis* - understanding of the reported incident, in order to solve it;

6. *Escalation* - delegation of the incident to a higher level of specialists, in case of first-level ones are unable to complete the diagnosis;
7. *Resolution* - incident is resolved and the service reestablished; and
8. *Closing* - final documentation and lessons learned, which can be consulted in the future and help other people.

The first driver is **Reduced Response Time**. Response time is defined as the amount of time between the user first creates an incident report and the first level specialist responds. It acts directly in the *initial diagnosis* step. This activity comprises the entire process of searching on Service Desk team for a solution.

One of the literature studies (PALILINGAN; BATMETAN, 2018) also present the absence of operational standards and procedures of incident management makes 80% of incidents only handled manually and the reaction time is not enough. Some others [R5, R6, R12] indicated the reducing reaction time to deal with an incident as a big challenge. So, in order to mitigate the problems, some actions were proposed do reduce this time, such as: i) *creation of a specialized first level group* aiming to search for answers in the knowledge base, in the company's technical procedures, together with suppliers or with their colleagues; ii) *creation of a corporate email box* aiming to prevent the message from being sent directly to a sustaining team analyst; iii) *structuring instant messaging groups* aiming to quickly address the requests.

The second driver is **Reduced Resolution Time**. Resolution time is defined as the amount of time between the user first creates an incident report and when the problem is actually solved. It is an accurate stat regarding just how quickly the incident will be solved and acts directly in the *resolution* step.

Many studies [R5, R6, R7, R12, R14] have discussed this driver, which makes it very relevant within the context of incident management. In our selected studies, the meaning for ´´total service fix time above the desired time" is a desire to reduce resolution time. Several actions are proposed in practical experience to keep the number of incidents down. There are several steps that can be taken, and when done together, can have a positive impact as following:

- *Mapping critical systems* - the knowledge and understanding of a certain process is essential to be able to analyze what are the gaps and bottlenecks of the business;
- *Increasing in the productive capacity of the sustaining team* - eliminate or delegate unimportant tasks and replace them with value-added ones;

- *Creation of knowledge base* - The knowledge base makes it possible for information about a company's products or services to be available in an accessible way for its users. It is possible to obtain advantages (e.g., providing a good customer experience, having an efficient team, and reducing costs);

- *Creation of historical baseline* - A baseline provides a stable point of the service desk incident operations;

- *Creation of level 2 group* - it is related to incident escalation. If the first level specialist does not have the necessary technical knowledge to resolve the incident, the task will be delegated to the second level of support; and

- *Creation 24-7 in touch group* - incidents do not appear by appointment. Having a trained team at any time becomes a relevant factor to resolve incidents as quickly as possible.

The third driver is **Improved Communication**. Some studies [R6, R12, R22] highlighted that a communication plan is an obstacle to the incident management. This statement is also in line with practical experience. A good incident communication allows the sustaining team managers to bring together all involved users during the hard incident events and establish quick and easy communication within this group. Some actions are proposed to booster this strategic driver, such as:

- *Creation of infrastructure logbook* - register daily operation activities of the IT Infrastructure;

- *Delivery planning with weekly update* - meet with sustaining team members to communicate the priorities and expectations for their respective roles;

- *Participation in availability committee* - stakeholders promptly updated with the latest information can take specific actions aiming to help in decision-making procedures when a crisis occurs;

- *Notification of critical problems in instant messaging groups* - in order to support and to complement other forms of communication, the sending notifications by instant messaging groups can be used to keep the stakeholders informed on the status of the incident;

- *Disclosure of an action plan* - create a transparent incident communication plan when a crisis occurs; and

- *Creating of basic KPIs (Key Performance Indicator)* - track metrics and KPIs are critical to the effective incident management and it is a way to measure the sustaining team performance.

Finally, the fourth driver is **Reduced Backlog Quantity**. The incident backlog is a metric that corresponds to the number of active/open tickets at any given point in time. It represents if sustaining team is keeping up with demand and will help to avoid a surprise with backlog growing. One of the literature studies (PALILINGAN; BATMETAN, 2018) quotes a slow resolution of incidents and in many cases are not even resolved, increasing the backlog. Some actions are proposed to reduce the backlog, such as:

- *Creation of a management center* - maintain the follow-up and evolution of incidents in a management center and check on a daily basis that each member of sustaining team has taken responsibility to progress any incidents tickets open in their personal queue;
- *Bug fix agile implementation methodology* - handle incident using agile methodology. The strategy in this approach is to deal with bugs in a separate backlog to optimize the bug fix process as quickly as possible; and
- *Creation of a working group among IT specialists and business area* - up a multidisciplinary working group with sustaining team´s developers and business analysts in order to filter incidents that do not represent errors but, rather, doubts or lack of knowledge of the end user.

Therefore our study has illustrated that the strategic drivers are a collection of people, conditions, and information that start and support activities and will help the organization to provide quality services aligned with business needs. These motivators represent the main influences or factors that matter for the success of the organization.

2.4.4 Threats to validity

The reliability of the results is directly linked to the validity of the study. Every study has threats that should be addressed and considered together with the results, considering the classification proposed in (RUNESON et al., 2012).

The results may be affected by bias researcher on study selection. To mitigate the risk about the results that may be affected by bias researcher, when there was doubt about the inclusion criteria, the matter was discussed with the others researchers and reached a common understanding.

In order to reduce cost and/or time to conduct a RR, we do not use several search engines. Our study focus was on Scopus digital library. It covers a wide research studies due to the scope of your search engine as evidenced in (KITCHENHAM; BRERETON, 2013). We perform a transparent process that allowed the practitioners to make their own assessment on validity.

Daily priorities and understanding the needs of each practitioner were other threats found in the RR. To mitigate them, the researcher was constantly present and available at any time, aiming to keep the team motivated and engaged, in order to achieve the objectives outlined in the planning of the RR study.

2.4.5 Conclusion

This section presented a rapid review study on incident management with three main goals: i) providing a body of knowledge bounded to practical problems; ii) investigating keystone's issues to handle incident management; and iii) exploring the keystone's strategies to model incident management process. 293 studies were retrieved from Scopus digital library, from which 23 were selected after applying the review procedures.

Incident management is the process of responding to an unplanned event or service interruption to restore the service to its operational state. Incidents are events of any kind that disrupt or reduce the quality of service. According to ITIL, the incident management process ensures that normal service operation is restored as quickly as possible and the business impact is minimized.

However, to support software maintainability and to keep the stable environment are quite complex tasks and require multiple skills of the sustaining team. Many studies invest only in technology and forget about the other two dimensions of the golden triangle for organizational management, such as, people and process. The tacit knowledge is concentrated on a few people. The lack of effort in implementing a process of knowledge transfer added to people's resistance to sharing knowledge contributes to incidents that are not properly handled or not adequately solved. To achieve organizational efficiency, there is a need to balance the three dimensions and the relationships between them.

We also noticed some strategic drivers to define how the results will be achieved and governed through indicators and metrics. Metrics are responsible for measuring results and need to be clear, simple and objective. It is possible to understand the behavior of strategic processes. The choice of right metrics are not easy tasks. In short, they need to be on time, have relevance, need to be useful; and easy to understand.

KPIs directly influence the drivers and are indispensable for evaluating the performance and results of the incident management process. KPIs are used to measure the performance of the processes used by an organization to achieve established objectives. They work as indicators to know if the organization managed to reach the initial objective. KPI is created from the metrics. Therefore, knowing traceable metrics and KPIs are critical to the effective IT Service Management. In our study, we concentrated on actions to reduce response time, reduce resolution time, improve workflow communication, and reduce backlog quantity.

2.5 Final remarks

This section summarizes the results arising from this chapter. The longitudinal literature study was performed on SECO governance from 2016 to 2020 as an extension of the previous SLR of Alves *et al.* (ALVES; OLIVEIRA; JANSEN, 2017). Next, we conducted a rapid review study to add to the body of knowledge around proprietary SECO governance in real scenarios.

Considering the longitudinal literature study, we noticed a trend of change in the governance mechanism *nurture collaborations* that belongs to the coordination of players category. This mechanism had the highest percentage increase considering the number of citations from the studies. Comparing the number of citations from our study with the SLR of Alves *et al.* (ALVES; OLIVEIRA; JANSEN, 2017) is a starting point of analysis in order to understand the changes in the market in recent years.

Relating to rapid review study, effective platforms are based on technological excellence but can't exist exclusively in the technology domain. To support software maintainability and to keep the stable environment are quite complex tasks and require multiple skills of the sustaining team. The technological platform governance should invest in other other two dimensions (in addition to the technical one): people and process.

Only a few people have access to tacit information. The lack of effort put into developing a knowledge transfer process, combined with people's aversion to sharing information, adds to incidents that are not appropriately managed or solved. It is necessary to balance the three dimensions and their relationships in order to attain organizational efficiency.

3. Exploratory Study

In this chapter, an exploratory study is discussed in order to identify characteristics that help us to achieve the objectives proposed in Chapter 1 based on the context described in Chapter 2. This study was published at an information systems conference (COSTA; FONTÃO; SANTOS, 2020a) and comprises an opinion survey and interviews to assess the SECO governance mechanisms applied to software asset governance in proprietary SECO based on practitioners' experience.

3.1 Introduction

The main challenges identified by the Information Systems (IS) community led to the question of how to conceptualize, build and evaluate a new generation of information systems to deal with the growing technical complexity and social diversity of contemporary society (BOSCARIOLI; ARAUJO; MACIEL, 2017). For example, aligning managers' actions with the interests of the central organization and developers, consumers and suppliers in relation to ownership of the software and related contributions (AVILA; LUCENA FILHO; COSTA FIGUEIREDO, 2017).

In this scenario, information and knowledge are concentrated around a proprietary software platform. It is an environment where the central organization provides tools and documentation for developers and IT service providers to share and reuse solutions (KUDE; HUBER; DIBBERN, 2018).

Around the platform, there are a set of relationships between companies, suppliers, and employees competing and cooperating, configuring a SECO scenario. SECO involves a set of actors functioning as a unit and interacting in a shared market for software and services, centered on a common technological platform (JANSEN; BRINKKEMPER; FINKELSTEIN, 2009). A proprietary SECO is one that depends on proprietary products, resources and projects, preserved by intellectual procedures that support the creation of value chains between users, developers and the central organization (MANIKAS, 2016), such as Platform as a Service (PaaS) and e-commerce ecosystems.

In the SECO environment, consumers and suppliers face challenges when trying to choose and maintain the technological solutions offered by the market over time (ALBERT, 2014). It has become necessary to allow expansion through contributions from external actors to the platform without the sharing of internal knowledge being exposed and undermining the robustness of the SECO. The traditional software industry is changing as a result of this scenario (SANTOS et al., 2012). The governance of software assets (components and services) in the context of proprietary SECO could be an opportunity to solve this challenge. In this context, SECO governance is a model that brings together a set of strategies (i.e., policies and guidelines) for the organization as well as the relationship between the parties (FONTÃO et al., 2018).

Thus, governing software assets, that is, establishing policies and guidelines, is a critical aspect of maintaining a sustainable SECO (ALBERT; SANTOS; WERNER, 2013), making it difficult for IT managers to always keep the systems that support the business's operation, allowing its growth (MANSUR, 2007). The purpose of this study is to investigate SECO governance mechanisms presented in the systematic literature review (ALVES; OLIVEIRA; JANSEN, 2017) applied to asset governance in the proprietary SECO of a large insurance organization, particularly in relation to managers' perceptions of relevance and the correlation between the mechanisms.

This chapter is organized as follows: Section 3.2 and 3.3 present the main research question and the research method of this study; Section 3.4 describes the survey method; Section 3.5 details and discuss the interviews with IT managers; Section 3.6 discusses the correlation results based on Pearson's coefficient; Section 3.7 reports some limitations; and finally, Section 3.8 describes the conclusion for this chapter.

3.2 Research question

The goal of this study is to investigate software asset governance mechanisms in a proprietary SECO of a large international insurance organization. The research question for this study is: *"How are SECO software asset governance mechanisms implemented in a proprietary SECO?"*.

3.3 Research method

This study analyzed the proprietary SECO scenario of a large insurance organization. The research method used in this study was conducted using empirical research guidelines. The goal of this study is to advance the investigation of SECO governance mechanisms applied to asset governance in a proprietary SECO.

The following methods were used separately: opinion surveys and interviews. Specifically, with the survey results, a correlation analysis was performed. The opinion survey was conducted in accordance with the procedures outlined by Molléri *et al.* (MOLLÉRI; PETERSEN; MENDES, 2016) and Linaker *et al.* (LINÅKER et al., 2015). The interview is a guided conversation, where the interviewer can direct the conversation according to the need for the investigation (YIN, 2017). The first method was performed to obtain a set of quantifiable data involved in the explored scenario and the second method is defined as an activity aimed at clarifying these findings.

3.4 Opinion survey

3.4.1 Planning

The objective is to verify the level of agreement regarding the importance of the software assets governance mechanisms in proprietary SECO, where the contributions are protected by intellectual property and confidentiality agreements. It was performed from the perspective of the actors (e.g., internal and external developers, project leaders, and managers) involved in asset governance in a proprietary SECO of a large organization.

3.4.2 Instrumentation

The survey was split into four sections. In the first section, an introduction paragraph was provided, which included the questionnaire's academic aims. In the second one, before accessing the questions, the participant must first read and agree/disagree with the Informed Consent Form (presented in Appendix C).

The third section intended to define the participants' academic and professional profiles: the company for which the practitioner worked (the available options were IT service providers and the organization itself); the education degree (High School, Bachelor, Specialization, Master, Ph.D); the hierarchical level he occupied (Trainee, Junior, Intermediate, Senior, Coordinator/Manager); and the time of experience with software development (I've never worked, Less than 1 year, From 1 to 3 years, From 4 to 7 years, From 7 to 10 years, More than 10 years).

Finally, the fourth phase had three questions related to the assessment of governance mechanisms in proprietary SECO using the 5-point Likert scale: Strongly Disagree (SD), Partially Disagree (PD), Neutral (N), Partially Agree (PA), and Strongly Agree (SA). Participants use this scale to indicate the level of agreement with a statement (MUNSHI, 2014). There were also two open questions where the participants could write about other categories and/or mechanisms that they considered relevant and comments covered in the study.

- Q1 - How important do you consider the involvement of the mechanisms to generate and deliver value to the entire ecosystem? (Likert scale)
- Q2 - How important do you consider mechanisms to maintain consistency and integration of activities, relationships and structures, both for customers and partners, seeking harmonious and effective coordination with ecosystem actors? (Likert scale)
- Q3 - How important do you consider mechanisms to support organizational models? (Likert scale)
- Q4 - Are there other categories and/or mechanisms that you consider relevant? (Open question)
- Q5 - Comments and/or suggestions. (Open question)

For the evaluation and refinement of the instruments in this study, a pilot was carried out with two participants and sent to potential participants in the sample. The questionnaire is presented in Appendix D and is available at:
https://forms.gle/6d14i9Eb648iiVPP9.

3.4.3 Execution

The survey was sent by email to 74 participants selected among the actors (e.g., developers, project leaders, and managers) involved in the proprietary SECO. According to a previous study on the adequacy of response rates for online and paper surveys, the response rate (45.9%, corresponding to 34 participants) is considered positive in studies such as this one (online surveys) (NULTY, 2008).

3.4.4 Analysis of results

Respondents mostly have a Bachelor's degree with a 55.9%, 35.3% Specialization's degree, and 5.9% Master's degree. Regarding the hierarchical level, the majority (47.1%) are senior systems analysts. Another relevant factor is that some of the participants have been working in software development for over 10 years, concentrating on 58.8%. This information is consistent with the fact that most respondents had a high seniority level.

Regarding the involvement of the **value creation** mechanisms, which generate and distribute value to the whole SECO, there is strong agreement with the *promote innovation* mechanism with 21 respondents. In second place, the *stimulate partner investments and share costs* mechanism had strong agreement of 14 participants and partial agreement of 10 participants, as shown in Table 3.1. In fact, innovation in a proprietary platform environment makes sense due to the need to remain competitive and use emerging technologies in new SECO products. Encouraging a community of partners where costs can be shared makes sense from the perspective that organizations with proprietary platforms need a value chain that allows cost savings for the expansion of proprietary SECO.

With regard to the **coordination of players** mechanisms, which support maintaining consistency and harmonious integration of activities for both clients and partners, the mechanism *enable effective communication channels* had 29 respondents indicating strong agreement, and secondly, the *establish roles and responsibilities* mechanism had 23 responses for strong agreement and 9 for partial agreement.

Regarding the use of effective communication channels, the central organization in a proprietary SECO needs to structure channels that allow communication between the actors in the ecosystem. It allows for a continuous feedback and knowledge management channel between the players involved in the SECO. Another important point is that, in order to coordinate, roles and responsibilities must be clear within the proprietary SECO. Roles can help establish levels of access to knowledge and products that are under proprietary policies, as shown in Table 3.1.

For the question about the mechanisms around **organizational openness and control**, in the investigated scenario of proprietary SECO, the *share knowledge* mechanism stands out as the highest level of agreement, with 28 respondents indicating strong agreement. It should be noticed that, for the first time in the questionnaire, we had a strong disagreement rate with the *distribute power* mechanism, summarizing 3 respondents. The most critical point within a proprietary SECO is knowledge sharing, as it serves to support platform expansion and acquire new (or enhance) assets. Care must be taken not to expose internal knowledge and negatively impact the SECO robustness. Table 3.1 describes the outcomes.

Table 3.1: Results from an opinion survey on governance mechanisms in the proprietary SECO, where SD-Strongly Disagree, PD-Partially Disagree, N-Neutral, PA-Partially Agree, and SA-Strongly Agree.

Category	Mechanism	SD	PD	N	PA	SA
Value creation	Promote innovation	21	8	2	3	0
	Manage licenses	7	15	10	2	0
	Create revenue models	11	14	7	2	0
	Attract and maintain varied partners	18	7	6	3	0
	Stimulate partner investments and share costs	14	10	9	1	0
Coordination of players	Create partnership models	15	15	4	0	0
	Define rules to manage relationships	13	19	2	0	0
	Establish roles and responsibilities	23	9	2	0	0
	Enable effective communication channels	29	4	1	0	0
	Manage conflicts	21	10	3	0	0
	Manage resources	16	10	8	0	0
	Manage risks	21	7	5	1	0
	Manage expectations	15	12	5	2	0
	Nurture collaborations	25	6	2	1	0
Organizational openness and control	Support autonomy	11	12	9	2	0
	Share knowledge	28	2	2	2	0
	Distribute power	6	11	10	4	3
	Share architectural decisions	17	11	4	1	1
	Share roadmaps	13	16	4	1	0
	Define entry requirements	13	11	10	0	0
	Define quality standards and certifications	18	12	2	2	0

The open question about other categories and/or mechanisms that are thought to be relevant received three responses, with respondents emphasizing *training* as an item to be considered. In response to the final comments, only one response was obtained, which is in the short cited text *"The organization's architecture needs to be less rigid and more open to good practices"*.

This study was based on a secondary study, the systematic literature review of Alves *et al.* (ALVES; OLIVEIRA; JANSEN, 2017), seeking to assess whether the mechanisms identified as the highest degree of agreement within the organization of a proprietary SECO are the same ones highlighted by Alves *et al.* (ALVES; OLIVEIRA; JANSEN, 2017). The classification of governance mechanisms proposed by primary studies has a total of 89 studies. It was noticed that the most cited mechanisms are: *attract and maintain varied partners* (28 studies, 31%), *share knowledge* (20 studies, 22%), *promote innovation* (25 studies, 28%), and *manage licenses* (21 studies, 23%).

According to the opinion of the proprietary SECO developers of the organization where this study was carried out, these mechanisms are not the most relevant. The mechanism with the highest agreement (checked as "Strongly Agree") within the *value creation* category was *promote innovation*, with 21 respondents, corresponding to 61%. The *at-*

tract and maintain varied partners mechanism drew attention, with 3 respondents marking "Partially Disagree", corresponding to 8%, despite this item being the most cited in the literature (ALVES; OLIVEIRA; JANSEN, 2017).

In the category *coordination of players*, the mechanism that received the highest agreement was *enable effective communication channels* with 29 respondents checking the option “Strongly Agree”, corresponding to 85%. However, in the SLR of Alves *et al.* (ALVES; OLIVEIRA; JANSEN, 2017), it was discovered that this mechanism is ranked third in terms of citations.

In the *organizational openness and control* category, both in the SECO studied and in the SLR of Alves *et al.* (ALVES; OLIVEIRA; JANSEN, 2017), there was a common result for the *knowledge sharing* mechanism. This mechanism was the most cited in this category in the study (ALVES; OLIVEIRA; JANSEN, 2017) and had the highest level of importance among developers, being checked by 28 respondents, corresponding to 82%.

Due to the ascending influence of mid-level managers on strategic planning, which is considered a relevant factor in decision making (SCHILIT, 1987), we sought to deepen the analysis of a particular research group. The following characteristics have been observed: governance mechanisms with the highest agreement among coordinators/managers are the same as those indicated by the total number of respondents: *promote innovation*, *enabled effective communication channels* and *share knowledge*.

Because the "coordinator/manager" group occupies a position of trust in the organization, directly influencing the corporation’s performance, a quantitative analysis was carried out on this group of managers. This profile was selected for further analysis. The following section brings a set of interviews in order to deepen the understanding of these governance mechanisms with the highest agreement.

3.5 Interviews with managers

This subsection presents a set of interviews planned and executed aimed at refining and understanding the choice of software asset governance mechanisms by managers in the proprietary SECO.

3.5.1 Study goal

The interviews were planned and carried out with the goal of determining why the managers who took part in the previous study identified those software asset governance mechanisms as having the highest agreement in the organization's proprietary SECO. The discussion about lesser agreement mechanisms may be the target of future work.

3.5.2 Instrumentation

An Informed Consent Form (presented in Appendix C) was presented to the participants. In addition, a set of questions was defined to guide the semi-structured interviews, as following:

- Q1 - How is *promote innovation* mechanism being used to manage software assets within the organization?
- Q2 - What are the benefits and difficulties of this mechanism within the organization?
- Q3 - How is *enable effective communication channels* mechanism being used to manage software assets within the organization?
- Q4 - What are the benefits and difficulties of this mechanism within the organization?
- Q5 - How is *share knowledge* mechanism being used to manage software assets within the organization?
- Q6 - What are the benefits and difficulties of this mechanism within the organization?

3.5.3 Execution

To assess the governance mechanisms of software assets with the highest agreement, semi-structured interviews were conducted with 8 IT managers. These participants were selected from those who responded to the questionnaire used in the survey. To do so, the perception of the group of 8 respondent managers (managers and coordinators) was investigated through semi-structured interviews. In this group, we had different skills and profiles according to leadership, knowledge, and experience time. The characterization of each one is described below:

- six IT coordinators: oversee a small group of employees; support and coach existing employees; manage information technology systems, increasing productivity; and have five years of managerial experience.

- two IT managers: have more than five years of managerial experience; guide supervisors; manage department budgets, and possess strong decision-making skills.

3.5.4 Analysis of results and discussion

Regarding the 6 suggested questions aimed at the concept of asset governance in proprietary SECO, which were synthesized from the studies found in the opinion survey, 6 answers with evidence are highlighted below, according to some participants:

- Q1 - How is *promote innovation* mechanism being used to manage software assets within the organization?

> *The process of adopting new technologies is time-consuming and bureaucratic. The IT architecture area should mobilize more quickly and authorize the use of new resources.* (Participant 1)

This participant's statement is consistent with the study of Assink (ASSINK, 2006), which examines the reasons why large companies frequently fail to develop disruptive innovations. The study identifies several important inhibitors or barriers that hamper these developments.

- Q2 - What are the benefits and difficulties of this mechanism within the organization?

> *An innovative company becomes more competitive in the market. The customer has a different perception.* (Participant 3)

This participant's answer may be evidenced through the study of Freire *et al.* (FREIRE et al., 2002), where analysis work was carried out in the software industry, from the point of view of innovation and competitiveness, in developing countries in a globalized scenario.

- Q3 - How is *enable effective communication channels* mechanism being used to manage software assets within the organization?

> *The internal tool responsible for storing the assets does not have the correct disclosure. For example, the corporate intranet should be exploited for this purpose.* (Participant 2)

This participant's statement backs up the study of Men (MEN, 2014), which looks at the effectiveness of various communication channels within an organization.

- Q4 - What are the benefits and difficulties of this mechanism within the organization?

  The biggest benefit would be the productivity gain due to the reuse of less developed source code and less effort. In the company, there is no culture of using an asset repository. The current repository is not user-friendly. (Participant 8)

According to the study of Swartz and Vysniauskas, software asset management (SAM) is a relatively new practice concerned with the efficient management of software assets within an organization. The goal of the study is to investigate the challenges that large-scale organizations face when managing software assets. The benefits pointed out by Participant 8 are addressed in the study (SWARTZ; VYSNIAUSKAS, 2015).

- Q5 - How is *share knowledge* mechanism being used to manage software assets within the organization?

  The obligation to meet deadlines makes the training of new professionals and the transfer of knowledge always a second moment. The knowledge remains with the people. (Participant 5)

The study of Tonet and Paz (TONET; PAZ, 2006) addresses knowledge sharing at work, which is extremely important for organizations but difficult to achieve given the organization's knowledge transfer process. In addition, it offers guidance to help reflect on the elements that make up the process of sharing knowledge between people.

- Q6 - What are the benefits and difficulties of this mechanism within the organization?

  Due to organizational changes in recent years, where many senior professionals have left, the lack of a knowledge base has prevented the transfer of knowledge safely. The obligation to achieve performance goals is another factor that makes it difficult, as the effort is dedicated to accomplishing another task. Through knowledge management, risks such as the loss of important information can also be mitigated. (Participant 8)

Participant 8's statement is in line with a study conducted by Unifi Network, a subsidiary of Pricewaterhouse-Coopers, which examined the impact of employee turnover on customer satisfaction in six different sectors: banking, investment management, personal computing, property and casualty insurance, retail sales and telecommunications. According to this study, the survey results show a strong link between employee retention and service quality as perceived by customers (CASEY; WARLIN, 2001).

3.6 Correlations between the most agreed governance mechanisms of the "managers/coordinators" group

The study of the correlation between variables is an important source for understanding a problem and a method for finding potential solutions (BENESTY et al., 2009). With this objective, an analysis was carried out to try to find some relationship between the mechanisms *promote innovation*, *enable effective communication channels* and *knowledge sharing*, which are characterized by governance of software assets with the highest agreement in the group of "managers/coordinators" based on the results of the opinion survey described in Section 3.4. For this, we used the R programming language and its development IDE known as RStudio[1].

3.6.1 Correlations execution

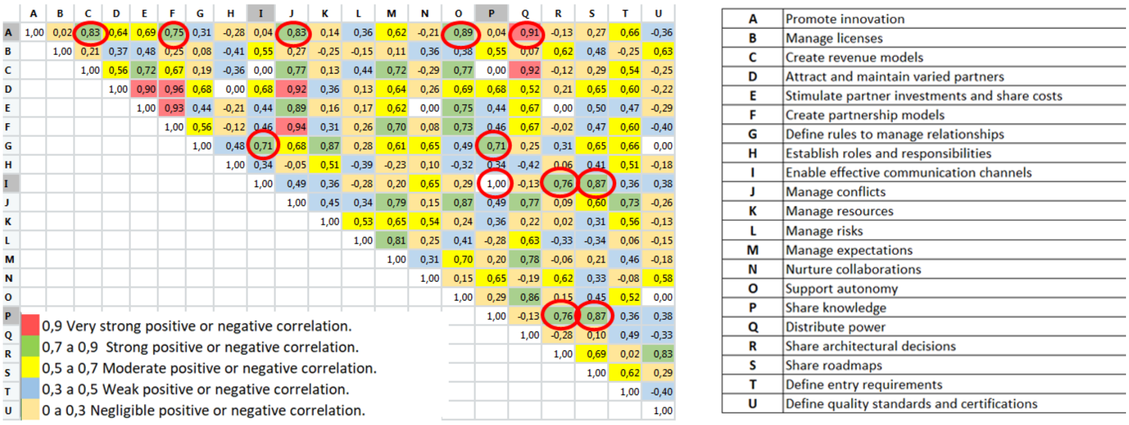
In descriptive statistics, the Pearson correlation coefficient, also called the "product-moment correlation coefficient" or simply "Pearson's p", measures the degree of correlation (and the direction of that correlation - whether positive or negative) between two metric scale variables (FIGUEIREDO FILHO; SILVA JÚNIOR, 2009).

Interpreting p = 0.9 for plus or minus indicates a very strong correlation; 0.7 to 0.9 positive or negative indicates a strong correlation; 0.5 to 0.7 positive or negative indicates a moderate correlation; 0.3 to 0.5 positive or negative indicates a weak correlation; and 0 to 0.3 positive or negative indicates a negligible correlation.

3.6.2 Correlation selection criteria

In order to understand the relationships within the proprietary SECO, all correlations with strong and very strong coefficients that the group of managers elected with the highest degree of agreement during the opinion survey were selected. That is, *promote inno-*

[1] RStudio is a free software integrated development environment for R, a programming language for graphics and statistical calculations



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
A	1,00	0,02	0,83	0,64	0,69	0,75	0,31	-0,28	0,04	0,83	0,14	0,36	0,62	-0,21	0,89	0,04	0,91	-0,13	0,27	0,66	-0,36
B		1,00	0,21	0,37	0,48	0,25	0,08	-0,41	0,55	0,27	-0,25	-0,15	0,11	0,36	0,38	0,55	0,07	0,62	0,48	-0,25	0,63
C			1,00	0,56	0,72	0,67	0,19	-0,36	0,00	0,77	0,13	0,44	0,72	-0,29	0,77	0,00	0,92	-0,12	0,29	0,54	-0,25
D				1,00	0,90	0,96	0,68	0,00	0,68	0,92	0,36	0,13	0,64	0,26	0,69	0,68	0,52	0,21	0,65	0,60	-0,22
E					1,00	0,93	0,44	-0,21	0,44	0,89	0,16	0,17	0,62	0,00	0,75	0,44	0,67	0,00	0,50	0,47	-0,29
F						1,00	0,56	-0,12	0,46	0,94	0,31	0,26	0,70	0,08	0,73	0,46	0,67	-0,02	0,47	0,60	-0,40
G							1,00	0,48	0,71	0,68	0,87	0,28	0,61	0,65	0,49	0,71	0,25	0,31	0,65	0,66	0,00
H								1,00	0,34	-0,05	0,51	-0,39	-0,23	0,10	-0,32	0,34	-0,42	0,06	0,41	0,51	-0,18
I									1,00	0,49	0,36	-0,28	0,20	0,65	0,29	1,00	-0,13	0,76	0,87	0,36	0,38
J										1,00	0,45	0,34	0,79	0,15	0,87	0,49	0,77	0,09	0,60	0,73	-0,26
K											1,00	0,53	0,65	0,54	0,24	0,36	0,22	0,02	0,31	0,56	-0,13
L												1,00	0,81	0,25	0,41	-0,28	0,63	-0,33	-0,34	0,06	-0,15
M													1,00	0,31	0,70	0,20	0,78	-0,06	0,21	0,46	-0,18
N														1,00	0,15	0,65	-0,19	0,62	0,33	-0,08	0,58
O															1,00	0,29	0,86	0,15	0,45	0,52	0,00
P																1,00	-0,13	0,76	0,87	0,36	0,38
Q																	1,00	-0,28	0,10	0,49	-0,33
R																		1,00	0,69	0,02	0,83
S																			1,00	0,62	0,29
T																				1,00	-0,40
U																					1,00

🟥 0,9 Very strong positive or negative correlation.
🟩 0,7 a 0,9 Strong positive or negative correlation.
🟨 0,5 a 0,7 Moderate positive or negative correlation.
🟦 0,3 a 0,5 Weak positive or negative correlation.
🟧 0 a 0,3 Negligible positive or negative correlation.

A	Promote innovation
B	Manage licenses
C	Create revenue models
D	Attract and maintain varied partners
E	Stimulate partner investments and share costs
F	Create partnership models
G	Define rules to manage relationships
H	Establish roles and responsibilities
I	Enable effective communication channels
J	Manage conflicts
K	Manage resources
L	Manage risks
M	Manage expectations
N	Nurture collaborations
O	Support autonomy
P	Share knowledge
Q	Distribute power
R	Share architectural decisions
S	Share roadmaps
T	Define entry requirements
U	Define quality standards and certifications

Figure 3.1: Strong and very strong correlations between proprietary SECO governance mechanisms in the organization.

vation, *enable effective communication channels*, and *knowledge sharing* and duplicate correlations have been eliminated.

The greater the absolute value of the coefficient, the stronger the relationship between the variables. Figure 3.1 depicts the outcome of strong and very strong correlations.

3.6.3 Analysis of correlations in the context of proprietary SECO

The goal is to evaluate whether there is statistical evidence for a relationship between the same pairs of variables in the survey results. The justifications below refer to an analysis of the strong and very strong correlations between the governance mechanisms of software assets in the context of proprietary SECO coming from the organization studied.

Promote innovation & Create revenue models (coefficient: 0,83 – strong): the strong correlation between promoting innovation and creating revenue models within the proprietary SECO can be analyzed as essential for survival in an increasingly competitive and globalized scenario. When a consumer organization within SECO is able to efficiently manage business in relation to its revenues, using innovations in the business model (such as a disruptive product that transforms an industry), expanding and improving its products and services from already existing ones, it will be better prepared for the future and one step ahead of its competitors.

Promote innovation & Create partnership models (coefficient: 0,75 – strong): the strong correlation between the promotion of innovation and the creation of partnership models within the proprietary SECO can be verified through alliances between consumer organizations. With a market that is constantly changing, employing this type of strategy can increase returns by causing these organizations to seek out new opportunities, such as attracting the attention of strategic partners as well as new customers. Not only consumer organizations benefit in this regard. Supplier organizations can also take advantage of this relationship. The creation of a partnership model together with an innovation strategy in both organizations may create a new performance standard for software developers as it will support cooperation.

Promote innovation & Manage conflicts (coefficient: 0,82 – strong): the strong correlation of innovation promotion with conflict management within the proprietary SECO can be analyzed through a dilemma that the consumer organization verified in this example has: the reluctance to do anything that could jeopardize the current model, because the success of the current product is a consequence of the current business model. Therefore, within this SECO, we have a conflicting relationship, mainly between the consumer organization and its suppliers. Supplier organizations encourage the adoption of new technologies aiming at new service provision contracts and the consumer organization studied in this example acts with resistance, becoming an obstacle to innovation.

Promote innovation & Support autonomy (coefficient: 0,88 – strong): the strong correlation between promoting innovation and supporting autonomy within the proprietary SECO can be confirmed by the fact that the consumer organization in question is totally dependent on its holding[2] and many decisions come from another consumer organization, where it is mandatory to follow these determinations. There is no autonomy in the consumer organization studied for decision making regarding the adoption of new technologies. There is a veiled relationship with parasitism, as the consumer organization is totally dependent on another consumer organization.

Promote innovation & Distribute power (coefficient: 0,90 – very strong): the fact that power is centralized in another consumer organization of the same group (Holding) explains the very strong correlation between the promotion of innovation and the distribution of power within the proprietary SECO. There is no incentive for actors to be encouraged to innovate, generating a culture of innovation, as there is a dependence on the guidelines of another organization, with no collaborative relationship. This relationship also harms suppliers, as it is impossible to separate them from this environment.

Share knowledge & Enable effective communication channels (coefficient: 1,00 – very strong): because of the organizational changes that have occurred in recent years by consumer organizations, where many professionals with a seniority profile have been dismissed, the very strong correlation of knowledge sharing with the permission of ef-

[2] holding is a company whose main activity is the majority shareholding in one or more companies and has control of their administration and business policies

fective communication channels within the proprietary SECO can be proven. The lack of a knowledge base hampered the safe transfer of knowledge. The risks of the loss of information could be mitigated if there was an efficient communication channel allied to knowledge management. There are several ways to invest and ensure that knowledge is shared within the organization. However, this initiative is not part of the organizational culture in the case studied.

Share knowledge & Share architectural decisions (coefficient: 0,88 – strong): the strong correlation of knowledge sharing with sharing architecture decisions within the proprietary SECO can be verified in several situations. For example, in the consumer organization examined, the decisions enacted in a project are direct consequences of the direction of an architectural opinion issued by the area of Enterprise Architecture. This opinion takes into account the company's culture, the development process and restrictions existing at the time of decision making. Developers from both the consumer and supplier organizations may be required to implement some procedures without prior agreement at some point. Therefore, it is important to document decisions made in software projects to share understanding before any changes are made.

Share knowledge & Share roadmaps (coefficient: 0,76 – strong): the strong correlation of knowledge sharing with the sharing of architectural roadmaps within the proprietary SECO can be assessed through a fine-tuned relationship between the consumer and supplier organization, helping both to achieve better results and business (win-win). If the development team knows the sequential steps towards the integral construction of the product, there will be greater peace of mind for the continuity of the work and greater alignment with all interested parties, sharing knowledge in the work environment, not only sharing or passing on information, but making room for exchange and for personal and professional growth. The lack of visibility of this continuity of work generates instability in consumer and supplier organizations, as developers are left without a perspective, generating apprehension.

Share knowledge & Define rules to manage relationships (coefficient: 0,71 – strong): the strong correlation of knowledge sharing with the definition of rules to manage relationships within the proprietary SECO can be verified through a disharmonious relationship within the consuming organization, where developers compete for knowledge. This competition is due to the fact that there are people who still think that knowledge should be retained by a single individual. The same thinking can be propagated by suppliers. Dependence on knowledge by a supplier can create friction in the relationship between teams, becoming harmful to SECO.

Enable effective communication channels & Define rules to manage relationships (coefficient: 0,71 – strong): the strong correlation of allowing effective communication channels with the definition of rules to manage the relationships within the proprietary SECO can be verified through a hostile organizational environment on the part of the consumer organization. There is currently an example of a lot of demands, pressure, and an unstable economic scenario, and many people demonstrate that they are having difficulty dealing with this stress.In this context, where people do not manage their emotions, it is difficult to communicate ideas. As a result, caring about the efficiency of the communication plan can harm task execution as well as personal and organizational constraints if it is misinterpreted. The supplier organization, once it experiences this scenario, ends up being affected as well.

Enable effective communication channels & Share architectural decisions (coefficient: 0,76 – strong): the strong correlation between enabling effective communication channels with sharing architecture decisions within the proprietary SECO can be assessed by understanding the clarity of a message after it is transmitted across the various types of communication channels. In the example of a consumer organization, there is a need to prepare an architectural decision document (architectural opinion), disclosed and elaborated on for each project. This should be a simple text file describing the reasons for the decision and its consequences, preferably cataloged in an asset repository. In practice, changes in software occur due to the need to correct existing bugs or to add new features and functionality. Such changes require that architectural decisions support a set of requirements and that they are communicated through all communication channels of the consumer organization. Otherwise, the risks to SECO are enormous, potentially leading to project failure or cancellation.

Enable effective communication channels & Share roadmaps (coefficient: 0,87 – strong): the strong correlation between allowing effective communication channels and sharing roadmaps within the proprietary SECO can be determined when everyone involved in the evolution process knows the variables included in this activity. However, this is not always the case for the consumer organization in question, as communication difficulties make it difficult for product developers to organize their own ideas. For the success of this communication plan, neither the consumer organization's developer nor the supplier organization can have any doubts about the final objective. If this purpose succeeds, everyone wins. Otherwise, everyone loses.

3.7 Limitations

The limitations of a study are those characteristics of design or methodology that impacted or influenced the interpretation of the findings from the research. Study limitations are the constraints placed on the ability to generalize from the results or to further describe applications to practice (PRICE; MURNAN, 2004).

The first limitation concerns the generalization of the results. Our study involved only one organization, and it is not possible to generalize the results to organizations not similar to the studied organization (Banking, Financial Services, and Insurance industry - BFSI). The second one is linked to the knowledge of the opinion research participants. Despite the researcher's availability during the opinion survey to resolve any doubts, industry practitioners may not yet be familiar with the concepts of SECO.

3.8 Final remarks

The reuse of artifacts generated throughout proprietary software development has been improved to support and promote relationships among vendors, providers, consumers, and a keystone that maintains the common technological platform. As the organization studied had the ecosystem centered on a closed platform with contributions protected by intellectual property and confidentiality agreements, a proprietary SECO is configured. In this case, establishing software asset management policies and guidelines is a critical aspect of maintaining a sustainable SECO.

This study was based on a secondary study performed by Alves *et al.* (ALVES; OLIVEIRA; JANSEN, 2017), which sought to determine whether the mechanisms identified as having the highest degree of agreement within the organization of a proprietary SECO were the same ones highlighted by Alves *et al.* The study investigated asset governance mechanisms in a proprietary SECO by: (i) a survey research with 34 participants to gather insights on some mechanisms, (ii) a set of 8 interviews with a group of managers to analyze the most relevant mechanisms; and (iii) a correlation analysis of the managers' opinions. Through the results of the opinion survey, we compared the governance mechanisms proposed in the *value creation*, *coordination of players*, and *organizational openness and control* categories (ALVES; OLIVEIRA; JANSEN, 2017). Next, we identified that these governance mechanisms received a different level of agreement than those indicated in the literature.

The most cited mechanisms in the secondary study of Alves *et al.* (ALVES; OLIVEIRA;

JANSEN, 2017) were *attract and maintain varied partners*, *share knowledge*, and *manage licenses*. For the actors of the proprietary SECO where this study was carried out, the most relevant mechanisms were *promote innovation*, *enable effective communication channels*, and *share knowledge*. The governance mechanisms with the highest agreement among coordinators/managers are the same as those indicated by the total number of respondents: *promote innovation*, *enable effective communication channels*, and *share knowledge*.

4. Participative case study

In this chapter, we describe a participative case study conducted in a large international organization that owns a proprietary SECO. The purpose is to implement new governance strategies based on governance mechanisms and health metrics provided by Alves *et al.* The study helped us to achieve the objectives proposed in Chapter 1. The results of this study are published in an international journal (COSTA; FONTÃO; SANTOS, 2021d).

4.1 Introduction

The challenge of selecting SECO governance strategies that contributes to the SECO health motivated Alves *et al.* (ALVES; OLIVEIRA; JANSEN, 2017) to conduct a systematic literature review. The authors provided an overview of SECO governance definitions and mechanisms, as well as SECO health metrics, covering literature from 2006 to 2015. In our work, we report on a longitudinal literature study focused on proprietary SECO governance and health covering from 2016 to 2020, updating and refining the previous study of Alves *et al.* (ALVES; OLIVEIRA; JANSEN, 2017).

In this context, this chapter presents a participative case study in a large international organization which owns a proprietary SECO. For each new strategy, we associated health metrics related to the governance mechanisms. Based on the catalog of health metrics provided by Alves *et al.* (ALVES; OLIVEIRA; JANSEN, 2017), the metrics were selected to measure the governance strategies adopted for each mechanism. Next, we conducted an opinion survey in order to verify the participants' level of perception about the strategies related to governance mechanisms.

Case study is an adequate research method for situations in which it is difficult to establish a clear link between the studied phenomenon and its context, in such a way that it is not possible to investigate the phenomenon outside of the practical environment (YIN,

2005) (i.e., when studying the technological and social scalability of a system within an organization, it is not possible to separate the information systems from the organization and the actors).

In order to use the case study as a research strategy, we take into account two foundations based on Yin (2005): i) the investigation of a contemporary phenomenon within its real-life context; and ii) the researcher's access to an event or phenomenon hitherto inaccessible to scientific research.

Participative case study was selected as research method in this study in order to help the comprehension of situations investigated, enabling the emergence of new relationships (TRINKENREICH et al., 2019). In addition one of the researchers acts in a large international organization *(the name was omitted for privacy reasons)* which owns a proprietary SECO, being a participant in the observed process (BASKERVILLE, 1997). Together with other participants from the organization, information were gathered to understand the organization and defined strategies to implement governance practices related to governance mechanisms and health metrics in the proprietary SECO. Thus, the researcher may have control over the intervention on some variables during the study, such as suggesting the adoption of a governance mechanism in a given situation. The process as a whole was accompanied by the other two researchers who were supervising the participative case study in order to clarify and direct some actions.

These researchers used the same research protocol and had access to the same supporting documents (mind map and glossary) during the study. Both the principal and the supervisors' researchers were aware of the process to be followed and used the same concepts as a basis for aligning and directing the discussions.

This chapter is organized as follows: Section 4.2 presents the main research question; Section 4.3 describes the designing and planning of the participative case study; Section 4.4 presents how the execution of the participative case study was conducted; Section 4.5 shows the results; Section 4.6 defines the opinion survey to verify the participants' feedback; Section 4.7 outlines the importance to conduct our study and how will it impact future research in the SECO governance field; Section 4.8 presents the threats to validity; and finally, Section 4.9 concludes the chapter with final remarks.

4.2 Research question

The goal of this study is to understand the governance in a proprietary SECO of a large international insurance organization. The research question for this study is: *"How are SECO governance strategies and health metrics implemented in a proprietary SECO?"*.

4.3 Designing and planning

4.3.1 Organization characterization

Founded more than 80 years ago, it is currently one of the largest insurance groups in Latin America, operating nationwide and internationally in several insurance segments: auto, property, health, capitalization, and open supplementary pension. It has more than 200 branches (service centers, offices and customers service) across the country and a partnership with more than 40,000 insurance brokers.

4.3.2 Diagnosis

In a business environment, IT plays an important role in the performance of the organization, especially when it provides a flow of information that adds value without weakening organizational efficiency (BROWN, 2003). IT is considered an area focused on solving internal and technical problems. The organization in this study decided to change its vision, focusing on client services and generating value for the company's business. Based on this premise, the implementation of guidelines for IT management had a strong implication to change the old concept, designating the most appropriate solution aimed at the most efficient business as possible.

In order to meet a new perspective, a structured way of dealing with those challenges was implemented through IT service management (ITSM), from the strategic plan until the incidents management. Thus, a set of good practices for ITSM was implemented using ITIL framework, applying an integrated manner for the use of processes, people, and tools/products to promote the strategic alignment between IT services and the organization business model.

Increasingly, the market pressure for a state-of-the-art solution causes companies to work at a highly accelerated pace, passing this anxiety to IT project team, which must deliver results in an increasingly short time (KAPPELMAN; MCKEEMAN; ZHANG, 2006). As a consequence of the growing number of demands added to the lack of flexible processes, some problems emerged, such as people applying for layoffs due to healthcare problems, developers looking for other job opportunities, late projects, and over budget, then overloading IT project teams due to rework on software artifacts. Communication issues among client and organization and software suppliers are also a consequence. The result is a project delivered with several defects and without quality, producing incidents in the productive environment.

Maintaining a platform to mitigate the risks of incidents (i.e., unplanned service interruption) is one of the goals for the technical incident management team, also known Sustaining Team. The activities that support SECO governance can be an opportunity to solve challenges that are beyond technical problems, such as business and social concerns (SADI; YU, 2015). In such a complex scenario, the organization studied decided to implement incident management practices using ITIL methodology in the second semester of 2018, aiming to minimize these problems. As such, it established governance policies and guidelines as a critical strategy for maintaining a sustainable SECO platform. A sustainable approach is linked to how the platform can resist to natural changes, e.g., business evolution, technology obsolescence, and community changes (DHUNGANA et al., 2010).

It is noteworthy that ITIL organizes the processes around the five service lifecycle stages: Service Strategy, Service Design, Service Transition, Service Operation, and Continual Service Improvement. Each of the five stages is focused on a specific phase of the service lifecycle. The organization studied started the challenge in Service Operation, especially on incident management.

Incident management process is still very immature. According to the IT managers, the main difficulties were due to: i) resistance of participants - the organizational changes require significant transformations, several employees resist to accept the new processes and, sometimes, even boycott the new procedures; and ii) absence of monitoring of performance indicators - ITIL implementation is a process of constant improvement and must follow the development and evolution of the organization. Therefore, in our work, we proposed to use SECO governance strategies based on governance mechanisms of Alves *et al.* (ALVES; OLIVEIRA; JANSEN, 2017) to evolve organization from traditional to ITSM process, providing user and customer satisfaction. According to Benbasat *et al.*, the case study as a research method is appropriate for issues based on practice problems where the actors' experiences are important (BENBASAT; GOLDSTEIN; MEAD, 1987).

4.3.3 Planning

Before starting the participative case study, we proposed the reading of two reference artifacts for participants to feel familiar with SECO governance mechanisms. The first document is a mind map (Section 2.2.3.1) and the second one refers to a glossary (Section 2.2.3.2). A great benefit of this initiative was to create the same level of understanding for the participants.

This study aimed at using, evaluating and monitoring of the governance mechanisms proposed by Alves *et al.* (ALVES; OLIVEIRA; JANSEN, 2017) from the point of view of 12 participants (developers and technical leaders) of the organization's sustaining team in the context of the proprietary SECO. The methods for data collection were: i) observation to analyze the sustaining team's behavior in the face of problematic situations; ii) interviews to collect information on the adoption of governance mechanisms in everyday situations; and iii) opinion survey with participants to collect feedback based on using Visual Analogue Scale (VAS). In a case study, methods such as interviews, observation, and analysis of documentation and artifacts can be carried out in order to explain the phenomenon of the presence of the information systems in a given context (YIN, 2005).

The interviews were conducted by one of the researchers with developers and technical leaders. Participants were instructed to feel free to speak as much as they want to. Both observation and interviews aimed to understand the problems of using governance mechanisms in everyday situations of a proprietary SECO and to which extent the participants were familiar with the subject.

4.4 Execution and data collection

The researcher conducted a 60-minutes lecture with the entire sustaining team talking about the main reasons of this study: gathering information about the strategies for adopting, understanding and using the SECO governance mechanisms in a proprietary SECO (ALVES; OLIVEIRA; JANSEN, 2017). It focused on a detailed explanation of reference artifacts (Section 2.2.3).

Subsequently, we reinforce the team's understanding of the work proposal. From August 3, 2020, until September 4, 2020, during the observation period of the study (30 days), the researcher started the interviews to encourage the use of governance strategies in everyday situations based on mind map (Section 2.2.3.1) and glossary (Section 2.2.3.2). The goal was to obtain at least one new strategy for each governance mechanism. Data collection started with interviews to gather general information about the organization. The participants were invited to virtual meetings, moderated by one of the researchers, using the Cisco Webex[1] tool to discuss the elements described in the mind map document explained in Section 2.2.3.1 in order to understand the current governance deficiencies scenario and incentivate the application of the governance mechanisms described in Section 2.2.3.2.

The interviews were conducted with developers and technical leaders. Each interview lasted about 30 minutes. The maximum number of participants per virtual meeting was twelve. The researcher took notes of all interventions, orientations and directions as well as the use or not of a specific governance mechanism through the logbook.

Structured interviews represented by a script of questions previously established and carried out by the researcher ensured alignment and removed any doubts from the team regarding the task. The intuitions and perceptions of the researcher arising from this moment may improve the quality of the work, offering greater depth of understanding. One of the characteristics of the case study is the investigation of different entities or actors, such as people, groups, and organizations. These results depend on the researcher's integration view (BENBASAT; GOLDSTEIN; MEAD, 1987) (YIN, 2005).

The interviews were conducted by the main researcher and fulfilled by two other researchers with experience in SECO and qualitative data analysis, involving 12 participants (developers and technical leaders) of the organization's sustaining team in the context of a proprietary SECO. We performed qualitative data analysis to capture the perceptions using a thematic analysis from sustaining team practitioners' comments who participated in the study. Thematic analysis is a method for identifying, analyzing, and reporting patterns/themes from a dataset (BRAUN; CLARKE, 2006).

Because the sustaining team occupies a position of trust in the organization, directly influencing governance actions, Section 4.5 presents the results obtained during the observation period of the study. The sustaining team has different developer profiles (senior, intermediate, and junior) according to technical experience, business knowledge, and leadership skills. Table 4.1 summarized the roles and profiles.

The technical lead profile oversees the company's developers and the projects they undertake, analyzes briefs, writes progress reports, identifies risks, and develops work schedules. The senior profile has a greater capacity to act under pressure, better strategic vision, and greater knowledge of the IT architecture of the applications. Within the

[1] Cisco Webex is an American company that develops and sells web conferencing and video conferencing applications. https://www.webex.com/

Table 4.1: Participants profile of sustaining team.

Profile	Skills
Junior developer	• triage systems • end-user support • knows how to scale technical solutions
Intermediate developer	• less critical systems • takes risks on a smaller scale • reliability in daily activities
Senior developer	• good performance under big pressure • strategic vision • IT architecture overview • autonomy for decision making
Technical leader	• oversees the company's developers • writes progress reports • develops work schedules

team, this kind of profile can address complex technical issues with autonomy and may behave as a technical leader. The intermediate profile is responsible for the maintenance of less critical systems, manages to take risks considering the organizational rules, and can manage the pressure in daily activities. The junior profile acts in the triage and end-user support. This profile has technical knowledge that allows guiding the end-user on how to use the system and can be proactive in identifying bugs based on end-user complaints. In some cases, it needs support and direction in scaling technical solutions. We need attention to all of these profiles because they are composed of practitioners possessing expertise and skills relevant to a specific response and are responsible for organizing and directing activities to restore the IT services as quickly as possible.

4.5 Results and discussion

SECO governance mechanisms are managerial tools of players that have the goal of influencing an ecosystem's health (ALVES; OLIVEIRA; JANSEN, 2017) divided in three main categories as shown in Figure 2.2. After obtaining a broad view of the organization and understanding how it behaves, the researcher and the participants reflected on current governance behaviors and defined new strategies according to the mechanisms.

Therefore, we created Table 4.2 to identify undesirable behaviors, i.e., software deliverables with low quality. We follow a peculiarity of the case study according to Benbasat *et al.* (BENBASAT; GOLDSTEIN; MEAD, 1987) and Yin (YIN, 2005): the researcher should have a positive attitude towards exploration to obtain good results. To build Table 4.2, the participants identified situations in which new governance strategies (ST) based on the governance mechanisms (GM) could be used through their daily perceptions.

The strategies aiming to propose improvements for undesirable behaviors (UB) that happen in the organization are listed in Table 4.3 and are refered as *"(STxx)"* where *"ST"* is the governance strategy and *"xx"* is the ID. The situations were observed by the researcher in a logbook that is compiled in Table 4.2 with descriptive causes (C). The undesirable behaviors and causes were identified mainly from the daily participants' actions and perceptions. For each mechanism, we propose a new governance strategy, as shown in Table 4.3.

Using Goal-Question-Metric (GQM) approach, for each strategy we list health metrics in Table 4.4 and associate health metrics related to the governance mechanisms that need to be monitored and evaluated. Based on the catalog of health metrics provided in Alves *et al.* (ALVES; OLIVEIRA; JANSEN, 2017), we defined the metrics that should be used to measure the governance strategies **(ST1 to ST21)** adopted for each mechanism, also shown in Table 4.4. The choices were made through alignment and consent meetings between the researcher and the participants. Based on this scenario, the case study research also provides the opportunity to face a technically unique situation in which there will be more variables of interest than data points (BENBASAT; GOLDSTEIN; MEAD, 1987) (YIN, 2005). For each undesirable behavior, we detail the reasons and discussions about the governance strategy in each topic:

- **(UB) Project deliverables with many defects & (C) Poor automated testing tool**: it is essential that the developed products undergo continuous validations to reduce the number of defects and avoid costs generated by low quality. Therefore, having a formal testing step performed by a specialized team is essential for identifying and

Table 4.2: Causes of undesirable behaviors with new governance strategies.

GM	Undesirable Behaviors (UB)	Causes (C)	ST
M1	Project deliverables with many defects	Poor automated testing tool	ST1
M2	Software vendors deliverables are not satisfactorily accepted	Evaluation criteria of software vendors does not exist	ST2
M3	Difficulties in using the approval environment	There is no concept of configuration architecture	ST3
M4	Few software vendors with expertise	Limited knowledge base	ST4
M5	Tacit knowledge is concentrated in a few people	There is no knowledge management culture	ST5
M6	Only one software vendor has a proprietary product license	Product is evolving in the maturity process within the organization	ST6
M7	Cannibalization of human resources among software vendors	Tacit knowledge is concentrated in a few people	ST7
M8	Insufficient software vendors accountability	Lack of governance for software vendors	ST8
M9	Delivery failures	Lack of alignment between stakeholders	ST9
M10	Poor knowledge transfer from the project team to the sustaining team	Lack of handover process	ST10
M11	Incidents in the production environment increase organization expenses	Root cause analysis is not performed	ST11
M12	Low quality deliverables without penalties for software vendors	Lack of a guarantee process	ST12
M13	Operational tasks become more important than structural projects	Large incident quantity in production environment	ST13
M14	Exhausted limit of the sustaining team's productivity capacity	Developers are looking for other job opportunities constantly	ST14
M15	Software vendors do not have autonomy to propose improvements to business managers	Meetings with business managers must take place with the presence of an employee of the organization	ST15
M16	Tacit knowledge is concentrated in a few people	Difficulty finding professionals with expertise and skills	ST16
M17	Battle among software vendors for control of the product's most valuable features	Obtain competitive advantages to negotiate better service contracts in the future	ST17
M18	Software vendors are unaware of the organization's manuals, guidelines, policies, and processes	Lack of definition of minimum requirements for new players	ST18
M19	Developers neither know architectural recommendations nor have a best practice manual	Application development framework documents are missing	ST19
M20	Stakeholders do not have visibility on the evolution of the product	Lack of sharing roadmap products by bussiness managers	ST20
M21	Poor quality product with many defects	Software developers without proper technical certifications	ST21

Table 4.3: New governance strategies (ST) to be adopted by the organization.

ID	Strategy (ST)	References
1	Using automated testing tools	(BORJESSON; FELDT, 2012) (HUSSAIN; RAZAK; MKPOJIOGU, 2017) (GUPTA; PRASAD; MOHANIA, 2008)
2	Creating IT service provider assessment process	(CURRIE; SELTSIKAS, 2001) (KARAMI; GUO, 2012)
3	Deploying configuration architecture concepts	(WESTFECHTEL; CONRADI, 2001)
4	Opening competition to increase the number of software consultants	(ROHRBECK; HÖLZLE; GEMÜNDEN, 2009)
5	Investing in learning process and intellectual capital	(BASSI; VAN BUREN, 1999) (HSU; FANG, 2009)
6	Increasing the number of certificate partners	(JANSEN; BRINKKEMPER; FINKELSTEIN, 2009)
7	Improving people management	(PURCELL et al., 2008) (VAN MARREWIJK; TIMMERS, 2003)
8	Giving corporate visibility in relation to the IT service provider management	(SHWARTZ et al., 2007)
9	Defining procedures to improve service delivery management	(BROWN; POTOSKI, 2006)
10	Stimulating the knowledge transfer process	(AGOSTINI et al., 2003)
11	Investing in a root cause analysis process	(GUPTA; PRASAD; MOHANIA, 2008) (MAHTO; KUMAR, 2008)
12	Invoking guarantee process for software vendors	(MAGNANINI; FERRETTI; COLAJANNI, 2019)
13	Scheduling meetings to introduce new technology solutions	(COZZOLINO; VERONA; ROTHAERMEL, 2018)
14	Applying the job rotation culture	(ORTEGA, 2001)
15	Defining performance boundaries of software consultants	(KITAY; WRIGHT, 2004)
16	Establishing knowledge management process	(HAGGIE; KINGSTON, 2003) (GREINER; BÖHMANN; KRCMAR, 2007)
17	Reviewing software vendor contracts	(GEFEN; WYSS; LICHTENSTEIN, 2008)
18	Providing entry guidelines for new players	(SHWARTZ et al., 2007)
19	Sharing architecture decision records in collaborative tools	(CAPILLA et al., 2006)
20	Promoting workshops with stakeholders	(AYUSO et al., 2011)
21	Mandating technical certification of software vendor consultants	(GOPAL; KOKA, 2010)

fixing errors in the future. The absence of automated tests result in an exponential increase in workload, raising the team's financial cost. The new governance strategy **(ST1)** to be adopted is based on the mechanism *"promote innovation"* **(M1)** to invest in innovative procedures that support the detection of defects preventively through automated test tools capable of performing tests, reporting results and comparing results with previous tests.

- **(UB) Software vendors deliverables are not satisfactorily accepted & (C) Evaluation criteria of software vendors does not exist**: the evaluation criteria should consider the performance of partner companies in past software development deliverables, the impact on the value chain, the ability to deliver future projects, and the financial health of the software vendor. When a software vendor delivers a poor quality product, value creation is damaged and less revenue is generated. The new governance strategy **(ST2)** to be adopted is based on the mechanism *"manage licenses"* **(M2)** to implement an effective supplier assessment process, capable of minimizing or eliminating great risks, cataloging all poor quality deliveries.

- **(UB) Difficulties in using the approval environment & (C) There is no concept of configuration architecture**: in software development environments, there is an infrastructure for homologating new programs similar to the production environment. The approval environment is smaller than production, but it has all the characteristics of the hardware and software infrastructure to ensure quality in the final tests. In this study, the organization does not have a specific environment for the homologation process, with inconsistency data and low tests quality. The new governance strategy **(ST3)** to be adopted is based on the mechanism *"create revenue models"* **(M3)** from which a software consultancy would be hired with the responsibility of maintaining the environment's configuration architecture. Architecture configuration management helps developing teams build robust and stable systems through the use of tools that automatically manage and monitor updates to configuration data. The support and service contracts for maintaining the environment would be a new source of revenue for the software consultancy.

- **(UB) Few software vendors with expertise & (C) Limited knowledge base**: with a limited knowledge base, the company becomes vulnerable, losing productivity and becoming dependent on people and software consultants to obtain important information for the business. A new governance strategy **(ST4)** could be adopted using the mechanism *attract and maintain varied partners* **(M4)** to open contracts for new players specialized in several subjects. The contracting consulting services will occur that gradually they can absorb the knowledge over time.

- **(UB) Tacit knowledge is concentrated in a few people & (C) There is no knowledge management culture**: tacit knowledge cannot be expressed through texts, images and documents and cannot be acquired from theoretical training. Tacit knowledge is on the employees' mind and has been absorbed daily. If the organization does not have the development of a knowledge management culture, it can be hostage from people and software consultants knowledge. The new governance strategy **(ST5)** to be adopted is based on the mechanism *"stimulate partner investments and share costs"* **(M5)**, in which the keystone encourages the software consulting to invest in a learning process and in the continuous improvement of intellectual capital through techniques such as coaching, mentoring, and training. In return, software consulting will receive new project demands gradually.

- **(UB) Only one software vendor has a proprietary product license & (C) Product is evolving in the maturity process within the organization**: the purchase of a particular product was linked to a license owned by a single software vendor. In the service contract between the keystone and the software vendor, the use of certified professionals in that technology was mandatory. The new governance strategy **(ST6)** to be adopted is based on the mechanism *"create partnership models"* **(M6)**. Alliances with new players will be proposed, expanding the product licenses to become another certificate partner in new technologies. As such, it will be possible to work together to increase efficiency, enhance returns, add skills, and reduce costs.

- **(UB) Cannibalization of human resources among software vendors & (C) Tacit knowledge is concentrated in a few people**: software vendors with greater purchasing power try to outsmart others by hiring experienced human resources from competitors. As such, they increase revenue from consulting services above the rest. The keystones must monitor the practices through the governance mechanism *"define rules to manage relationships"* **(M7)**, avoiding a predatory relationship that could cause disharmonious SECO relationships. The strategy **(ST7)** to be adopted is to balance the competition by contractually avoiding turnover (within the scope of people management, it is related to the dismissal of some employees and the entry of others). All software vendors must submit a monthly list of professionals who are requesting dismissal in order to verify any exchange among them.

- **(UB) Insufficient software vendors accountability & (C) Lack of governance for software vendors**: the keystone does not yet have a management model for software suppliers with defined processes, versatile tools, stakeholders visibility, transparency, and accountability. Software suppliers management is essential to ensure IT services quality. The keystone must use the governance mechanism *"establish roles and responsibilities"* **(M8)** to implement software suppliers management through guidelines and procedures such as: scheduling weekly status report meetings, highlighting a technical leader as a focal point, establishing a plan for achieving metrics and indicators, and defining SLA (Service Level Agreement is a commitment between a service provider and a client). Based on these governance practices **(ST8)**, the keystone will be able to more accurately measure and identify the risks they are exposed to.

- **(UB) Delivery failures & (C) Lack of alignment between stakeholders**: software development projects have different communication needs, depending on the complexity, the number of people, the culture and even the political moment of the organization. When communication needs do not happen, the project is exposed to failures and risks that can delay deliveries, affect the budget and reduce the quality of results. The keystone must use the governance mechanism *"enable effective communication channels"* **(M9)** to implement a communication management plan to ensure that information is available to people at the right time through an appropriate channel, so that information is transmitted as little noise as possible. Some strategies **(ST9)** will be carried out, such as the preparation of a manual of good practices for conducting meetings and the generation of minutes with the acceptance of the participants will be mandatory. The final document will be stored on a file server indexed by the project name.

- **(UB) Poor knowledge transfer from the project team to the sustaining team & (C) Lack of handover process**: at the end of the projects, teams are demobilized, deliveries are completed and the closing statement is sent to all the stakeholders. At this point, knowledge transfer must be carried out between the project team and the sustaining team. However, this activity is not performed correctly, as there is no handover process (i.e., transferring knowledge acquired in an activity). The keystone must use the governance mechanism *"manage conflicts"* **(M10)** to formalize an official handover process among software vendors avoiding disputes over new service contracts. This would also be a new strategy **(ST10)** to attract new partners, offering new business opportunities and balancing the SECO.

- **(UB) Incidents in the production environment increase organization expenses & (C) Root cause analysis is not performed**: gathering the sustaining team to correct bugs in the production environment increases the organization's expenses. Expenses negatively influence a financial market indicator known as EBITDA[2]. As long as there is no investment in a Root Cause Analysis (RCA) process, software bugs will be treated in a palliative manner and may recur in the future. The

[2] EBITDA or Earnings Before Interest, Taxes, Depreciation, and Amortization, is a measure of a company's overall financial performance. Simply, is a measure of profitability.

new governance strategy **(ST11)** to be adopted is based on the governance mechanism *"manage resources"* **(M11)** to implement a process capable of balancing the software assets improvements and evolutions through structural demands, making applications more robust. As such, the organization would increase investment in RCA and would decrease expenses with recurring bugs.

- **(UB) Low quality deliverables without penalties for software vendors & (C) Lack of a guarantee process**: constantly, updating products can pose a risk to other systems running. It is not uncommon to discover software project delivery with poorly designed code reuse, low performance, inadequate scalability, and a lack of confidence in data consistency. In the organization where this study was conducted, there is no penalty policy for the software provider. The keystone intends to improve this aspect through the governance mechanism *"manage risks"* **(M12)** with the strategy **(ST12)** of implementing a 90-day delivery guarantee process for software providers. During this period, any maintenance will be the responsibility of the software provider. In this situation, the keystone must manage the risks in decision making among maintenances and software evolutions.

- **(UB) Operational tasks become more important than structural projects & (C) Lack of strategic vision of the software vendor**: software vendors are very present in the organization's day-to-day operations. There are countless opportunities to propose several improvements such as refactoring the architectural design of some applications, new solutions aligned with technological innovation, training, and process automation. Therefore, software vendors lack strategic vision for new business opportunities. The new governance strategy **(ST13)** to be adopted is based on the governance mechanism *"manage expectations"* **(M13)** to schedule an executive monthly meeting in which software vendors will present new solutions that can add value to the business and make them recognized and differentiated from their competitors, providing another opportunity to increase revenue.

- **(UB) Exhausted limit of the sustaining team's productivity capacity & (C) Developers are looking for other job opportunities constantly**: sustaining team is constantly under pressure to increasingly correct bugs as quickly as possible. It creates a situation of tension and stress where not everyone knows how to deal with it. The threat leads developers to look for other job opportunities directly affecting the productive capacity of the team, that is, the number of services with a certain amount of human resources, in a given period. The new governance strategy **(ST14)** to be adopted is based on the governance mechanism *"nurture collaborations"* **(M14)** to implement the job rotation culture. It is the most dynamic way to train and adapt internal employees and software vendors on a daily basis. In practice, it is the understanding of different areas of the organization and its importance increases throughout the organizational system. The goals are: i) learning about the business with a macro view according to the different processes and multiplying the knowledge so that more than one person is qualified for the job activity; and ii) motivating and not overloading the same people with repetitive activities.

- **(UB) Software vendors do not have autonomy to propose improvements to business managers & (C) Meetings with business managers must take place with the presence of an employee of the organization**: this study was carried out in a bureaucratic organization with rules, regulations, processes, procedures and standards formulated to guide the functioning of the organization. One of these rules is the prohibition of direct contact between software vendors and business managers. The new governance strategy **(ST15)** to be adopted is based on the governance mechanism *"support autonomy"* **(M15)** to authorize meetings with the presence of at least one participant of the sustaining team, guiding the limits that the software vendor may have. For example, hiring new licenses can only be done by the keystone IT manager. A contractual penalty may be applied to a software vendor if the rule is disregarded.

- **(UB) Tacit knowledge is concentrated in a few people & (C) Difficulty finding professionals with expertise and skills**: the resistance to sharing knowledge allows a false notion that information belongs of a single owner. The organization becomes hostage to people and software consultants. In addition, dependence on people prevents proper management of processes, systems and indicators. The keystone must use the governance mechanism *"share knowledge"* **(M16)** to establish a knowledge management strategy **(ST16)** with clear policies present in the organization, such as training in the company, professional development courses, lectures with technical and business matters, and acquisition of collaborative tools. These practices should encourage employees and software consultants to participate, as the focus on sharing information facilitates the dissemination of knowledge in a fluid and natural way.

- **(UB) Battle among software vendors for control of the product's most valuable features & (C) Obtain competitive advantages to negotiate better service contracts in the future**: the most attractive features are desired by software vendors with the intention of negotiating new requirements, demands and projects. Through the governance mechanism *"distribute power"* **(M17)**, the keystone must establish a balance strategy **(ST17)** among all software vendors. Based on some characteristics such as innovation, prices, quality and deadlines, it will be up to the organization to choose and define the appropriate software supplier. As such, the keystone will prevent a possible imbalance in the future where software vendors with greater purchasing power tend to beat the competition.

- **(UB) Software vendors are unaware of the organization's manuals, guidelines, policies, and processes & (C) Lack of definition of minimum requirements for new players**: new players want to establish themselves in a market to which they do not belong. In our case, they are software suppliers who intend to provide IT consulting services and software development that need to present quality before others already consolidated in the organization. However, the new players need to overcome the challenge of entry barriers, such as mastery of technologies and processes, learning curve and initial capital investment. Through the governance mechanism *"define entry requirements"* **(M18)**, the keystone must provide a manual with guidelines and minimum requirements for the selection of new players such as knowledge of organizational processes, service structure, and commercial office and references from professionals demonstrated through successful cases **(ST18)**.

- **(UB) Developers neither know architectural recommendations nor have a best practice manual & (C) Application development framework documents are missing**: the decisions made on a software project are often consequences of the company's culture, the development process or the restrictions existing at the time of decision making. Software developers can make a decision or implement something that was decided without even agreeing. The keystone must use the governance mechanism *"share architectural decisions"* **(M19)** to use a collaborative content management and document management tool (such Microsoft SharePoint) to store and share Architecture Decision Record (ADR). ADR is a document that captures a decision, including the context of how the decision was made and the consequences of adopting it **(ST19)**.

- **(UB) Stakeholders do not have visibility on the evolution of the product & (C) Lack of sharing roadmap products by bussiness managers**: the study was carried out in an organization that does not have a culture of publicizing the launch planning of products and frameworks. It is important that all stakeholders have access to the roadmap. That way, they will know what stage the process is in and what the next steps are. The strategy **(ST20)** to be adopted by the keystone using the governance mechanism *"share roadmaps"* **(M20)** is to constantly promote workshops with all stakeholders, including IT professionals. The workshop is a moment of learning and knowledge transfer where the main advantage is that it takes place quickly and dynamically, allowing to glimpse which aspects deserve more attention.

- **(UB) Poor quality product with many defects & (C) Software developers without proper technical certifications**: the quality of the software product is directly related to the quality of the process that produces it and to the experience and expertise of the professionals involved in the software project. The strategy **(ST21)** to be adopted by the keystone using the governance mechanism *"define quality standards and certifications"* **(M21)** is to force software vendors consultants to be certified according to the area of expertise. For example, developers must prove proficiency in the fundamentals of Java programming. A project manager must take Project Management Professional Certification and so on. The technology market is extremely dynamic and requires IT professionals to keep up to date. The main reason for requiring certifications is to prepare the IT professionals to perform specific functions in certain areas with quality.

Measuring SECO performance is essential for the success of a good management, knowing and understanding whether the organization is on the desired path and how much remains to reach the objectives. The complementary information allows managers to monitor the results and, through a continuous improvement process, optimize the adjustments to achieve the objectives satisfactorily. Table 4.3 summarizes the references that support new governance strategies for each mechanism. The application of metrics will cause board members to govern, control, and manage SECO. Managers can make better decisions when, where, and how to invest and will have the indicators to assess which governance techniques are effective for proprietary SECO.

Based on GQM approach, we are inspired to link the governance strategies **(ST1 to ST21)** adopted for each governance mechanism with the health metrics provided by Alves *et al.* (ALVES; OLIVEIRA; JANSEN, 2017) as shown in Table 4.4. The GQM approach is a proven method for driving goal-oriented measures throughout a software organization. The GQM model is developed by identifying a set of quality and/or productivity goals. With GQM, we start by defining the goals we are trying to achieve, then clarifying the questions we are trying to answer with the data we collect. Measurement definitions occur in a top-down way, that is, we identify the goals, questions, and measurements that will answer both questions quantitatively and qualitatively (CALDIERA; ROMBACH, 1994).

Table 4.4: Proprietary SECO strategies using GQM approach to assess governance mechanisms (ALVES; OLIVEIRA; JANSEN, 2017) proposed in participative case study.

Strategy	Health Indicator	Health Metric(s)
ST1	Productivity	Productivity improvement; Technologies/innovations introduced; Return on invested capital
	Robustness	Artifacts quality and certification model; Core network consistency; Switching costs; Revenue increase
	Niche creation	Value creation and innovations
ST2	Productivity	New related projects
	Robustness	Artifacts quality and certification model; Community building/Partnership model
	Niche creation	Visibility in the market/Reputation
ST3	Productivity	Productivity improvement; Technologies/innovations introduced; Return on invested capital
	Robustness	Artifacts quality and certification model; Revenue increase
ST4	Productivity	Active contributors/developers
	Robustness	Community building/Partnership model
	Niche creation	Variety; Openness/transparency level
ST5	Productivity	Active contributors/developers; Return on invested capital
	Robustness	Switching costs; Community building/Partnership model; Profit growth
	Niche creation	Variety; Average number of supported languages; Perceived level of intimacy/Orchestrator support
ST6	Productivity	Active contributors/developers
	Robustness	Community building/Partnership model
	Niche creation	Value creation and innovations
ST7	Productivity	New related projects
	Robustness	Core network consistency
	Niche creation	Perceived level of intimacy/Orchestrator support
ST8	Productivity	Productivity improvement; Orchestration techniques
	Robustness	Core network consistency
	Niche creation	Value creation and innovations; Visibility in the market/Reputation
ST9	Niche creation	Number of new projects

Table 4.4 continued from previous page

Strategy	Health Indicator	Health Metric(s)
ST10	Productivity	New related projects; Active contributors/developers; Number of Apps/projects/extensions
	Robustness	Core network consistency; Community building/Partnership model
	Niche creation	Variety
ST11	Productivity	Return on invested capital
	Robustness	Persistence of structure; Stakeholder/Contributor satisfaction
	Niche creation	Visibility in the market/Reputation
ST12	Robustness	Artifacts quality and certification model
ST13	Productivity	Technologies/innovations introduced
	Robustness	Persistence of structure
	Niche creation	Value creation and innovations
ST14	Productivity	Events for developers; Active contributors/developers
	Robustness	Community building/Partnership model
ST15	Productivity	Productivity improvement
	Robustness	Stakeholder/Contributor satisfaction
	Niche creation	Perceived level of intimacy/Orchestrator support
ST16	Productivity	Active contributors/developers
	Robustness	Community building/Partnership model
	Niche creation	Perceived level of intimacy/Orchestrator support
ST17	Productivity	Number of Apps/projects/extensions
	Robustness	Community building/Partnership model
	Niche creation	Value creation and innovations; Number of new projects
ST18	Productivity	Active contributors/developers
	Robustness	Community building/Partnership model
	Niche creation	Value creation and innovations; Entry barriers
S19	Productivity	Productivity improvement
	Robustness	Artifacts quality and certification model
	Niche creation	Entry barriers; Average number of supported languages
ST20	Productivity	Technologies/innovations introduced
	Robustness	Artifacts quality and certification model
	Niche creation	Variety; Number of new projects; Visibility in the market/Reputation; Average number of supported languages

Table 4.4 continued from previous page

Strategy	Health Indicator	Health Metric(s)
ST21	Productivity	Active contributors/developers; Return on invested capital
	Robustness	Artifacts quality and certification model; Community building/Partnership model; Stakeholder/Contributor satisfaction
	Niche creation	Value creation and innovations; Visibility in the market/Reputation; Entry barriers; Average number of supported languages

4.6 Opinion survey

Evaluation procedures face several challenges. In addition to the quality, relevance and timeliness of the evaluation itself, a major challenge lies in conveying the evaluation results to multiple audiences inside the organization (PRICE; HANDLEY, et al., 2010). Thus, feedback and communication of evaluation results are integral parts of the evaluation cycle as mentioned in the studies (LAANTI; SALO; ABRAHAMSSON, 2011)(LO; NAGAPPAN; ZIMMERMANN, 2015) (SOUZA; MOREIRA; FIGUEIREDO, 2019). Effective feedback contributes to improving development policies, procedures and practices by providing relevant information to researchers making future decisions. In our study, we monitored an improvement cycle with new strategies based on governance mechanisms, which in turn are associated with SECO health metrics.

Although we based our longitudinal literature study protocol as an update and refine the previous study of Alves *et al.* (ALVES; OLIVEIRA; JANSEN, 2017), our research focus is on governance mechanisms and strategies. By selecting appropriate governance mechanisms, organizations can gain a strategic advantage over others leading them to better performance. The governance mechanisms and the metrics have a more operational focus while the strategies have an organizational one. We direct our efforts towards the governance mechanisms research in a real scenario and will target SECO health metrics in more depth on how to operationalize them for future studies.

4.6.1 Planning

The opinion survey aiming to verify the participants' level of perception about strategies related to SECO governance mechanisms. The survey consists of an electronic questionnaire to be filled in 20-30 minutes. It was sent to the participants' e-mails; in this case, experts of the sustaining team (developers and technical leaders) of a large international insurance organization in the context of its proprietary SECO. The complete questionnaire is presented in Appendix E.

The survey was split into 4 sections. In the first section, an introductory text was presented bringing the objectives of the questionnaire for academic purposes. In the second one, the participant should read and agree/disagree with the Informed Consent Term (ICT) before having access to the questions.

The third section aimed to characterize the professional profile of the participants. We asked the participants' hierarchical level (Junior, Intermediate, Senior). Finally, the fourth section contained four open questions related to the assessment of strategy of governance mechanisms and three questions using Visual Analogue Scale (VAS)[3] with 5 points: 1 (Strongly unsatisfied); 2 (Partially unsatisfied); 3 (Neutral); 4 (Partially Satisfied); and 5 (Strongly Satisfied). There was also one last question which the participant could write relevant and general comments on the topics covered in the study. We defined questions aligned with the survey's goals, as follows:

- Q1 - What are the benefits of SECO governance mechanisms to the organization?
- Q2 - What are the difficulties of SECO governance mechanisms to the organization?
- Q3 - What are the opportunities of SECO governance mechanisms to the organization in future use?
- Q4 - What are the threats of SECO governance mechanisms to the organization?
- Q5 - What is your perception on the strategies for adopting SECO governance mechanisms required for Value Creation category?
- Q6 - What is your perception on the strategies for adopting SECO governance mechanisms required for Coordination of Players category?
- Q7 - What is your perception on the strategies for adopting SECO governance mechanisms required for Organizational Openness and Control category?
- Q8 - Comments and/or suggestions. (not mandatory)

[3] VAS is a psychometric response scale which can be used in questionnaires. It is a measurement instrument for subjective characteristics or attitudes that cannot be directly measured.

For the evaluation and refinement of the instruments of this opinion survey, a pilot study was carried out with two participants. Finally, it was sent to the potential participants. The questionnaire is available at: `https://forms.gle/SadktvPSww4uYQpF8`.

4.6.2 Execution

The survey was sent by email to 12 participants of the organization's sustaining team (developers and technical leaders) affected by governance strategies in a proprietary SECO. 10 responses were submitted. The response rate (83%) corresponds to the audience of the sustaining team developers in the proprietary SECO of the organization studied.

The profiles in sustaining team that participated in the opinion survey require either a background as a software developer with additional operations experience or in an IT operations role that also have software development skills. The practitioners were the same as in the participative case study indicated in Section 4.4. The sustaining team is responsible for how code is deployed, configured, and monitored, as well as the availability, change management, emergency response, and capacity management of services in production environment. In short, they have a more comprehensive understanding of the governance strategies used daily.

4.6.3 Results

Regarding the respondents' hierarchical level, the majority (50%) is formed by senior developers, 30% of intermediate and 20% of junior developers. This information is consistent because professionals in sustaining team have to know how to deal with corrections of great complexity and which need to be carried out in increasingly shorter deadlines. At this level of seniority, the developers are prepared to work under strong pressure at certain times. We had a step of categorizing the responses of the participants considering the governance mechanisms used to address the 21 strategies. This step was reviewed by the other authors and aligned through a consensus meeting. Therefore, Table 4.5 was built with the governance mechanisms identified from the analysis of the text fragments of the responses of each respondent. We organized Table 4.5 through identifiers (IDs) corresponding to the governance mechanism that were being described.

We observed that the *share knowledge* **(M16)** mechanism is the most commented in the responses to benefits, difficulties and opportunities. Within the organization investigated in this study, it is a permanent concern and this result is fully adherent to the governance strategy **(ST16)**. The explicit and tacit knowledge are complementary and

Table 4.5: Governance mechanisms identified by each participant.

ID Participant	Benefits	Difficulties	Opportunities	Threats
#1	M2, M8, M17	M8, M17	M8	M6
#2	M3	M3	M3	M3
#3	M13	M13	M1	M1, M6, M15
#4	M16	M15, M16	M16	M19
#5	M5, M9, M10, M14	M5, M9, M10, M14	M5, M9, M10, M14	M5, M9, M10, M14
#6	M19, M16	M19, M16	M16	M19
#7	M1, M4, M11, M16	M1, M5, M16	M14, M20	M19
#8	M1, M7, M12, M21	M1, M7, M12, M16, M21	M1, M7, M16	M13, M17
#9	M4, M11	M17	M18	M17
#10	M6, M20	M14, M16	M7, M21	M16

can be acquired by employees through training. Employees are unable to make decisions and solve problems with only theory in mind. Without practice, employees are at risk of making mistakes when exposed to a real situation, which can be negative for both, employees and organization. That is why team members need a lot of practice aiming to learn from their mistakes, gain experience and develop new skills. They will be able to deal with different situations in reality. Therefore, training must offer explicit knowledge to employees and, at the same time, encourage practice to acquire tacit knowledge.

In the organization, the concern with knowledge sharing within the proprietary SECO becomes evident due to the organizational changes that have taken place in recent years by the company board, where IT senior professionals were encouraged to voluntary dismissal requests or get fired. The use of a knowledge base may provide tacit knowledge transfer in a secure manner and the risks of losing information could be mitigated if knowledge management policies existed.

Regarding the question on threats, the most cited governance mechanism was *share architectural decisions* **(M19)**. This is due to the fact that this mechanism is responsible for defining the organization's standardization and process integration requirements, i.e., the logical data organization, applications, and infrastructures defined from policies, relationships, and technical decisions adopted to serve the business area. This does not mean that it has to be rigid, but new and legacy applications need a solid foundation to be built and updated. Architectural decisions are difficult to get right and often no single optimal solution for any given set of problems exists. Before a decision is made, the decision needs to be negotiated, as the scope can influence the entire technological platform of the organization.

We highlighted the text fragments related with *share knowledge* **(M16)**:

- **Benefits (3 citations, corresponding to 30%):**

Preventing knowledge from focusing on few people.

[Participant #4]

It does not depend on software providers.

[Participant #6]

Spreading knowledge across the organization.

[Participant #7]

- **Difficulties (5 citations, corresponding to 50%):**

To increase the software development team, more financial investment will be needed.

[Participant #4]

Increasing and training the development team.

[Participant #6]

IT Professionals' resistance.

[Participant #7 and #8]

Hiring qualified people to absorb knowledge in complex technologies.

[Participant #10]

- **Opportunities (3 citations, corresponding to 30%):**

Having more qualified IT professionals, we will no longer have a bottleneck to solve some problems.

[Participant #4]

New software providers may be part of the solution.

[Participant #6]

Propagating knowledge across the organization and have a consolidated knowledge base.

[Participant #8]

The participants' text fragments mentioned in *share architectural decisions* **(M19)**:

- **Threats (3 citations, corresponding to 30%):**

> *The biggest threat will be applied to the software vendor who will need to have more management controls.*
>
> [Participant #4]

> *People's coincientization.*
>
> [Participant #6]

> *Sharing decisions risks exposing externally weaknesses and vulnerabilities.*
>
> [Participant #7]

We observed that participants highlighted other governance mechanisms, such as:

- **Benefits:**

  > *Through innovative technologies we will have opportunities to improve our daily work. (Promote innovation - M1)*
  >
  > [Participant #7]

- **Difficulties:**

  > *Aggressive delivery times on projects do not allow time for handover and collaboration processes. (Nurture collaborations - M14)*
  >
  > [Participant #10]

- **Opportunities:**

  > *Having more IT professionals with knowledge of diverse subjects, we will no longer have bottlenecks to s olve some problems. (Share knowledge - M16)*
  >
  > [Participant #8]

- **Threats:**

  > *Some people may feel threatened and may boycott this kind of initiative. (Share knowledge - M16)*
  >
  > [Participant #10]

Figure 4.1 shows the perception level about the strategies for adopting the governance mechanisms of *value creation*, *coordination of players*, and *organizational openness and control* categories by the participative case study's participants. For the governance mechanisms of the *value creation* category, 80% declared very satisfied and 20% little satisfied in adopting new strategies. We observed in the *coordination of players* category that 70% declared themselves very satisfied, 20% little satisfied, and 10% indifferent in adopting new procedures. Finally, the behavior of the participants in the *organizational openness and control* category noticed the lowest percentage of satisfaction that 60% declared very satisfied, 20% little satisfied, and 20% indifferent. In general, the study achieved the objectives by encouraging participants to use new guidelines, standards, and processes to ensure alignment between IT and the business plan aiming to generate value for the organization. We received an answer to the final question on comments or suggestions:

> *It was an interesting exercise which we had the opportunity to think of strategies that improve our daily work with IT software vendors.*
>
> [Participant #9]

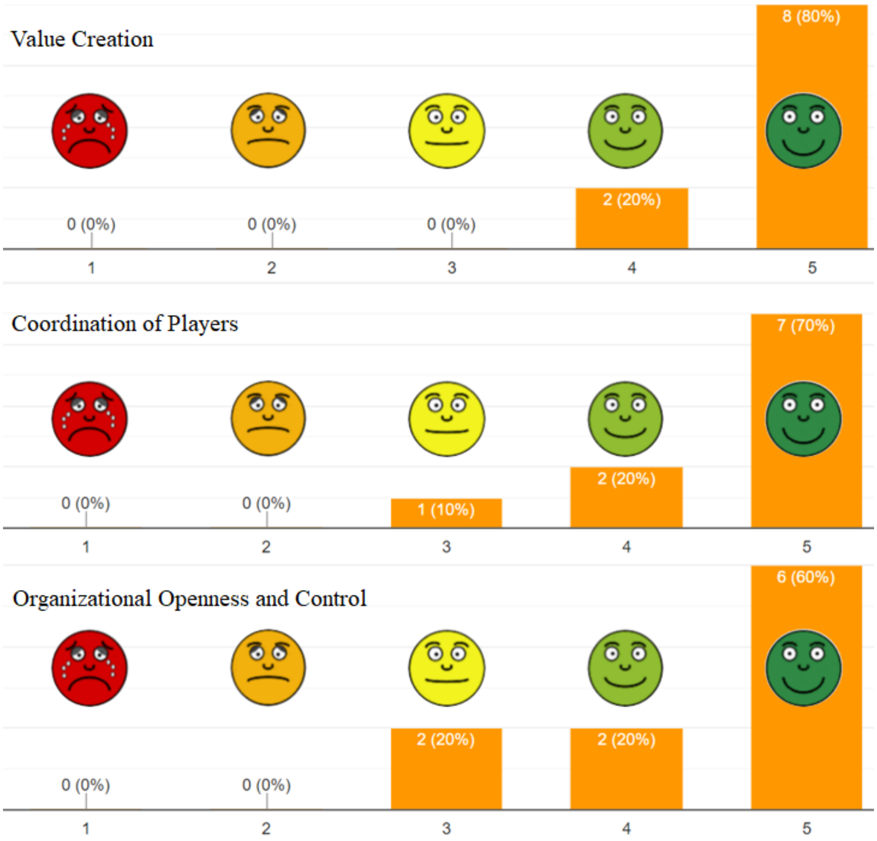


Figure 4.1: Perception for adopting governance mechanisms in proprietary SECO.

4.7 Discussion and implications

The researchers discussed the practical implications through working meetings based on the results of previous studies to provide a research agenda for the academic community and the software industry. This section serves to discuss the practical implications for both scenarios.

For the academic community, we realized that ecosystem governance influences the ecosystems health. This means that governance strategies and managerial decisions taken by keystones will affect the healthy evolution of the entire ecosystem. There are health metrics that provide operational indicators on how SECO are governed. The concept of ecosystem health is related to the performance of each participant and consequently with the performance of the entire ecosystem. By using SECO health metrics to improve efficiency, support decision making and increase participants' satisfaction, the keystone will gain a competitive advantage in the market, generating attraction for new participants and new business opportunities for the entire community.

In the governance mechanisms identified by *value creation*, *coordination of players*, and *organizational openness and control* categories (ALVES; OLIVEIRA; JANSEN, 2017), we verified a small trend of change in the literature body as described in Section 2.3.2. The governance mechanism *nurture collaborations* belonging to the Coordination of Players category had the highest percentage increase in the citations of the studies. In the other categories, the governance mechanisms *attract and maintain varied partners* e *share knowledge* remained as the most relevant ones. The increased literature citations of *nurture collaborations* is due to the need to establish collaboration between players and stakeholders in SECO, aiming to form partnerships and to improve ecosystem performance. In this scenario, collaboration can be defined as a decision-making process between business partners, with integrated responsibility for results (STANK; KELLER; DAUGHERTY, 2001). A good partnership offers investment in resources, information sharing, rewards, and responsibilities (SOOSAY; HYLAND; FERRER, 2008).

For the software industry, based on our findings and their relevance, we verified that most of the governance strategies that were addressed in the organization are concerned with knowledge management, software assets quality, and investment in innovative solutions. These actions aim to obtain competitive advantage over competitors. Innovation is increasingly important for companies' strategy and innovation management seeks to boost the organization's culture and processes in order to transform the business (BETZ, 2003). Companies need to innovate in order to stay ahead of their competitors, adopting new management and process models, and adhering to new technologies. The ultimate goal is customer satisfaction with the active participation of employees.

Software systems have evolved and become more complex due to the growing demand from customers and users. In this context, the software product quality becomes a competitive differential (POWELL, 1995). The great challenge for organizations is to provide quality products, with shorter delivery times and reduced costs. Organizations that face high levels of demand consider quality management as a competitive differential.

Knowledge management is an important practice in organizations that want to be competitive (NDLELA; DU TOIT, 2001). Organizations motivated by the advancement of innovative solutions, increased productivity and improved product quality need to transform tacit knowledge (acquired throughout life based on experience) into explicit knowledge (stored in some way). In order to transfer knowledge between employees, it is necessary to overcome barriers such as professional insecurity and power (SINGH; KANT, 2008). Knowledge transferring may mean loss of influence, reputation, respect and job security. Therefore, to implement knowledge management systems, it is necessary to have an alignment among comprehensive view, information technology and people management.

Finally, the traditional IT processes of an organization tend to move slowly to prevent instabilities from disrupting the company's productive activities (HOCHSTEIN; ZARNEKOW; BRENNER, 2005). The transition to a service management model framework that is concerned with the development of people, processes and technology, such as ITIL, aims to reduce or eliminate waste from productive activities. This requires changes in culture organization and actions in governance that will add more value to the company. The use of metrics is different in each scenario. While in traditional IT the objective is to reduce costs and time of activities, ITIL concept suggests that the improvements applied should always be related to the company's strategic objectives (HOCHSTEIN; ZARNEKOW; BRENNER, 2005). Another different view of ITIL concept is in knowledge management and team organization. The suggestion is that knowledge is widespread, that is, an IT employee is able to work in several business fields, differently from the specialist model in traditional IT. In the proposed scenario, the team becomes multifunctional, capable of working within several areas, and no longer centralized in a business area.

There is a famous Peter Drucker quote that says that *"culture eats strategy for breakfast"*. This implies that the culture of the organization always determines success regardless of how effective one's strategy may be (DRUCKER, 1995). Drucker pointed out the importance of the human factor in any company. No matter how detailed and solid the strategy is, if the people executing it do not nurture the appropriate culture, the projects will fail. While strategy defines direction and focus, culture is the habitat in which strategy lives or dies (DRUCKER, 1995). Strategy focuses on a leader's skills, while culture defines engagement and execution. With proper strategy, the organization creates the rules for playing, but culture determines the way the game will be played (DRUCKER, 1995).

In short, the organizational culture leverages or overturns the strategy. Any change in goals must come with an analysis of the organizational culture to understand whether the objectives are converging or not. Everything that happens in the organization, consciously or not, communicates messages that are decoded by people (HATCH, 1993).

4.8 Threats to validity

The reliability of the results is directly linked to the validity of the study. Every study has threats that should be addressed and considered together with the results, considering the classification proposed in (RUNESON et al., 2012).

On the participative case study, this type of study is biased and subjective because the results depend on the researchers acting directly in the case as a professional (BASKERVILLE, 1997). The researcher who conducted the study gave the lecture, followed the day-to-day observation, guided the interviews, and promoted the discussion operates in the organization where this study took place. The researcher participation affects *Internal Validity*, which is concerned with the relationship between results and the applied treatment, *External Validity*, which refers to how to generalize the findings to apply to other settings from a case-specific until different cases, and *Reliability Validity*, which regards to what extent data and analysis rely on or are linked to a specific researcher.

As *Constructo Validity*, which is concerned with the relationship between theory and observation, in other words, it refers to the extent to which the experiment setting reflects the theory, the main threat is that we did not define indicators to evaluate results. Data collection was performed through interviews, which involve subjectivity. To mitigate this threat, we double-checked with the participants all the obtained strategies in order to establish a relationship between our experiment and the observed outcomes, and ensure that there is a correspondence to the cause we have controlled. Moreover, we define some measures to the sustaining team aimed to evaluate the new behaviors caused by the proposed strategies. Regarding the mentioned threats that restrict the generalization of the results, the study involved only one organization. Thus, it is not possible to generalize the results to cases without intervention by the researcher or to organizations not similar to the studied organization (Banking, Financial Services and Insurance industry - BFSI).

As *Criterion Validity*, which involves the correlation between the survey and a criterion variable taken as representative of the constructo, in other words, it compares the survey with other measures or outcomes already held to be valid (DROST, 2011), we ensure that all respondents participated in the case study. To reduce the threats, two other researchers outside the organization also evaluated the collection, data analysis, and participated in the results discussion.

4.9 Final remarks

We described a participative case study carried out in a proprietary SECO of a large insurance organization. Information were gathered to understand the current governance practices in the organization and defined new strategies to implement governance mechanisms related to proprietary SECO health metrics. As result, we verified that most of the governance strategies that were addressed in the organization are concerned with knowledge management, software assets quality, and investment in innovative solutions. All these actions aim to obtain competitive advantage over competitors.

As lessons learned, the system complexity is becoming exponentially more difficult to plan for because of the increased velocity, diversity of platforms, and interdependencies between distributed application components (ELSAYED, 2020). Even so, IT managers are beset by high expectations of offer reliability in modern and complex environments. We have a central organization with concerns on different platforms, mixed technologies, internal and external developers, different IT software providers, organization IT managers, and the emergence of new software projects frequently.

Moreover, to meet the market pressure from state-of-the-art solutions, the IT managers try to implement more software projects than they can. As one of the consequences, new software releases bring new production defects and stability concerns (ELSAYED, 2020). This behavior leads to customer dissatisfaction. Considering the new strategies to implement governance mechanisms related to proprietary SECO health metrics relating to the old ones, our study takes a position that quality and reliability are related.

From an academic point of view, there is an opportunity for further studies on how to address the reliability in platform software projects considering IT service providers of a proprietary SECO. As practical implications, organizations need to rethink the allocation of resources across a portfolio of projects due to the productive capacity of the IT managers that cannot lead several projects at one time.

Finally, we performed a feedback and communication of evaluation outcomes through an opinion survey aiming to verify the participants' level of perception about the new strategies related to SECO governance mechanisms. As result, we achieved the objectives by encouraging participants to use new guidelines, practices, standards, and processes to ensure alignment between IT and the business plan aiming to generate value for the organization.

5. An Approach for Incident Management to Support Governance in Proprietary Software Ecosystems

In this chapter, we present the PSECO-IM approach, a set of studies that helped us to concept of a process-based approach for incident management to support governance in a proprietary SECO. The PSECO-IM approach consists of the process (PSECO-IM process) and the support tool (PSECO-IM tool). PSECO-IM tool was developed in order to instantiate part of the PSECO-IM process. The dashboard report aims to support the IT management team with confidence level assessment of the proprietary SECO.

5.1 Introduction

Analyzing the SECO relationships between organizations where several actors are involved, such as outsourcing companies, software providers, developers, and IT managers is not trivial due to its complexity and need balance similarly to natural ecosystems. In addition, it does not have enough support according to the initial ad hoc literature review (Chapter 2). The information available to IT managers and architects for making decisions is often tacit knowledge or data spread through several outdated documents.

The organization that is responsible for keeping the proprietary SECO platform which is characterized by overcrowding of several products, technologies, and architectures of other ecosystems, must establish governance policies as a critical strategy for ensuring a sustainable platform.

There are some studies pointing out causes of systems unavailability that harm an organization's sustainability, productivity and revenue, in addition to damaging its image and reputation. The lost time and money associated with downtime causes far more than an inconvenience. The incidents can easily inflict a blow capable of driving an organization out of business altogether.

The information stored in a database is valuable for IT managers to understand how the proprietary SECO is formed and the relationships among its players. In other words, they require information and a visualization model, such a dashboard, that helps them to identify who is unbalancing the ecosystem as a whole.

The way in which architectural decisions are made changes as IT managers comprehend the behavior of the proprietary SECO. Recent changes in production environment may disturb the ecosystem, causing incidents. Most organizations invest heavily in incident management systems to enable smooth resolution processes. However, a lot of them struggle to meet Service Level Agreements (SLA) because of the huge number of incidents being raised every day. Every incident that is raised in the system costs money and man hours. The sustaining team are so stressed and busy resolving incidents that there is little or no time left for innovation.

In this context, we developed a solution approach based on the principle that the organization still needs processes and mechanisms to reduce incident volume in the proprietary SECO. However, as a strategic driver, instead of focusing on backlog incidents, the goal is to avoid open ones. Every change made in the applications (web, mobile, and desktop) or infrastructure has the potential to cause incidents and disruption, e.g., deploying changes with insufficient test coverage can give rise to major incidents. Therefore, we develop a support tool to evidence potential risks of a change, formulate ways to mitigate them, and identify potential risk drivers.

Traceability for this incident management approach is based on ITIL best practices combined with the longitudinal literature study as described in Section 2.3. The contribution to the customization of the process aimed at proprietary SECO came from the rapid review study and the participative case study, also described in Sections 2.4 and 4.1. The proposed approach must be performed by the organization to improve incident management process.

This chapter is organized as follows: Section 5.2 presents the main research question; Section 5.3 explores the approach of incident management in the proprietary SECO; Section 5.4 describes the support tool; Section 5.5 outlines the importance to conduct our study and discusses the results; and finally, Section 5.6 concludes the chapter.

5.2 Research question

The goal of this study is to understand the incident management in a proprietary SECO of a large international insurance organization. The research question for this study is: *"How to reduce incident backlog on a technological platform of the proprietary SECO?"*.

5.3 PSECO-IM: approach definition to support governance

This section presents an incident management approach to be explored within the existing relationships to support governance in the proprietary SECO, where we have a central organization with concerns about the technological platform, mixed technologies, internal and external developers, different IT software providers, organization IT managers, and the emergence of new software projects frequently. Our approach proposal relating to the processes involved in incident management *(PSECO-IM process)* is based on previous studies (COSTA; FONTÃO; SANTOS, 2020a) (COSTA; FONTÃO; SANTOS, 2021b) (COSTA; FONTÃO; SANTOS, 2021c) (COSTA; FONTÃO; SANTOS, 2021d) and ITIL guidelines (LONG, 2012) with two processes: incident handling and backlog incident diagnosis, as shown in Figure 5.1. Next, we propose a tool *(PSECO-IM tool)* to support the decision-making of the IT management team.

The blue objects in Figure 5.1 were based on ITIL guidelines combined with our longitudinal literature study (Section 2.3). The yellow objects were grounded on the contributions of our previous studies that led us to customize the incident management process in order to meet the needs of a proprietary SECO. The contributions came from the rapid review study (Section 2.4) and the experts' opinions that emerged in the participative case study (Section 4.7).

As noticed in Chapter 4, the participative case study gathered some undesirable behaviors that happened in the daily routine associated with several causes in the studied organization. To cite a few, the proprietary SECO suffered from: i) project deliverables with many defects due to low quality; ii) software providers' deliverables are not satisfactorily accepted by the organization; and iii) incidents in the production environment increase organization expenses.

In addition to this scenario, as described in Chapter 2 (Section 2.4), most studies discuss solution alternatives related to incidents backlog reduction rather than incidents opening reduction. We ground our approach on these studies aiming that senior leadership may change the focus of the organization's main strategic driver: from reducing backlog incidents to reducing open incidents. To do so, we customized and enhanced the incident management process (Figure 5.1) that was based on ITIL best practices in order to create a new metric to reveal the number of major incidents resulting from recent changes.

This metric is not just for eliciting positive reactions or drumming up interest from senior leadership. Major incidents resulting from changes may be one of the most effective metrics in the technological platform of the proprietary SECO because it shows the service quality level of the software assets being deployed. It holds teams accountable for the impact they have on the business. It gauges the interruption to the business caused by IT itself. In other words, it is the "shoot ourselves in the foot" measurement.

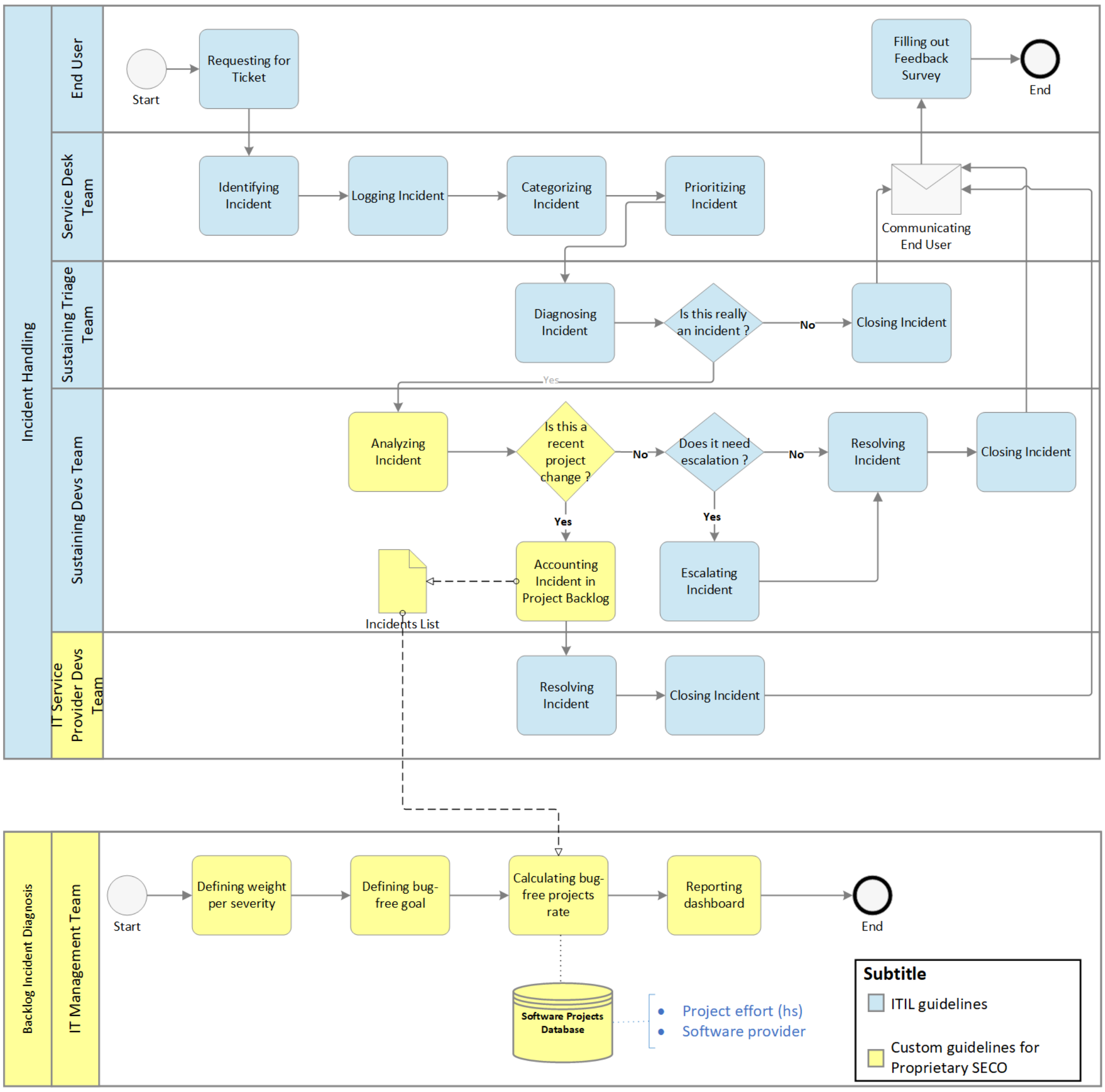


Figure 5.1: Incident management process.

5.3.1 Activities on incident management process to support governance in proprietary SECO

Incident management is closely aligned with the service desk team, which is the single point of contact for all users communicating with IT. When a service is disrupted or fails to deliver the promised performance, it means an incident (HOCHSTEIN; ZARNEKOW; BRENNER, 2005). The major goal of incident management is to get the service restored to a normal level of operation as quickly as possible. According to ITIL Service Operation book (LONG, 2012), the flow of basic activities (the blue ones in Figure 5.1) involved in the incident management process are:

1. **Requesting for Ticket** - most incidents originate on calls made by end-users of the system;

2. **Identifying Incident** - incidents can be identified by the service desk team, by monitoring systems, and by the users. Therefore, calls arrive through different channels such as chat, e-mail, and instant messaging;

3. **Logging Incident** - all incidents must be recorded according to the ITIL ticket system tool adopted by the organization (e.g., JIRA Service Management, HP Application Lifecycle Management). This step creates a history that makes it possible to consolidate a knowledge base. Therefore, whenever the service desk team receives a call, they can consult the base and check if this incident has already been resolved and what solution was found. The registration also facilitates workflow communication;

4. **Categorizing Incident** - the service desk team will classify the incident and make sure if it is an incident. Otherwise, the service desk will delegate to the appropriate process. In this step, we also define the catalog service to which the incident is related;

5. **Prioritizing Incident** - it is the step of defining whether the incident should be dealt with now or you can wait a while. To do so, it is necessary to use criteria related to urgency and impact. An urgent incident needs to be dealt with immediately. An impacting incident can generate great risks to the business;

6. **Diagnozing Incident** - it is the understanding phase. This activity comprises the entire process of searching for a solution. Typically, the sustaining triage team searches for answers in the knowledge base, in the organization's technical procedures, together with IT service providers or with colleagues. It is also important to

notice that, if the attendant realizes that information is missing for a resolution, it should be requested to the user or the person in charge;

7. **Escalating Incident** - if the first-level support does not have the necessary technical knowledge to resolve the incident, he will delegate the task to the second-level. It is very interesting to have this division of care into levels because it generates a better distribution of tasks according to the skills of the team. We should avoid the most expensive sustaining team member to waste time dealing with small incidents that could have been resolved by other developers;

8. **Resolving Incident** - it is the phase in which the incidents are resolved, either by the first-level support or later. In addition to resolving the user´s request, the attendant must also record all relevant information about the incident and resolution. Another very important point is to guarantee that the incident has been resolved by communicating with the user. The resolution of an incident can erase traces and evidence that could be used to solve a problem (root cause). Therefore, care must be taken at this time;

9. **Closing Incident** - it is the closing of the incident, which must be documented for future searches. It is also necessary to export the information to the knowledge base, making it accessible to any other person. If this base does not feed, there is a risk of wasting time trying to find a solution to an incident that has already been resolved before; and

10. **Filling out Feedback Survey** - it is the post-closure survey conducted to collect the end-user feedback. It should be used to gain insights in some key areas, such as: i) if there was any difficulty for the end-user to report an incident; ii) whether the incident was resolved promptly; and iii) whether the end-user is satisfied with the resolution.

The main reason for this sequence of activities is they flow from general to specific, but each organization has its own peculiarities, such as the empowerment of managers (LONG, 2012). Eventually, we should adopt new activities to meet some specific needs. It was the case evidenced in our work and according to the discussions of the studies (COSTA; FONTÃO; SANTOS, 2021c) (COSTA; FONTÃO; SANTOS, 2021d), we aggregate other activities (the yellow ones in Figure 5.1) related to the incident management process in the context of a proprietary SECO, as follows:

1. **Analyzing Incident** - it is the phase where the incidents are already being analyzed by the sustaining developers team. This team organizes the incoming appointments,

distributes them according to sustaining specialist developers, and verifies if the incident is valid. In many cases, the tickets are opened due to a lack of knowledge of business rules, causing an undue perception of system error;

2. **Accounting Incident in Project Backlog** - it is the phase where the sustaining developers team designates the name of the software project that caused the incident, directs to the project developers team, and updates the severity impact (scale values: low, medium, high, and critical) due to further investigation;

3. **Defining weight per severity** - it is the step where the IT manager defines a weight for each incident severity (scale values: low, medium, high, and critical);

4. **Defining bug-free goal** - it is the step where the IT manager defines a reliability goal for each software project and each IT service provider;

5. **Calculating bug-free projects rate** - it is the step where the IT manager calculates a reliability rate for each software project and each IT service provider; and

6. **Reporting dashboard** - it is the phase in which the measurement reports related to the reliability rates of the software project and the IT service provider are performed. The report provides inputs so that the IT manager can make decisions related to the governance of the technological platform.

5.3.2 Processes on proprietary SECO

Based on the activities mentioned in the previous section, we established where the processes can be applied. A process is a series of steps and decisions involved in the way work is completed. The main components of any process are events, tasks, inputs, and outputs (FEILER; HUMPHREY, 1993).

From the analysis of the activities and elements that compose a proprietary SECO, it was possible to identify relations among actors and the processes as shown in Figure 5.2: i) incident handling - emerges from the interaction among end-user, service desk team, sustaining developers team, and IT software providers developers team; and ii) backlog incident diagnosis - emerges from the interaction among sustaining developers team, IT management team, and central organization.

Sminia (SMINIA, 2009) highlights the importance of organizing processes in a company, such as:

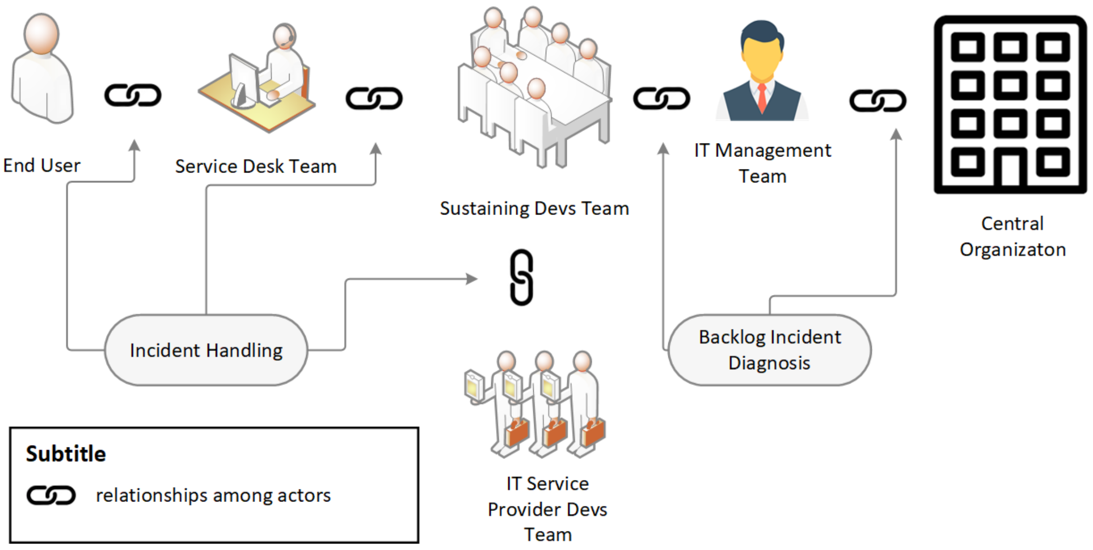


Figure 5.2: Relations among actors and the processes: incident handling and backlog incident diagnosis in a proprietary SECO.

- **Increased productivity** - organized processes flow quickly between departments, no more time is wasted on rework or procedures that do not add value to the end-user;
- **Reduce costs** - it is possible to keep smaller teams and focused on strategic rather than operational activities; and
- **Deciding on grounds** - the organization of processes contributes directly aiming to make decisions more consciously, as the data is organized, classified, and available in real-time. By eliminating uncertainties, risks are reduced and opportunities are maximized.

The PSECO-IM approach details that can be applied to any proprietary SECO and contributes to the maintainability and health of the technological platform is presented in the next section.

5.3.3 Approach details to support governance in the proprietary SECO

The notation used for modeling the processes that make up the proposed approach was based on the BPMN (Business Process Model and Notation)[1] notation because of the easy to describe step-by-step logic of a process thought diagrams. It is possible to have simply

[1] BPMN was originally developed by the Business Process Management Initiative (BPMI). They released a version 1.0 to the public in May, 2004. In June 2005, BPMI merged with OMG, the Object Management Group.

and directly, a graphical view to demonstrate the entire business process. The approach is composed as follows:

1. **Incident handling** - five actors, thirteen activities, and one artifact;
2. **Backlog incident diagnosis** - one actor and four activities.

5.3.3.1 Incident Handling Process

The main goal of the incident handling process is to orchestrate all the steps for addressing an incident from the first contact of the user until the evaluation of the service at the time of the ticket's closing. The management cycle goes through the identification, logging, categorization, prioritization, analysis, diagnosis, accounting, escalation, resolution, and closing steps. Besides, it aims to coordinate some relationships among the service desk team, sustaining developers team, and project developers team actors with the concern of accomplishing the SECO indicators. The roles responsible and participant, and the artifact are described in Table 5.1 and 5.2.

Table 5.1: Roles in incident handling process.

Role	**Central organization**
Description	Responsible for providing standards and practices to handle an incident in the technological platform.
Type	Responsible
Reference	(MOELLER, 2013) (COSTA; FONTÃO; SANTOS, 2020a) (COSTA; FONTÃO; SANTOS, 2021b) (COSTA; FONTÃO; SANTOS, 2021c) (COSTA; FONTÃO; SANTOS, 2021d)
Role	**End-User**
Description	Responsible for consuming any software service or for using particular software product.
Type	Participant
Reference	(LONG, 2012) (COSTA; FONTÃO; SANTOS, 2021d) (COSTA; FONTÃO; SANTOS, 2021c)
Role	**Service Desk Team**
Description	Responsible for the primary point of contact for users when there is a service disruption. They are collaborators who belong to the central organization.
Type	Participant

Table 5.1 – continued from previous page

Reference	(LONG, 2012) (COSTA; FONTÃO; SANTOS, 2021c) (COSTA; FONTÃO; SANTOS, 2021d)
Role	**Sustaining Triage Team**
Description	Responsible for the first check and for performing the administrative tasks necessary to support activities within the process. They are internal developers.
Type	Participant
Reference	(COSTA; FONTÃO; SANTOS, 2021c) (COSTA; FONTÃO; SANTOS, 2021d)
Role	**Sustaining Developers Team**
Description	Responsible for the daily operational activities needed to manage the IT applications throughout their life-cycle. They are also internal developers.
Type	Participant
Reference	(MOELLER, 2013) (COSTA; FONTÃO; SANTOS, 2021c) (COSTA; FONTÃO; SANTOS, 2021d)
Role	**IT Service Provider Developers Team**
Description	Responsible for the development of applications that compose the technological platform of the SECO. They are external developers.
Type	Participant
Reference	(MOELLER, 2013) (COSTA; FONTÃO; SANTOS, 2021c) (COSTA; FONTÃO; SANTOS, 2021d)

Table 5.2: Artifact in incident handling process.

Artifact	**Description**
Incidents List	Describes the incidents and severities that have been assigned and accounted to the IT service provider developers team.

In this process, the activities aim to generate the basis for the incident handling and management in the proprietary SECO. For this reason, the central organization is responsible for all activities. The activities have the participation of the organization's teams (e.g., service desk, sustaining, and IT providers) and can contribute to the generation of some artifacts.

In our approach, we have included an activity Accounting in Project Backlog that will provide an artifact related to incident backlog management. Once an incident is identified as the source of recent project deployment, the organization will be able to measure how much this threat could affect the stability of the technological platform of the proprietary SECO. The artifact will also help the Backlog Incident Diagnosis Process in Section 5.3.3.2. The activities of the incident handling process are described in Table 5.3.

Table 5.3: Activities in incident handling process.

Activity	**Accounting Incident in Project Backlog**
Description	Accounting in the group of software project development team and verifying the incident severity. Severity can be reclassified into four domains: • **Low** - are those that do not interrupt users or the business and can be worked around; • **Medium** - affect a few staff and interrupt work to some degree; • **High** - affect a large number of users, interrupt business, and service delivery; • **Critical** - affect a large number of users and have financial losses and significant reputation damage. Besides, the correction may demand a huge operational work.
Input Criteria	N/A
Output Criteria	Incident assigned to a software project's developer group.
Responsible	Central organization.
Participants	Sustaining developers team.
Input Artifacts	N/A.
Output Artifacts	List of incidents with their severities.
Activity	**Requesting for Ticket**
Description	A user requests for a incident ticket.
Input Criteria	N/A.
Output Criteria	Evidence and detail data regarding the incident.
Responsible	Central organization.

Table 5.3 – continued from previous page

Participants	End-user.
Input Artifacts	N/A.
Output Artifacts	N/A.
Activity	**Identifying Incident**
Description	This activity aims to recognize and report the incident to the service desk team. Incidents come from users in whatever forms the organization allows. The service desk then decides if the issue is truly an incident or if it is another type of request.
Input Criteria	Evidence and detail data regarding the incident.
Output Criteria	The ticket is opened and identified as an incident.
Responsible	Central organization.
Participants	Service desk team.
Input Artifacts	N/A.
Output Artifacts	N/A.
Activity	**Logging Incident**
Description	This activity aims to log the incident reported in a ticket system or other tool used by the organization. The ticket should contain information such as the user's name, contact details, incident description, and other related details.
Input Criteria	The incident identification.
Output Criteria	The incident data logged.
Responsible	Central organization.
Participants	Service desk team.
Input Artifacts	N/A.
Output Artifacts	N/A.

Table 5.3 – continued from previous page

Activity	**Categorizing Incident**
Description	This activity aims to classify the incident to determine how the issue has to be handled. It allows the service desk to sort and model incidents based on their categories and subcategories. Some of the issues may be automatically prioritized. The process makes it easier for the service desk team to track and identify the incidents.
Input Criteria	The incident data logged.
Output Criteria	The incident data updated.
Responsible	Central organization.
Participants	Service desk team.
Input Artifacts	N/A.
Output Artifacts	N/A.
Activity	**Prioritizing Incident**
Description	This activity aims to prioritize the incident. An incident's priority is determined according to its impact and urgency using a priority matrix. Urgency is how quickly a resolution is required. The impact is the measure of the extent of the potential damage the incident may cause. Severity can be classified into four domains: i) **Low** - services to users and customers can be maintained. These issues do not interrupt users or the business and can be worked around; ii) **Medium** - users may be slightly affected or inconvenienced. These issues affect a few staff and interrupt work to some degree; iii) **High** - disruptions of services and/or operations. These issues affect a large number of users, interrupt business, service delivery, but limited damage; and iv) **Critical** - affect a large number of users, have financial losses, and significant reputation damage. Besides, the correction may demand a huge operational work.
Input Criteria	Data information about the urgency and the impact.
Output Criteria	The incident data updated.

Table 5.3 – continued from previous page

Responsible	Central organization.
Participants	Service desk team.
Input Artifacts	N/A.
Output Artifacts	N/A.
Activity	**Diagnosing Incident**
Description	This activity aims to analyze if the incident is valid. The sustaining triage team has skills and enough expertise to identify an invalid incident. In many cases, the tickets are opened due to a lack of knowledge of business rules by the users. In this scenario, the incident will be addressed to closure.
Input Criteria	All available data of incident.
Output Criteria	Knowledge base updated.
Responsible	Central organization.
Participants	Sustaining triage team.
Input Artifacts	N/A.
Output Artifacts	N/A.
Activity	**Analyzing Incident**
Description	This activity aims to understand the problem and comprises the entire process of searching by the sustaining developers team for a solution. The troubleshooting questions can be searched in the knowledge base. If the information is missing for a resolution, it should be requested to the user or the person in charge. In this phase, the sustaining developers team may identify if the incident is due to a recent (three months) software project deployment. Also in this phase, it is possible to request the incident escalation.
Input Criteria	All available data of incident.
Output Criteria	Knowledge base updated.
Responsible	Central organization.
Participants	Sustaining developers team.
Input Artifacts	N/A.
Output Artifacts	N/A.

Table 5.3 – continued from previous page

Activity	Escalating Incident
Description	This activity aims to delegate the incident to a higher level of specialists, in case of the first-level ones are unable to complete the diagnosis. It may happen when an incident requires advanced support. Most incidents should be resolved by the first-level support and should not make it to the escalation step.
Input Criteria	All available data of incident.
Output Criteria	Knowledge base updated.
Responsible	Central organization.
Participants	Sustaining developers team.
Input Artifacts	N/A.
Output Artifacts	N/A.
Activity	**Resolving Incident**
Description	This activity aims to resolve and reestablish the service. It happens. It happens when the user's service has been restored.
Input Criteria	Knowledge base.
Output Criteria	Knowledge base updated.
Responsible	Central organization.
Participants	Sustaining developers team, and sustaining software projects developers team.
Input Artifacts	N/A.
Output Artifacts	N/A.
Activity	**Closing Incident**
Description	This activity aims to close the incident and the process ends. Final documentation and lessons learned are stored.
Input Criteria	Knowledge base.
Output Criteria	Final documentation and lessons learned.
Responsible	Central organization.
Participants	Sustaining triage team, sustaining developers team, and sustaining software projects developers team.
Input Artifacts	N/A.
Output Artifacts	N/A.

Table 5.3 – continued from previous page

Activity	Filling out Feedback Survey
Description	This activity aims to collect end-user feedback. It is a way of evaluating the level of satisfaction with the service.
Input Criteria	N/A.
Output Criteria	Evaluation form.
Responsible	Central organization.
Participants	End-user.
Input Artifacts	N/A.
Output Artifacts	N/A.

5.3.3.2 Backlog Incident Diagnosis Process

The main goal of the backlog incident diagnosis process is to provide inputs to the IT management team about which software projects have generated incidents causing instability in the productive environment of the technological platform of the proprietary SECO. The management team is able to make decisions regarding the other actors and the governance of the technology platform architecture in the proprietary SECO.

The best way to monitor this practice is to adopt KPIs to optimize organizational management. Based on ITIL guidelines (LONG, 2012), we defined a metric to be used to measure the reliability of software projects and IT service providers. The activities will allow us to follow the goals established through a indicator. The roles of responsible and participant are described in Table 5.4.

Table 5.4: Roles in backlog incident diagnosis process.

Role	Central organization
Description	Responsible for providing goals relating to software projects delivery.
Type	Responsible
Reference	(MOELLER, 2013) (COSTA; FONTÃO; SANTOS, 2021c) (COSTA; FONTÃO; SANTOS, 2021d)
Role	**IT management team**
Description	Responsible for making decisions regarding the governance of the technology platform based on reliability dashboard.

Table 5.4 – continued from previous page

Type	Participant
Reference	(LONG, 2012) (MOELLER, 2013) (COSTA; FONTÃO; SANTOS, 2020a) (COSTA; FONTÃO; SANTOS, 2021c) (COSTA; FONTÃO; SANTOS, 2021d)

In this process, the activities aim to generate the basis for the reliability evaluation of software projects and IT service providers in the proprietary SECO. For this reason, the central organization is responsible for all activities. The activities have the participation of the organization's management and sustaining teams. The activities that are part of the backlog incident diagnosis are described in Table 5.5.

Table 5.5: Activities in backlog incident diagnosis process.

Activity	**Defining weight per severity**
Description	This activity aims to define a weight for each incident severity (scale values: low, medium, high, and critical) to be used in the reliability formula. It is a free value that allows the IT manager to calibrate this parameter, taking into account the criticality of the incident.
Input Criteria	N/A
Output Criteria	Database updated.
Responsible	Central organization
Participants	IT management team
Input Artifacts	N/A
Output Artifacts	N/A
Activity	**Defining bug-free goal**
Description	This activity aims to define a reliability goal to be used in the software projects and IT software providers evaluation. It will also be used in the reliability formula.
Input Criteria	N/A
Output Criteria	Database updated.
Responsible	Central organization
Participants	IT management team
Input Artifacts	N/A
Output Artifacts	N/A

Table 5.5 – continued from previous page

Activity	Calculating bug-free projects rate
Description	This activity aims to calculate the reliability rate for each software project and each IT service provider.
Input Criteria	Incidents list and severities.
Output Criteria	Database updated.
Responsible	Central organization
Participants	IT management team
Input Artifacts	N/A
Output Artifacts	N/A
Activity	**Reporting dashboard**
Description	This activity aims to measure the reliability rates of the software project and the IT service provider. It provides inputs to make decisions related to the governance of the technological platform.
Input Criteria	Reliability rates
Output Criteria	Diagnosis of software projects and IT software providers that failed to achieve the established goals.
Responsible	Central organization
Participants	IT management team
Input Artifacts	N/A
Output Artifacts	N/A

5.4 PSECO-IM tool

In order to support the PSECO-IM approach, a support tool was developed. This tool uses data from the ITIL ticket system platform adopted by the central organization based on the calibration of some configuration parameters. The diagnosis report aims to help IT management team in confidence level assessment from the proprietary SECO perspectives. The tool was implemented in Node.js and React JS, using Material UI graphs API for graph visualization. The prototype has 1,121 lines of code (LOC) in the backend repository and 2,890 in the frontend repository, aside from the files created by booth frameworks. In addition, five new data model tables were created, managed by the API using a PostgreSQL connection library.

5.4.1 Tool's motivation

System complexity is becoming exponentially more difficult to plan for because of the increased velocity, diversity of platforms, and interdependencies between distributed application components (ELSAYED, 2020). Even so, IT managers are beset by high expectations of offer reliability in modern and complex environments. Traditionally, new software releases bring new production defects and stability concerns (ELSAYED, 2020). This behavior leads to customer dissatisfaction. To keep up with today's frequent deployment cycle, we must mitigate downtime proactively and not solely through reduce incident backlog practices.

The study of Klutke *et al.* (KLUTKE; KIESSLER; WORTMAN, 2003) takes a position that quality and confidence level are related. Our PSECO-IM tool enhanced two formulas to calculate the confidence level in software projects and IT service providers of a proprietary SECO. The formulas below were inspired by software quality metrics (GALIN, 2004), specially in *errors density* and *errors severity* ones. One of the elements that influence the calculation is the severity level of the incident based on a four-level scale linked to a custom assigned weight (HUTCHESON, 2003).

$$\mathsf{RS} = \left[1 - \frac{\sum(\mathsf{QTYIN} \cdot W)}{\mathsf{EP}}\right] \cdot 100 \tag{5.1}$$

Where,
RS: confidence level rate of software project (limited to zero)
W: severity weight
QTYIN: incident quantity
EP: effort per software project in hours

$$\mathsf{RP} = \frac{\sum(\mathsf{RS} \cdot \mathsf{EP})}{\mathsf{ET}} \tag{5.2}$$

Where,
RP: confidence level rate of IT software provider
RS: confidence level rate of software project developed by IT software provider
EP: effort per software project in hours
ET: effort total in hours

The reasoning behind the two formulas is detailed as follows:

From the moment that we customize the incident management process (Figure 5.1) and identify how many incidents and their severity (each one has a weight set up by the manager) come from the bad results of deployments in the production environment, we can discover the software project's and service provider's confidence levels.

For each incident of a given project, we multiply it by the severity weight *(QTYIN . W)* and divide it by the effort, in hours *(EP)*, for that project. This result is a decimal value that represents the impact of incidents from a software project have had on the platform. To find the confidence level percentage, just decrease the result by 1 and multiply it by 100. The concept of weight was based on the *errors density* metrics that define the number of defects confirmed in a software application (GALIN, 2004).

Based on the confidence level of each project *(RS)*, we are able to find out the confidence level of each service provider *(RP)*. For each project from a given service provider, we simply multiply *(RS . EP)* the percentage obtained in the software project confidence level by the effort, in hours, for the same project, divided by the total effort in hours *(ET)* of all projects performed by the service provider. This result is a percentage value that represents the service provider confidence level in the platform of the proprietary SECO.

In our personal lives, the importance of monitoring physical health indicators is widespread, even if there are no symptoms of disease. Those who do not periodically assess several aspects of health run the risk of discovering something, it will be too late. In organizations, it happens the same. Organizations that monitor the main indicators can detect anomalies and make corrections, applying punctual efforts in order to not harm the organization's survival and growth. Therefore, both formulas aim to help the management team diagnose undesirable behaviors in the technology platform arising from changes in the production environment.

5.4.2 Tool's requirements

As the tool support is a prototype, it does not implement all SECO Incident Management Process requirements. The tool requirements were elaborated by the researcher together with the practitioners through discussions of the rapid review study and the participative case study, also described in Sections 2.4 and 4.1. The tool implements the following requirements (TR) considered as essential:

- **TR1** - The tool should provide the user with a descriptive summary of each process activity;

- **TR2** - The tool should provide a user interface to input incident and severity;

- **TR3** - The tool should provide an administrative module to manipulate configuration parameters;

- **TR4** - The tool should provide a dashboard to report reliability rates; and

- **TR5** - The tool should automate a custom incident management process in a proprietary SECO.

5.4.3 Tool's architecture

The tool was built using a web-based application architecture as shown in Figure 5.3. The architecture represents relationships and interactions among components as user interfaces (client), transaction processing (server), and database. The tool architecture consists of three layers: client (front-end), server (back-end), and database. The front-end layer is a visual part of the application. Users can see an interface and interact with it. The client-side code responds to the users' actions. Our client-side used an open-source JavaScript library focused on creating user interfaces on web pages called React JS. The client component is developed with HTML, CSS, and JavaScript. Web browsers run the code and convert it into the interface. There is no need for an operating system adjustment.

The back-end layer is not visible to users, yet it makes the requests work. The back-end is responsible for the proper data exchange. This layer defines the logic for business operations and rules, such as CRUD operations (create, read, update, and delete). Our back-end was built using Node.js. Node.js is a platform that interprets JavaScript code and is used to build highly scalable, real-time applications. It uses an event-driven programming model and allows anonymous functions, which facilitates development and maintenance.

Finally, the database layer is the collection of files in which data created by users of our web application is stored. These files are managed by the DBMS (Database Management System). In our case, we chose PostgreSQL. Working correctly, the client, server, and database layers make up the web application software architecture. In summary, the data generated by our tool is stored in a local database originated by the user's inputs and tool's calculations. Information provided to IT management team will be interpreted to generate insights since the goal is to support decisions (and not to make it). Once the IT management team sets up the bug-free goal and severity weights, the next time the dashboard functionality is used, the data will be updated.

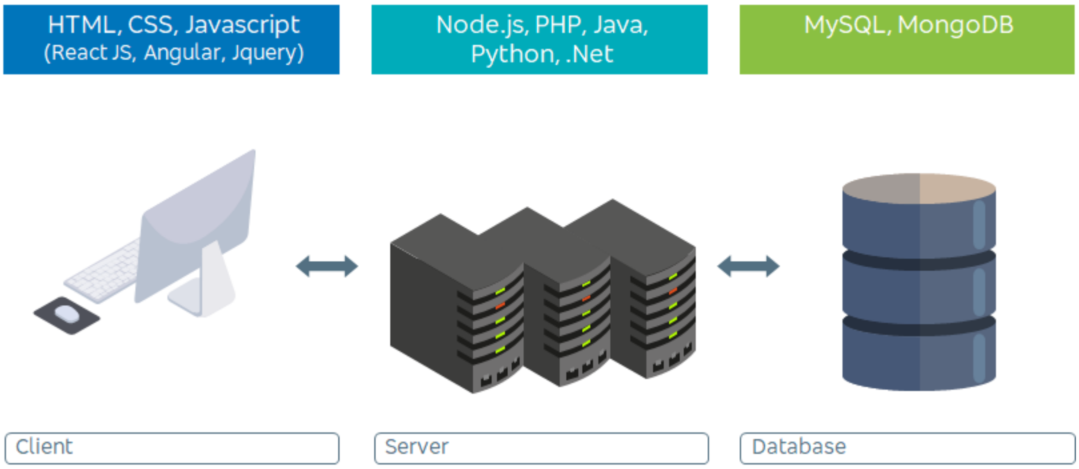
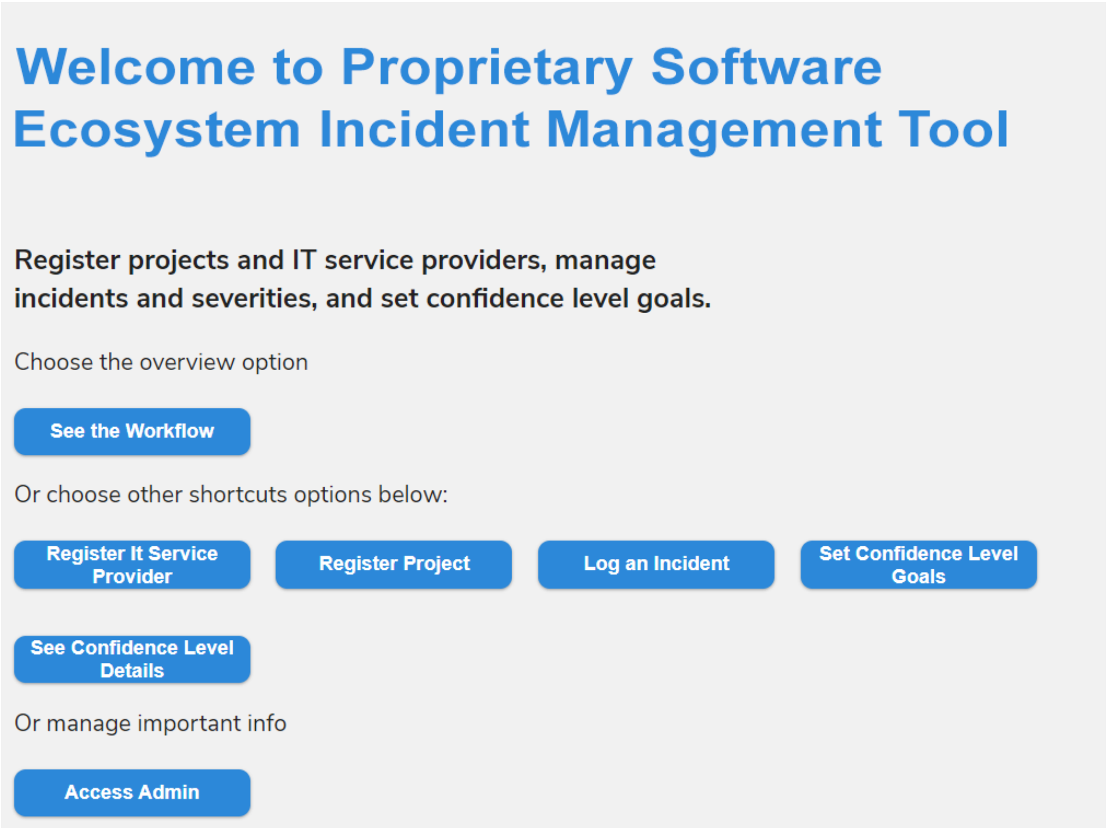


Figure 5.3: Web application architecture.

5.4.4 Support tool

The support tool offers three mains options: i) visualizing the proprietary SECO incident management process; ii) starting shortcuts for consulting the confidence level rates dashboard; and iii) accessing the administrative module. Figure 5.4 shows the tool's main screen. The tool is a web application with a graphical representation of the process, allowing the end-user to interact with activities, roles and attributes through mouse clicks.



Welcome to Proprietary Software Ecosystem Incident Management Tool

Register projects and IT service providers, manage incidents and severities, and set confidence level goals.

Choose the overview option

Or choose other shortcuts options below:

Register It Service Provider
Register Project
Log an Incident
Set Confidence Level Goals
See Confidence Level Details

Or manage important info

Figure 5.4: PSECO-IM's main screen.

After choosing the proprietary SECO incident management process workflow, all actors will be displayed according to the sequence of activities as shown in Figure 5.5. For each activity, there is a modal form screen presenting a summary of each one, as shown in Figure 5.6. It works as a help for practitioners.

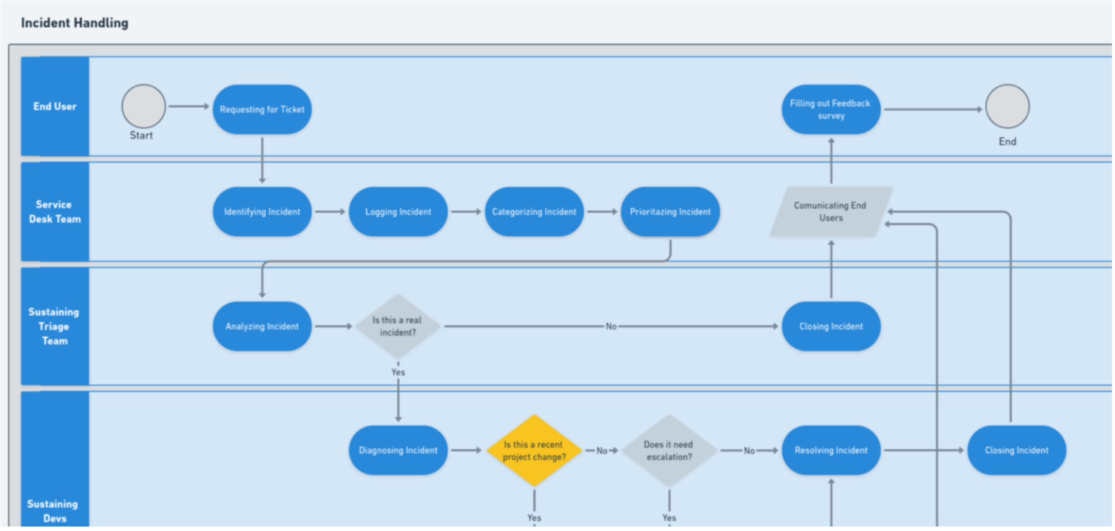
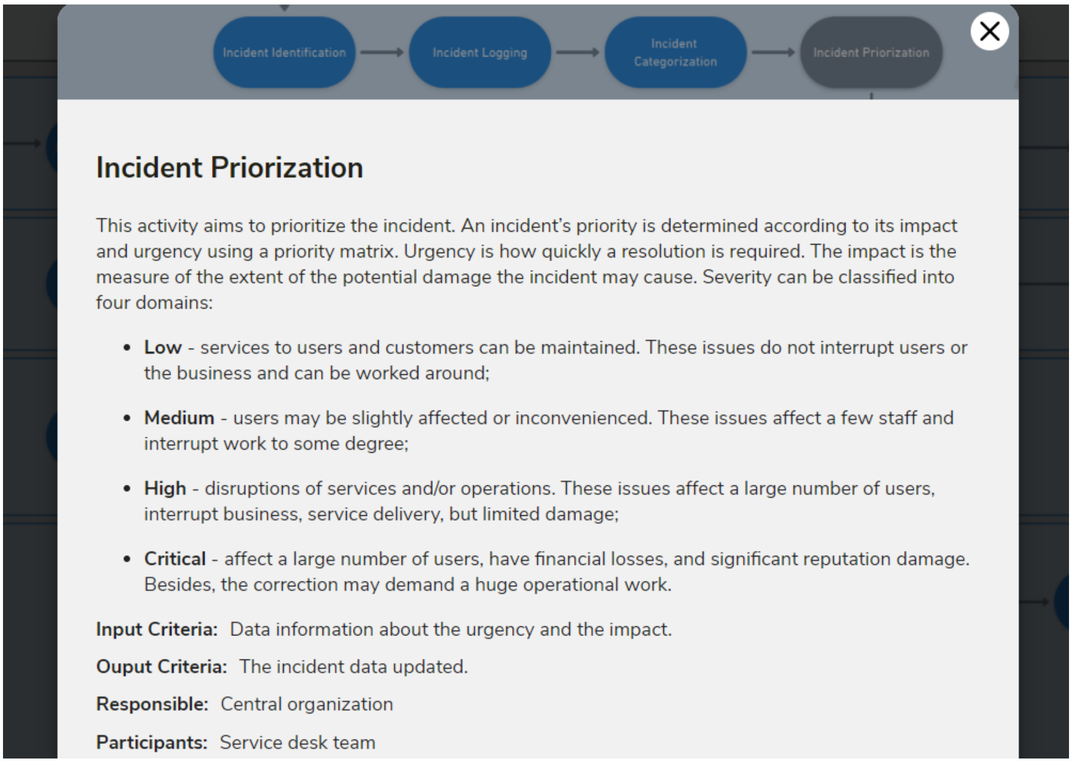


Figure 5.5: Proprietary SECO incident management process.



Incident Priorization

This activity aims to prioritize the incident. An incident's priority is determined according to its impact and urgency using a priority matrix. Urgency is how quickly a resolution is required. The impact is the measure of the extent of the potential damage the incident may cause. Severity can be classified into four domains:

- **Low** - services to users and customers can be maintained. These issues do not interrupt users or the business and can be worked around;
- **Medium** - users may be slightly affected or inconvenienced. These issues affect a few staff and interrupt work to some degree;
- **High** - disruptions of services and/or operations. These issues affect a large number of users, interrupt business, service delivery, but limited damage;
- **Critical** - affect a large number of users, have financial losses, and significant reputation damage. Besides, the correction may demand a huge operational work.

Input Criteria: Data information about the urgency and the impact.

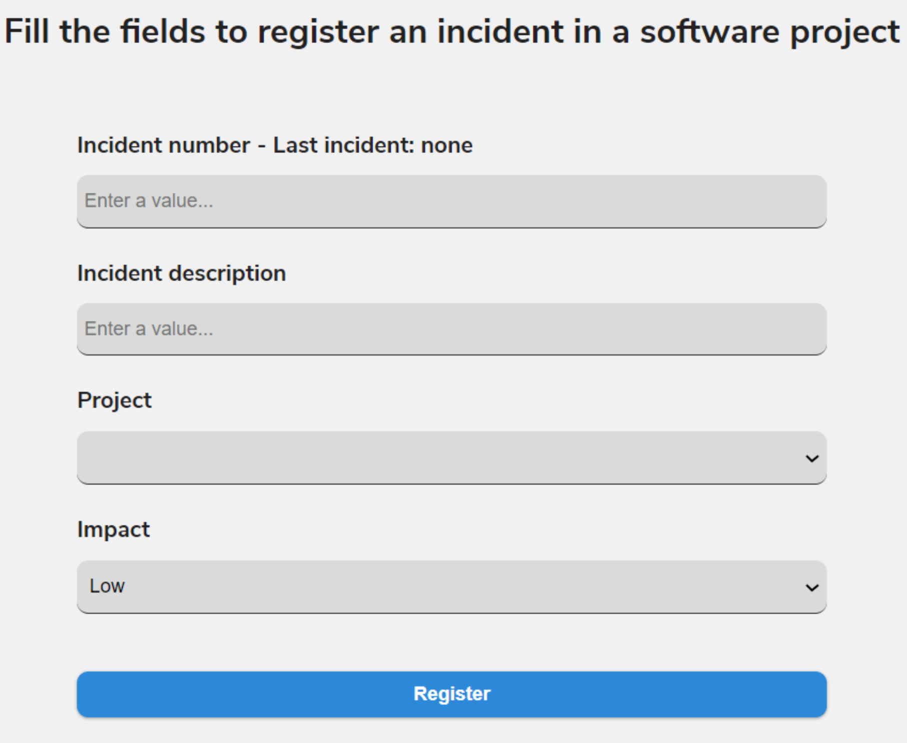
Ouput Criteria: The incident data updated.

Responsible: Central organization

Participants: Service desk team

Figure 5.6: Summary activity.

As the purpose of the *Accounting Incident in Project Backlog* activity is to manage the incidents caused by recent changes, there is a Register Incident screen to account for it in a software project, also shown in Figure 5.7.



Fill the fields to register an incident in a software project

Incident number - Last incident: none

Enter a value...

Incident description

Enter a value...

Project

Impact

Low

Figure 5.7: Assign the cause of the incident to a software project.

Once the incident, after analysis and diagnosis, is assigned to a software project, the confidence level dashboard is automatically calculated. The dashboard can be accessed through the activity *Calculating bug-free projects rate*. This activity is part of the process *Backlog Incident Diagnosis* as shown in Figure 5.8. Figure 5.9 shows the dashboard with four software project examples, where the red lines show those below the target rates and the green lines show those above. The tool is also able to calculate de IT Software Provider confidence level, as shown in Figure 5.10. The data has been anonymized, as it refers to people, software projects, and IT software providers in a real scenario that can not be identified.

Therefore, the tool is an operational prototype used by the organization to support governance in a proprietary SECO. This tool is available as an open source project for contributions from the developers' community and is also shared with the academic community on GitHub[2].

5.5 Discussion and implications

For the academic community, we noticed that confidence level is one of the important aspects of any software that cannot be ignored and hard to measure. Several approaches

[2] GitHub, Inc. is a provider of internet hosting for software development and version control using Git.

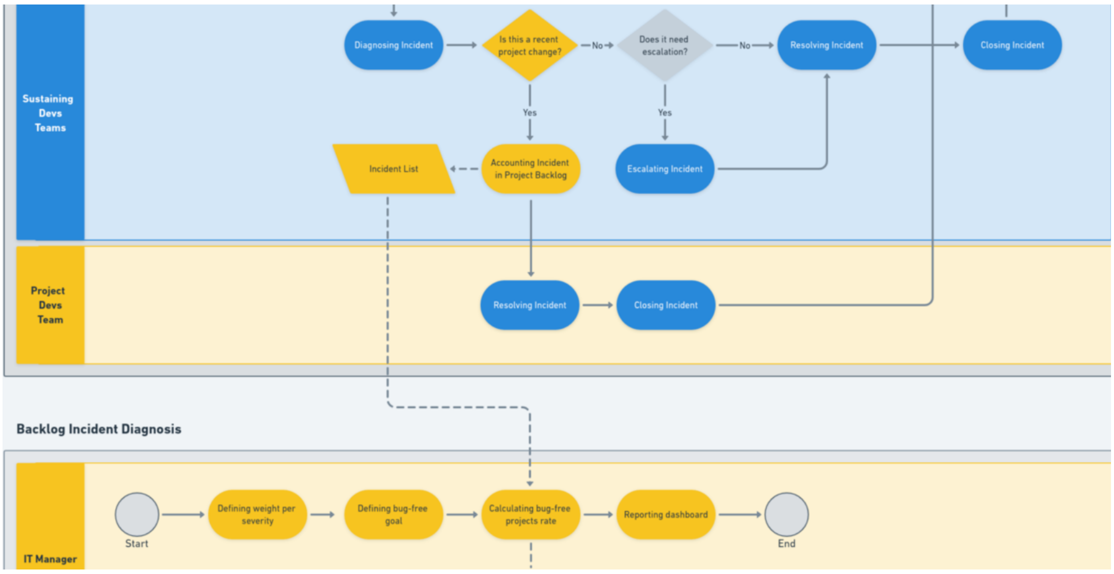
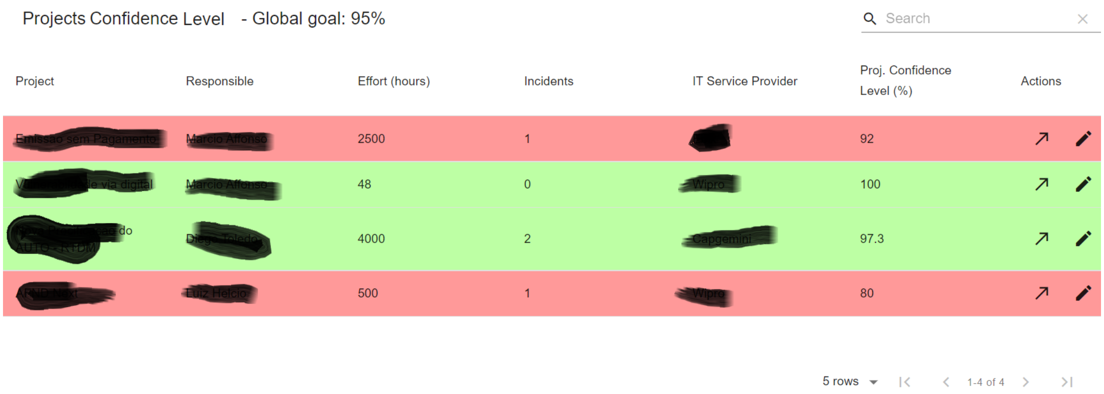


Figure 5.8: Backlog Incident Diagnosis in a proprietary SECO.



Projects Confidence Level - Global goal: 95%

Search

Project	Responsible	Effort (hours)	Incidents	IT Service Provider	Proj. Confidence Level (%)	Actions
[redacted]	[redacted]	2500	1	[redacted]	92	↗ ✎
[redacted]	[redacted]	48	0	[redacted]	100	↗ ✎
[redacted]	[redacted]	4000	2	[redacted]	97.3	↗ ✎
[redacted]	[redacted]	500	1	[redacted]	80	↗ ✎

5 rows ▾ |< < 1-4 of 4 > >|

Figure 5.9: Confidence level dashboard.

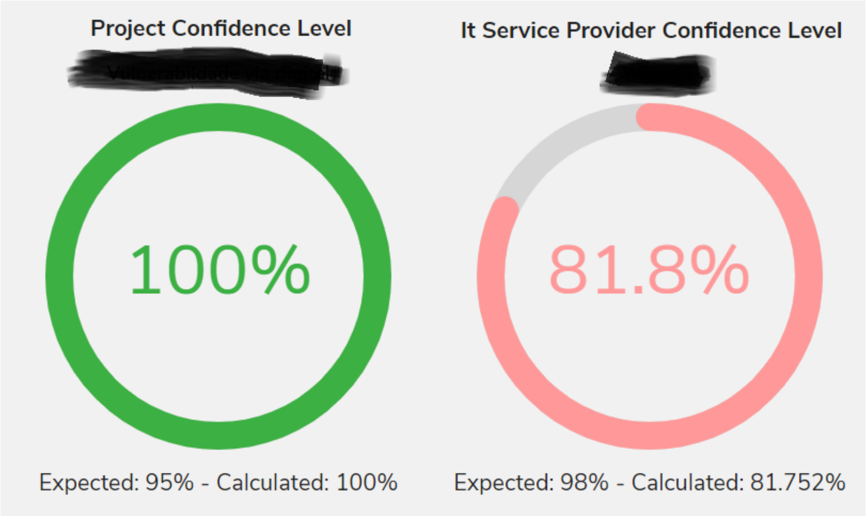

Project Confidence Level
[redacted]
100%
Expected: 95% - Calculated: 100%
It Service Provider Confidence Level
[redacted]
81.8%
Expected: 98% - Calculated: 81.752%

Figure 5.10: IT Software Provider confidence level.

can be used to improve the reliability of the software. However, it is hard to balance development time and budget with software reliability. Metrics used early in the software life cycle can aid in the detection and correction of requirement faults and the focuses on confidence level measurement techniques should prevent errors later.

For the industry community, in order to meet the market pressure for state-of-the-art solutions, the IT managers try to implement more than they can. As one of the consequences, new software releases bring new production defects and stability concerns (EL-SAYED, 2020). It is one of the reasons that organizations should invest in the confidence level measurement techniques. Software confidence level is the key task for achieving the high reliability of any software industry. Confidence level metrics are used to quantitatively express the reliability of the software product.

The definition of which metric is to be used depends upon the type of system to which it applies and the requirements of the application domain. Choosing the right confidence level metrics aiming to improve possible software errors during the design process before releasing the software to the public is not an easy task. Organizations must propose metrics with clear expectations to maximize the chances of achieving them using the **S.M.A.R.T** concept (ISHAK; FONG; SHIN, 2019):

- **Specific**: Specific metrics are clear and well-defined;
- **Measurable**: Progress toward metrics is monitored while work is underway;
- **Achievable**: Achievable metrics ensure that everything is in place to meet the metric;
- **Realistic**: Not all metrics that can be achieved are worth achieving; and
- **Timely**: Descriptions of metrics should include timelines, showing what is required, and when.

Therefore, instead of vague resolutions, as is most often the case, setting “SMART” metrics focuses on a particular target. Implementing a measurement program is not trivial and there are important drivers that need to be observed, such as: i) ensuring that there is an alignment with organizational needs (e.g., strategic objectives); and ii) defining actions based on the identified measures.

5.6 Final remarks

Initially, this chapter presented a process-based approach for incident management to be explored within the existing relationships in the proprietary SECO (PSECO-IM approach). We also developed a support tool in proprietary SECO to promote a robust management practice to enhance the governance of the technological platform (PSECO-IM tool). The governance mechanisms forms part of the keystone' strategies which aims to avoid systems outages and reduce the serious incidents that occur because of technology obsolescence and low-quality software.

Information was gathered during the incident management process to implement practices related to governance strategies in the proprietary SECO. As result, we address governance strategies to help the IT management team in the confidence level assessment from the proprietary SECO perspectives. The concerns are focused on knowledge management, software assets quality, and investment in innovative solutions. All these actions aim to obtain a competitive advantage over competitors.

As lessons learned, we discuss organizations that are very good at starting software projects, but not so good at finishing them. Moreover, we verified that the amount of pressure put on organizations to introduce software products and services faster, cheaper, and smarter comes at the price of quality.

When the output deliveries of a software project are rejected by the quality control department, the IT project manager needs to meet the quality standards requiring more time, ultimately delaying delivery. As they are evaluated by this indicator, this action is avoided. On the other hand, IT software providers cannot afford a delay in deliveries as there may be a clause in the contract with the customer regarding a penalty for delay in deliveries. As result, after the software project's deployments, we have a significant increase in the number of incidents damaging the success of the SECO technological platform.

The confidence level is the ability of a system or component to perform its required functions under stated conditions for a specified period of time. Considering the software deployments that occur at an organization's proprietary SECO, we propose a formula to calculate the confidence level rate according to the weight of the severity of each incident related to those deployments. It was possible to identify the representativeness of each problem for the technological platform.

Our proposal aims to intimidate the negligence of proprietary SECO actors, such as software providers, developers, and managers relating to the quality of IT software products. The intention is to educate them about the importance of quality. Moreover, we also made the IT organization board aware that a good strategic driver for the organization to have a competitive advantage in the market is to reduce the open incidents instead of reducing the backlog. “The cleanest street is not the one that is most swept, but the least dirty”. We must avoid that new demands affect the stability of the platform technology of a proprietary SECO, making it chaotic, damaging the image of the organization, and the satisfaction of the end-user.

One of the strategies for the survival of the SECO is to encourage the responsibility of IT suppliers, managers, and developer teams to maintain the quality of the project through collaborative relationships. Otherwise, this may result in loss of the project as a whole and consequently, loss of business and reputation. Poor quality control is a gift to competitors. Usually, the quality failings are publicized through the press or social media.

6. Evaluation

Chapter 5 defined a process-based approach (PSECO-IM) to support governance of the incident management aimed at helping the IT management team in the decision-making on the technology platform in a proprietary SECO. In order to assess the approach's main features, a focus group and a participative case study were conducted to evaluate the process and the support tool in a real industry scenario. This chapter describes the planning, execution, and results of each study.

6.1 Introduction

The keystone must also develop governance policies as an essential method for securing a long-term platform. The platform's ability to withstand natural challenges is referred to as a sustainable strategy. To achieve the main objectives, such organization relies on process and tools do reduce incidents in the technological platform.

The purpose of this study is to evaluate a process-based approach (PSECO-IM) to support governance of incident management in a proprietary SECO based on the opinions of industry experts (practitioners such as IT managers, developers, and business analysts) who are responsible for decision-making relating to governance strategies and maintaining the IT architecture in the organization's SECO.

To achieve this purpose, two studies were performed. In each study, secondary goals were defined through research sub-questions that helped to answer the main research question 6.2. The first study carried out a focus group to verify the understanding of experts on the characterization of the incident management process to support governance in the proprietary SECO. The second one was a participative case study in a large international organization in order to evaluate a process-based approach and a support tool to help the IT management team with the governance of the technology platform.

This chapter is organized as follows: Section 6.2 presents the main research question and the methodology of this evaluation study; Section 6.3 describes the focus group steps and instruments; Section 6.4 describes the participative case study procedures; Section 6.5 identifies some threats to validity; and finally, Section 6.6 concludes the chapter.

6.2 Research question

The goal is to understand the evaluation and applicability of an incident management process to support governance in a proprietary SECO of a large international insurance organization. The main research question for this part of the study is: *"What are the characteristics of a process-based approach for incident management to support governance applied in a proprietary SECO?"* To answer the research question, we ground our work on evaluations methods from Empirical Software Engineering guidelines (WOHLIN; RUNESON; HÖST, et al., 2012). The evaluation studies methodology of our work is divided in the following methods, as shown in Figure 6.1. The questions are refered as "(Qxx)" where "Q" is the opinion survey question and "xx" is the ID.

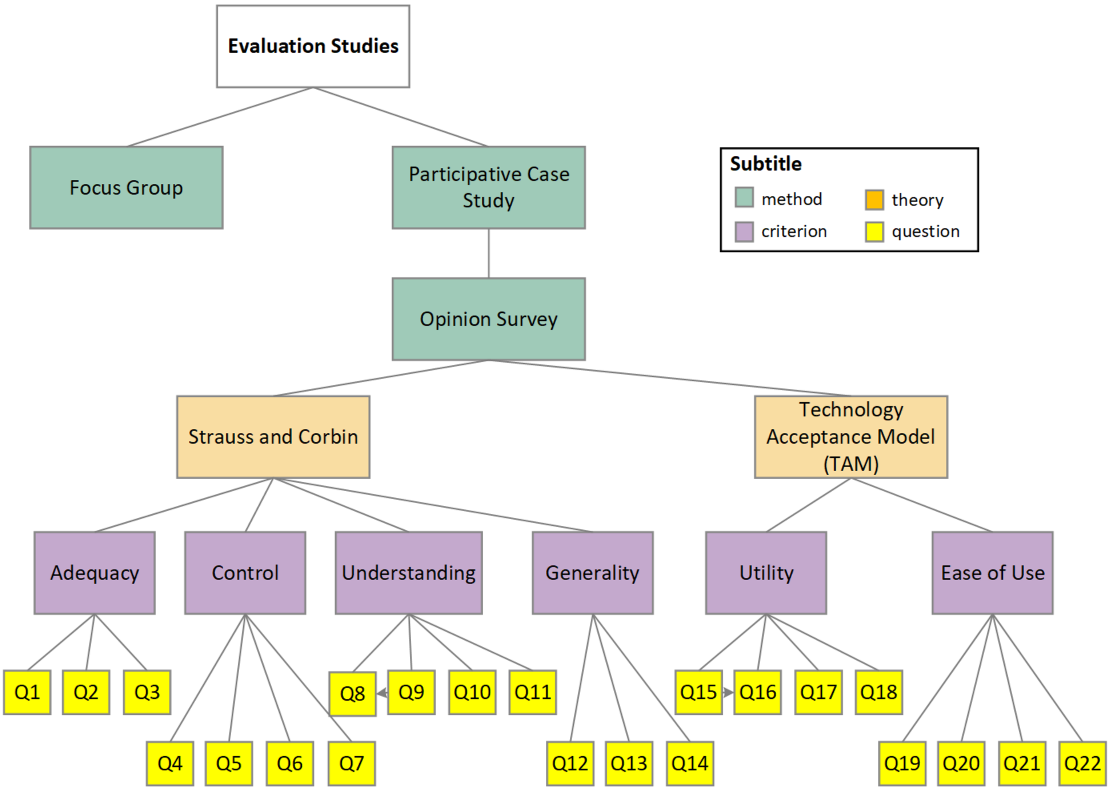


Figure 6.1: Evaluation studies methodology.

6.3 Focus group

Focus groups are qualitative research methods that use group interviews to gather information based on group communication and interaction (KITZINGER, 1995). This method orchestrates communication between research participants to generate data and it is useful for exploring the knowledge and people's experiences about a topic, in a limited period, allowing the researcher to focus on the research theme (KITZINGER, 1995).

6.3.1 Study goal

A focus group was performed to assess the effectiveness of the process-based approach for incident management to support governance in a proprietary SECO. This technique was used to verify the understanding of experts on the characterization of the incident management process in the organization, how the particularities of a proprietary SECO, the challenges of the IT management team, and other operational situations that interfere with the architecture of the technology platform are addressed.

6.3.2 Research sub-question

One research sub-question was defined to support the main research question (Section 6.2). The goal of this study is to verify the understanding of experts on the characterization of the incident management process in the proprietary SECO of a large international insurance organization. The research sub-question for this study is: *"How the particularities of an incident management process to support governance are characterized in a proprietary SECO?"*.

6.3.3 Planning

This section presents the protocol used to plan the study, describing the roles, participants, location, and script.

6.3.3.1 Roles

The roles used in this study were:

- **Moderator**

  The role is played by the researcher responsible for conducting the study and the author of the proposed process-based approach for incident management to support governance in proprietary SECO aimed at helping the decision-making of the IT management team relating to technology platform issues. The moderator will promote discussions, addressing issues related to the incident management process to support governance in proprietary SECO.

The moderator is responsible for promoting interaction between participants, enabling the emergence of new ideas, and not just producing a sequence of questions and answers (MORGAN; KRUEGER, 1998), as well as recording important interactions and conclusions arising during group discussions.

- **Participant**

  The role played by the people who will integrate the focus group with the functions of answering the questions of the moderator, participating in the group discussions, and suggesting modifications and improvements to the incident management process and the support tool in the proprietary SECO.

6.3.3.2 Participants

We invited two senior practitioner experts from the software industry with skills in governance and the ITIL framework, and a renowned Ph.D. professor with extensive experience and a specialist in SECO governance with several internationally published studies. The chosen practitioners are senior developers who work in the organization's sustaining team with extensive knowledge of Incident Management, a process that appears in the Service Operation volume of the ITIL framework.

According to Shull *et al.* (SHULL; SINGER; SJØBERG, 2007), the size of a focus group may range from 3 to 12 participants. Participants will not be explicitly identified in the logbook about responses and discussions during the group dynamic for reasons of confidentiality and anonymity.

6.3.3.3 Location

The focus group was carried out using the Google Meet[1] tool in order to make the schedule more flexible for participants and respect health protocols due to the COVID-19 pandemic.

6.3.3.4 Script

According to Williamson (WILLIAMSON, 2002), several questions were elaborated to guide the discussions during the focus group. The researcher who conducted the study

[1] Video communication tool developed by Google

was concerned with leveling the practitioners' knowledge about the concepts addressed during the focus group. For this, the researcher gave a lecture and provided material produced during the study containing a summary of the concepts of SECO, descriptions of the activities and actors of the incident management process in proprietary SECO, and the modeling of the process. The invitation was made by email with the attachments of the Informed Consent Form (presented in Appendix C) and the questions to be answered at the end of the meeting. The meeting was conducted following the script:

1. Presentation of practitioners and professor;
2. Clarification about the context of the study;
3. Study goal;
4. Reading the incident management process;
5. Analysis of the usefulness of the approach to address issues related to incident management in proprietary SECO; and
6. Discussion related to research questions.

At the end of the group focal meeting, the participants were invited to answer five questions, as following:

- Q1 - Was the description of activities defined correctly?
- Q2 - Is the sequence of activities consistent with ITIL library?
- Q3 - Are all roles defined as participants by these activities?
- Q4 - Are these activities present during incident management in proprietary SECO?
- Q5 - Do you consider customizing the incident management process in the context of proprietary SECO relevant to the organization's IT management team?

We leave the participants free to make suggestions for each question. The suggestions would be classified as: i) SA (Strongly Accepted) - the suggestion was fully applied to the evolution of the process; ii) PA (Partially Accepted) - parts of the suggestion were applied; and iii) NA (Not Accepted) - the suggestion had no connection with the objective of the process.

6.3.4 Execution

Although the SECO acronym is little used in the daily routine of practitioners in the software industry, the material and the model presented were sufficient for understanding the approach, as well as the situations that affect incident management. The researcher reinforced the participant's understanding of the work proposal. On July 2, 2021, from 09:00 a.m. until 11:00 a.m. GMT -3, the meeting was held. The focus group study participants had different profiles according to technical experience, business knowledge, and leadership skills. Table 6.1 summarized the roles and profiles.

Table 6.1: Profile of focus group study participants.

ID	Profile	Skills
P1	Software industry practitioner	Certified ITIL Practitioner and Certified COBIT Foundation
P2	Software industry practitioner	Certified Business Process Management
P3	Ph.D. professor	Over 20 years of experience in Software Engineering, working mainly in the following areas: Software Ecosystems, Requirements Engineering, and Business Process Management

In the SECO concepts for the industry scenario, one of the experts (P1) mentioned the importance of contracts and the establishment of collaboration with external business partners for systemic integration in the technology platform, such as automotive assistance partnerships (spare cars, trailers, and car repair shop). Through this type of integration, value is created for products and services, generating satisfaction for the end-user.

It was also commented (P2) that the web applications that support the organization's business initiatives have a mixed set of technologies and identifying a breakpoint becomes a difficulty. It is noteworthy that the technologies used in the development of these applications are imposed by the organization's IT Architecture and Software Quality areas.

A practitioner (P2) commented that the absence of monitoring mechanisms makes it difficult to deal with incidents and often harms the SLA. The professor (P3) asked if the tool would be manual or if the tool would have automatic management based on some business rules that have already been set up. According to the researcher's positive response, there was a debate about the support that the IT management team would have to monitor the technological platform of this proprietary SECO based on the input information in the tool.

There was a debate about how the tool could support technology platform governance of this proprietary SECO and help the IT management team make decisions based on input information from the tool. As the researcher read the process, in relation to the activity *Requesting for ticket*, one of the participants (P1) highlighted the importance of guiding the business areas to open incidents with the greatest possible detail of evidence, avoiding the absence of information for investigating the problem undermines the SLA.

Another participant (P2) mentioned the importance of the "Prioritizing incident" activity. Due to a large number of applications and the lack of knowledge of the ServiceDesk team, there is no clarity on the impact of that incident on the technology platform. As an example, some batch routines that run during the night were mentioned, and that some of them generate impact on the business in the case of abend[2]. However, the Service Desk team increased the criticality of the incident unnecessarily.

The moment of interest happened during the description of the activity *Accounting incident in project backlog*. One of the participants (P1) commented on the great expectations of this activity, mentioning that it was already an old desire of the sustaining team to identify which implementations of recent changes caused incidents and imbalances in the platform. The same participant said that this is an innovative proposal and that at the moment there is nothing similar in the organization and stated that the operationalization of this metric would be an important indicator for the evaluation of the actors involved in the ecosystem, such as developers and IT service providers.

Another participant (P2) added that it is necessary to evolve the maturity of the process to assign responsibilities and penalties for deployments in the production environment. There is a demand for the sustaining team to reduce the number of incidents. However, what is noticeable is that the number of incidents is increasing every day. Therefore, it is important to have some tools that can correlate incident occurrences with recent changes.

When the researcher demonstrated the result of the *Calculating bug-free projects rate* activity, the participants were excited. One of the participants (P2) mentioned the possibility of this tool also supporting the retrospective meetings held at the end of the sprint in which the entire Scrum team participates. It would be a way to improve communication, efficiency, and the quality of teamwork.

Finally, the professor (P3) commented on the importance of aligning business rules, from the point of view of platform governance. Guidance with partner teams is required before the incident occurs. One participant (P1) added to this comment by citing the example of an incident that depends on more than one IT service provider to be resolved.

[2] An abnormal end or abend is an abnormal termination of software, or a program crash

6.3.5 Results and discussion

We have identified two suggestions related to the questions. The rest of the speech was based on statements and comments that exemplified the scenario experienced in practice by the experts, as described in this section. According to our criteria, both suggestions were strongly accepted.

Relating to Q1, all participants agreed that the activities were defined correctly and were very objective. One of the participants commented that each of these activities is part of a system focused on generating results. The professor suggested that the name of activities modeled in each process started as a verb according to BPMN (Business Process Model and Notation) best practices.

Regarding Q2, the participants contributed by stating that the sequencing of activities is correct, including one of the experts who noted that if processes are disordered, work practices can be unsound, with everyone doing their own. When processes are organized, actions, responsibilities, and operational procedures become optimized (SMINIA, 2009).

Considering Q3, experts agreed that the actors are correct based on the scope of an incident's lifecycle. Actors are responsible for carrying out the tasks to demonstrate how the organization works. Previously, the business was seen vertically, that is, separated by features, areas, or departments, each with its activities and objectives. Currently, the business vision has become horizontal, with a process approach, where activities can be performed by various actors seeking to achieve organizational goals (MOELLER, 2013).

About Q4, there was a debate regarding the need for the organization to map a new actor for the process: IT software provider. Experts commented the suggestion and concluded that there was no such need, as the actor was already part of the sustaining team, and there was no need to share them. It was the organization's strategy to increase the team's productive capacity and improve the incident response SLA. It is noteworthy that these IT software providers work under confidentiality agreements (also known as NDA - Non Disclosure Agreement) to protect the company concerning information security, avoiding disclosure of business knowledge.

Finally, regarding Q5, all participants agreed positively and considered the contribution very relevant. The opportunities are huge, such as mitigating the opening of incidents, new metrics and new indicators to measure the health of the proprietary SECO, and the possibility of discovering patterns in software projects that could represent a greater chance of opening incidents.

The transparency that the tool will provide will enable decision-making related to accountability and possible penalties for the low quality of delivery of software projects. The tool is able to support the IT management team in identifying the software projects that caused the most incidents on the technological platform and unbalanced the ecosystem. The dashboard assembled by the tool is for eliciting positive reactions or drumming up interest from senior leadership.

This focus group study allowed us to make minor adjustments to the incident management process and tool, both used to support technology platform governance in a proprietary SECO. From this input, we realized the need to evaluate all the artifacts in a scenario within an organization through a participatory case study, as described in Section 6.4. As an example, we updated the names of the activities in each process according to BPMN guidelines and in the visual interface of the tool. We strong accepted the professor's suggestion.

6.4 Participative case study

Case study is an adequate research method for situations in which it is difficult to establish a clear link between the studied phenomenon and its context. This method is also indicated when it is not possible to investigate the phenomenon outside of the practical environment (YIN, 2005).

6.4.1 Study goal

Participative case study was selected as research method in this study in order to evaluate the PSECO-IM: i) a process-based approach for incident management to support governance in a proprietary SECO; and ii) the support tool to help the IT management team in the governance of a technology platform architecture. There is no relationship with the case study presented in Chapter 4. Just like in Chapter 4, the main researcher acts in a large international organization *(the name was omitted for privacy reasons)* which owns a proprietary SECO, being a participant in the observed process (BASKERVILLE, 1997). The researcher may have control over the intervention on some variables during the study, such as teaching how to operate the support tool. The process as a whole was accompanied by the other two researchers who were supervising the participative case study in order to clarify and direct some procedures.

6.4.2 Research sub-question

The goal of the sub-question in this study is to understand the particularities of incident management in a proprietary SECO of a large international insurance organization. The research sub-question aim to provide further support for the main research question (Section 6.2) is: *"How is a process-based approach for incident management to support governance implemented in a proprietary SECO?"*.

6.4.3 Planning

This study aimed at evaluating an approach for the proprietary SECO incident management process and a tool to support the IT management team in the governance decisions relating to the technology platform architecture. The participants belonged to the sustaining team and were composed of business analysts, internal and external developers, and IT managers, totaling 20 people. All participants received training on the tool and did a hands-on exercise in practice, prior to daily use. A script was also made available in case of further doubts.

The methods for data collection were: i) observation to analyze the participant's behavior in the face of everyday situations; ii) virtual meetings to gather information on the adoption of incident management process in everyday incidents; and iii) opinion survey with the participants to collect feedback.

6.4.4 Execution and data collection

The researcher conducted a 60-minutes lecture with the entire sustaining team talking about the main reasons of this study: gathering information about the incident management in a the proprietary SECO and the governance strategies for handling and reducing incidents in the organization's technology platform.

Subsequently, the researcher reinforced the team's understanding of the work proposal. From July 5, 2021, until July 25, 2021, during the observation period of the study (20 days), the researcher encouraged the use of a process-based approach for incident management in everyday situations of the proprietary SECO. We promoted the understanding of the recent incidents investigated, enabling the emergence of new governance decision-making relating to technology platform architecture performed by the IT management team.

Participants were instructed to feel free to ask questions to the main researcher. Comments and suggestions were noted in a logbook during this period. The participants were invited to virtual meetings, moderated by the main researcher, using the Microsoft Teams[3] tool to discuss doubts as soon as they emerged. The virtual meetings were conducted with the sustaining team and IT managers aimed at clarifying any participants' doubts and verifying if there had been some difficulty in understanding the process or using the tool. The researcher took notes of all interventions, orientations, and directions in the logbook.

6.4.5 Results and discussion

During the 20-days observation period, the participants were very interested in the execution of the incident management process and, consequently, in the use of the support tool. Table 6.2 shows the logbook.

Table 6.2: Participative case study logbook, where S - Suggestion, C - Comment, and D - Doubt.

ID	Role	Description	Type
#1	Internal Developer	Will we have to re-register the incident in the support tool?	D
#2	External Developer	Integrating the support tool with the corporate ticket tool	S
#3	Internal Developer	How are the types of severity classified?	D
#4	Internal Developer	Creating a severity reclassification activity in the incident management process and a new functionality in the the support tool	S
#5	IT manager	Great opportunity to show IT executives board where the focus should be on reducing the incident backlog	C
#6	IT manager	Opportunity to show that the governance area does not have quality metrics	C
#7	IT manager	Opportunity to show that the software project teams have productive capacity above the limit	C
#8	IT manager	Creation of a confidence level indicator for the other companies in the Holding	S
#9	IT manager	Concerns about confidence level numbers without analyzing root causes	C

Despite having been observed by different profiles, ID #1 and ID #2 show the concern of developers with the time that will be spent to re-register the incident in the support

[3] Microsoft Teams is a collaboration app that helps your team stay organized and have conversations—all in one place. https://www.microsoft.com/pt-br/microsoft-teams/download-app

tool. The approach to improve software reuse in global software development industry considering relations among companies and stakeholders (SANTOS et al., 2012) may also be considered in a proprietary SECO. The idea of reuse is to avoid rework so that previously developed solutions are used in new contexts. The developers who work on the sustaining team are very charged with resolving incidents within the pre-defined SLA.

There were two notes (ID #3 and ID #4) regarding *severity*. The severity factor has a strong weight in the calculation of the confidence level. As noted in software quality metrics (HUTCHESON, 2003), the defect severity level indicates the impact on the business for the end-user. Critical severity defects signal a low-quality product. Therefore, the developer suggested that it be allowed to reclassify the severity in the case of an error in the analysis of the sustaining team who investigated the incident.

Remark ID #5 evidences us in practice one of the results obtained in our rapid review study (Chapter 2, Section2.4.3): to reduce the incident backlog, strategic governance actions must be addressed to the opening moment and not the closing one. According to Warren Buffett (HAGSTROM, 2013), one of the most powerful businessmen in the world: *"We take 20 years to build a reputation and five minutes to destroy it."*. Remark ID #6 emphasizes that the lack of quality software can cause downfall to businesses. Poor software development (e.g., slowness, crashes to functionality, and improper application) limits organization growth and impacts the image in the market (GALIN, 2004).

The comment ID #7 addresses the workforce capacity issues. Traditionally, organizations assume that busier people produce more. Making resources as busy as possible without regard to workflow, lowers productivity and comes with hidden costs, such as low-quality software projects that cause incidents. Several software project teams become exhausted and burned out trying to meet delivery expectations. The result is a sense that the demands of work are unrealistic and cannot be met (BARTHELEMY, 2001).

The remark ID #8 proposes the expansion of this approach to other companies belonging to the Holding group aiming to compare the confidence level among the various proprietary SECO. On the other hand, the comment ID #9 is based on the idea that effective management requires more than "putting out fires" for problems that emerge, but finding a way to prevent them.

In the proprietary SECO of the organization studied, we verified that the success of the technological platform requires both IT service provider developers and sustaining developers teams to be aligned with the same business outcomes. When IT service providers begin to release software iteratively as frequent product increments, some actions may occur: i) the software grows in size and complexity; and ii) while the increments are smaller than traditional releases, the changes may impact other non-related applications.

In the traditional releases of corporate systems, the software project delivery date is very important and IT managers avoid sacrificing predetermined deadlines, as they are evaluated by this indicator. When there are only a few days left to the agreed deadline, the pressure to complete the project increases. Then, consciously, some wrong decisions are made by the IT software providers in agreement with the IT managers, such as: i) integration and user acceptance tests are performed in parallel; ii) skip more complex tests, especially the integration tests; and iii) bugs are fixed directly in production.

As a consequence, immediately after the software project's deployment, we have a significant increase in the number of incidents causing an unbalance in the technological platform of the proprietary SECO. According to Kaur and Bahl (KAUR; BAHL, 2014), there is a perception that to be agile the organizations will have to sacrifice quality and in many cases, this may be true. As shown in Figure 6.2, in the useful-life phase, software will experience a drastic increase in failure rate each time an upgrade is made. The failure rate levels off gradually, partly because of the defects found and fixed after the upgrades.

Therefore, the IT board instead of defining reducing the incident backlog as one of the main strategic drivers, should pursue the concept of continuous quality. Continuous quality expands the idea of quality assurance to a set of routine activities which span prevention, detection, and recoverability of functional and nonfunctional defects (LEWIS, 2017). A continuous quality strategy in the studied proprietary SECO, fosters a company-wide cultural change to achieve the goal of making "quality" the responsibility of all.

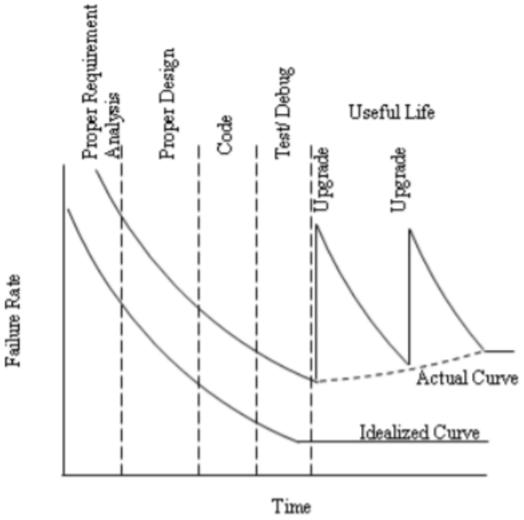


Figure 6.2: Software confidence level curve (KAUR; BAHL, 2014).

6.4.6 Opinion survey

The objective of this method is to obtain quantitative information about a certain group of people in order to identify whether or not such opinions are in accordance with reality (PRICE; HANDLEY, et al., 2010). In our study, we monitored the process based on incident management in a proprietary SECO and the use of the support tool to help the IT management team develop new strategies relating to the governance mechanisms of the technological platform.

6.4.6.1 Planning

The objectives of this study based on the GQM (Goal Question Metric) approach (BASILI, 1994) are: i) analyzing the incident management process to support governance of a proprietary SECO to assess the adequacy, control, understanding, and generality based on Strauss and Corbin (STRAUSS; CORBIN, 1998) criteria for the governance of the technology platform from the point of view of the sustaining team and IT managers; and ii) evaluating the support tool from the perspectives of its utility and ease-of-use based on the TAM (Technology Acceptance Model) (DAVIS, 1993). The complete questionnaire is presented in Appendix F.

6.4.6.2 Research sub-questions for the process

The purpose of the research sub-questions is to gather data in order to answer the main question (Section 6.2). For each criterion defined by Strauss and Corbin (STRAUSS; CORBIN, 1998), the sub-questions (SQ) and metrics associated with them are presented. Metrics are collected from participants responses. The answers contain the perceptions of the sustaining team's professionals and IT managers.

- SQ1 - Adequacy: What is the compliance level of the incident management process to support governance in a proprietary SECO?

  Metrics: Percentage of agreement and disagreement, at a partial or total level, for the adequacy of focus area, activities, and roles.

- SQ2 - Control: Does the process serve as a guide for the sustaining team's professionals and IT managers to monitor and intervene during incident management in a proprietary SECO?

  Metrics: Percentage of agreement and disagreement, at a partial or total level, with the perception of improvement in performance, productivity, and effectiveness of the sustaining team's professionals.

- SQ3 - Understanding: Can the sustaining team's professionals and IT managers use the process to handle incident management to support governance in a proprietary SECO?

  Metrics: Percentage of agreement and disagreement, at a partial or total level, for usefulness, clarity, and comprehension of the process, including the daily routines experienced by professionals.

- SQ4 - Generality: Does the process serve as a guide for sustaining team's professionals and IT managers to support governance in other proprietary SECO without losing its relevance?

  Metrics: Percentage of agreement and disagreement, at a partial or total level, with the relevance of the model for: (i) other proprietary SECO; (ii) governance strategies; and (iii) IT management team.

6.4.6.3 Research sub-question for the support tool

We evaluate the TAM fundamentals in two perceptions (DAVIS, 1993): (i) perceived utility; and (ii) perceived ease-of-use. This model gives an idea of how users will accept a new tool as well as perceptions of its use. Therefore, using the prototype in a real scenario gave the approach an indication of how it would be accepted.

As a way to support the main research question (Section 6.2), one research sub-question was defined for this part of the study: *"Are participants able to realize the impact of the incident management process to support governance in the proprietary SECO during IT management activities for technological platform maintenance?"*. It represents whether sustaining team professionals and IT managers are able to perceive opportunities in the support tool to develop new strategies relating to the governance mechanisms of the technological platform.

The survey consists of an electronic questionnaire to be filled in 10-15 minutes. It was sent to the participants' e-mails; in this case, experts of the sustaining team (business analysts, internal and external developers, and IT manager) of a large international insurance organization in the context of its proprietary SECO.

The survey was divided into 5 sessions. In the first session, an introductory text was presented bringing the objectives of the questionnaire for academic purposes. In the second one, the participant should read and agree/disagree with the Informed Consent Form (presented in Appendix C) before having access to the questions.

The third session aimed to characterize the professional profile of the participants.

We asked the participants' education degree (Bachelor, Specialization, Master, Ph.D.); the time of experience with software development (Less than 1 year, From 1 to 3 years, From 4 to 7 years, From 7 to 10 years, More than 10 years); the participants' role in the sustaining team (business analysts, internal developer, external developer, IT manager); the participants' experience with incident management process (ordinal scale from 1 to 5); and the participants' experience in SECO (ordinal scale from 1 to 5). The ordinal scale domain is defined as following: 1 - Beginner: has no knowledge in this area; 2 - Pre-intermediate: needs support in this area of knowledge; 3 - Intermediate: evidences a certain autonomy in this area of knowledge; 4 - Post-intermediate: has evidence of knowledge above expectations in this area; and 5 - Advanced: recognized as a reference in this area of knowledge.

The fourth session contained 14 questions related to the incident management process according to Strauss and Corbin (STRAUSS; CORBIN, 1998) criteria using 5-point Likert scale: Strongly Disagree (SD), Partially Disagree (PD), Neutral (N), Partially Agree (PA), and Strongly Agree (SA).

Finally, the fifth session contained 8 questions related to the support tool according to TAM fundamentals (DAVIS, 1993) also using 5-point Likert scale. There were also two open questions where the participants could write about positive/negative aspects of using the tool and suggestions/comments on the topics covered in the research.

For the evaluation and refinement of the instruments of this opinion survey, a pilot study was carried out with two participants. Finally, it was sent to the potential participants. The questionnaire is available at: `https://forms.gle/b2cp7QtV7dFQsptq6`.

6.4.6.4 Execution

The survey was sent by email to 20 participants of the organization's sustaining team affected by incident management process in the proprietary SECO. All guests participated in the participative case study described in Section 6.4. 15 responses were submitted. The response rate (75%) corresponds to the audience of the organization.

6.4.6.5 Results and discussion

In the characterization phase of the participants, it was possible to identify some relevant aspects. Respondents mostly have a Bachelor's degree with a 53% (8 respondents), 40% Specializations's degree (6 respondents), and 7% (1 respondent). Regarding the participant's role in the sustaining team, the majority corresponding to 40% are internal developers (6 respondents of organization). 26,7% are external developers (4 respondents of IT service provider), 20% are IT managers (3 respondents), and 13,3% are business analysts (2 respondents). Another relevant factor is that the majority of the participants have been working in software development from 7 to 10 years, corresponding to 40% (6 respondents).

Considering the participant's experience in the incident management process, 66,7% (10 respondents) shows experts skills in this area of knowledge, as shown in Figure 6.3. Relating to participant's experience in SECO, 60% (9 respondents) checked as an intermediate level, as shown in Figure 6.4. This information is justified by the fact that SECO concepts are still new to software industry professionals.

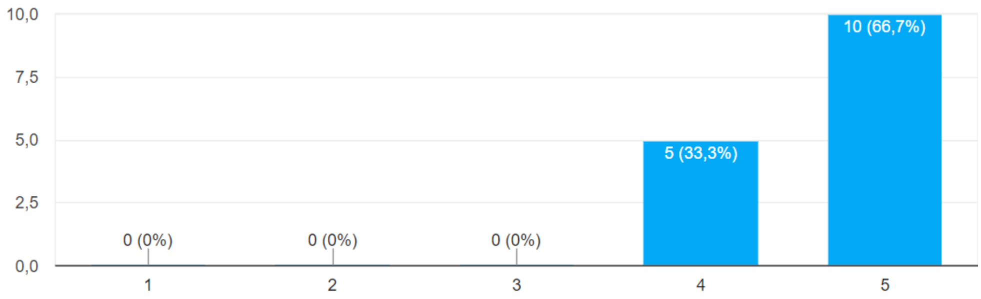


Figure 6.3: Experience in the incident management process.

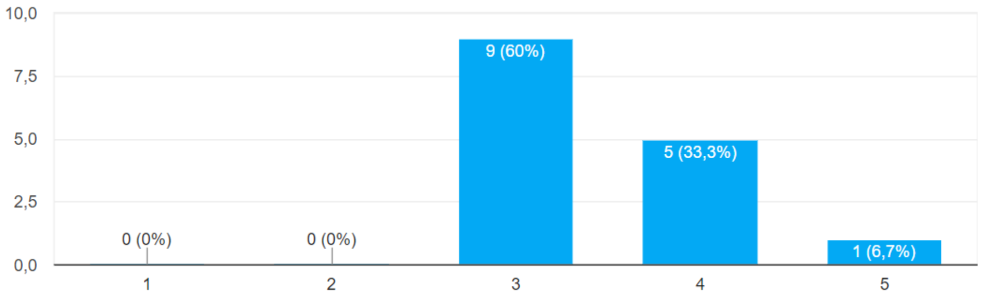


Figure 6.4: Experience in SECO concepts.

Figures 6.5, 6.6, 6.7, and 6.8 show the percentages in levels of agreement, neutrality or disagreement for each of the criteria (adequacy, control, understanding and generality) evaluated in a quantitative way. In relation to **adequacy** aspect, we evaluate the compliance level of the incident management process in a proprietary SECO. All participants partially or strongly agreed that the activities, roles and focus area are suitable for the proprietary SECO incident management process.

When the aspect analyzed is **control**, all participants partially or strongly agreed that the incident management process can improve the performance or make the activities of the sustaining team's professionals easier. There was a neutral level of effectiveness (20%) and productivity (33%) of the sustaining team's professionals. As a possible reason for the neutrality percentages, we considered the comments of participant (P3): *"... If this tool*

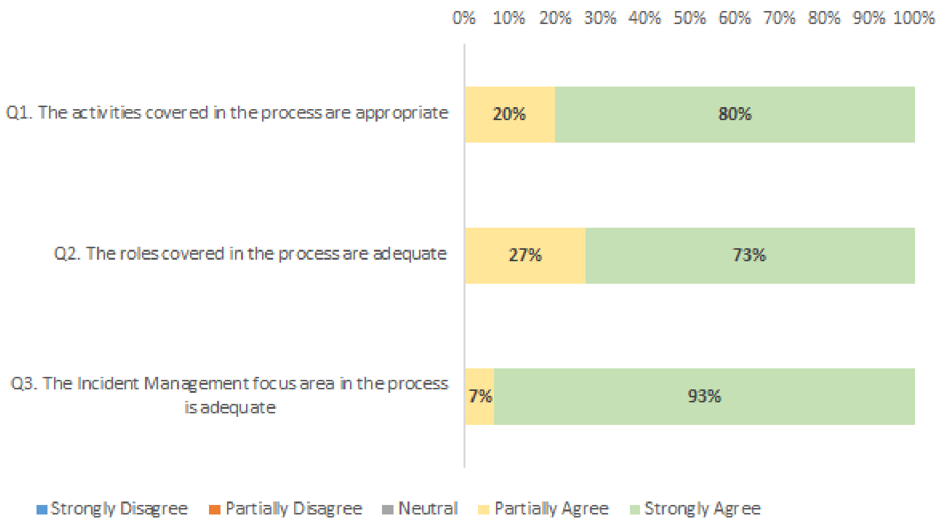


Figure 6.5: Adequacy aspect of incident management process in the proprietary SECO.

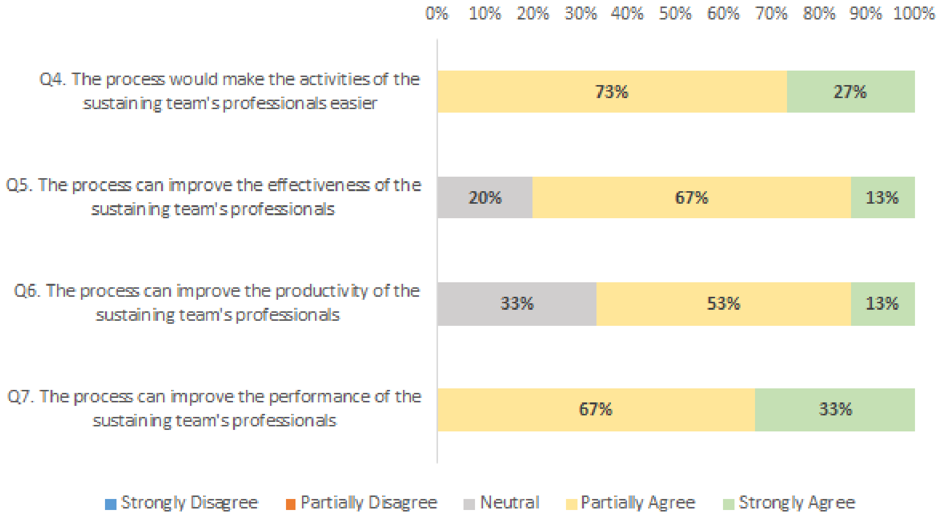


Figure 6.6: Control aspect of incident management process in the proprietary SECO.

was integrated with the corporate ticket management system, we would avoid retyping some information".

In relation to **understanding** aspect, we collect how much sustaining and management team professionals can use the proprietary SECO incident management process to support the governance of the technology platform. We highlighted that 100% of participants strongly agreed that the process is useful for the management team. In addition, all participants partially or strongly agreed that the process is clear and portrays reality.

Considering the **generality** aspect, we highlighted that 100% of participants strongly agreed that the process is relevant to support IT management team in the governance of the architecture of the technology platform. We noted 100% of participants partially

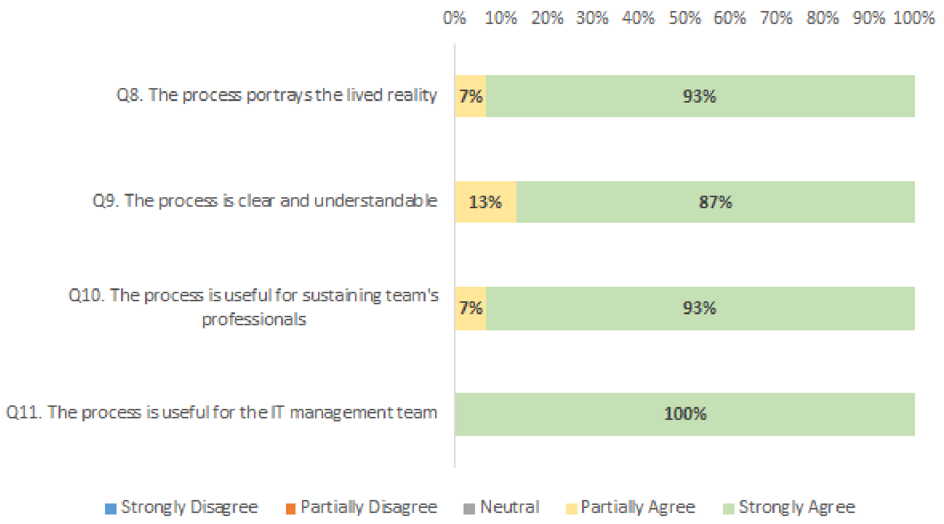


Figure 6.7: Understanding aspect of incident management process in the proprietary SECO.

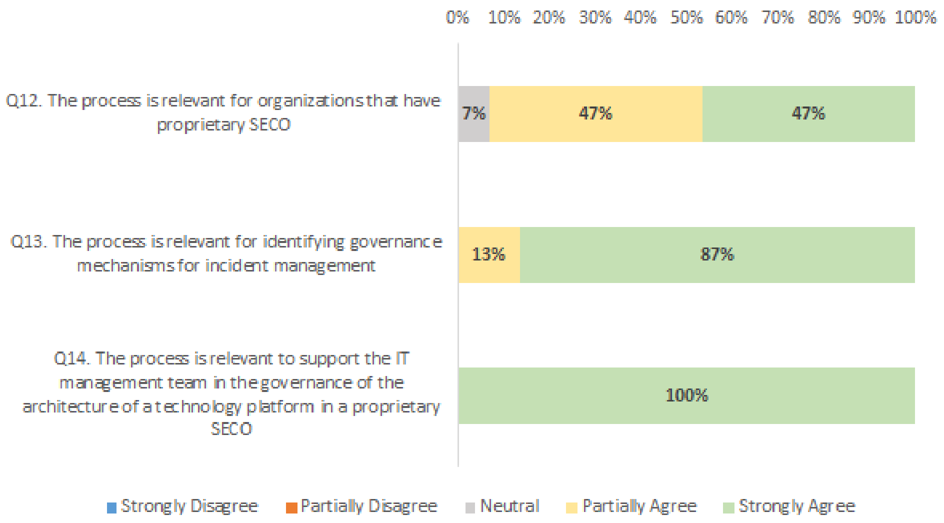


Figure 6.8: Generality aspect of incident management process in the proprietary SECO.

or strongly agreed that the process is relevant to identify governance mechanisms for incident management. There was a neutral level corresponding to 7% as mentioned by participant (P6): *"... each organization has particularities and different cultures"*.

Considering the research sub-question goal (Section 6.4.6.3), the metrics results are presented in Figures 6.9 and 6.10 relating to TAM fundamentals in two perceptions: perceived utility and perceived ease-of-use (DAVIS, 1993). Regarding the tool's **ease of use**, we noticed 100% of participants strongly agreed that the tool was easy, the tasks were performed easily and there was an understanding of what was happening. We also noticed that 40% corresponding to 6 participants partially agreed that they used the tool as they would like to use. It is noteworthy that during the development of this support tool, we did not have the participation of a UX expert, which could have led us to an improvement in the more intuitive and pleasant user experience.

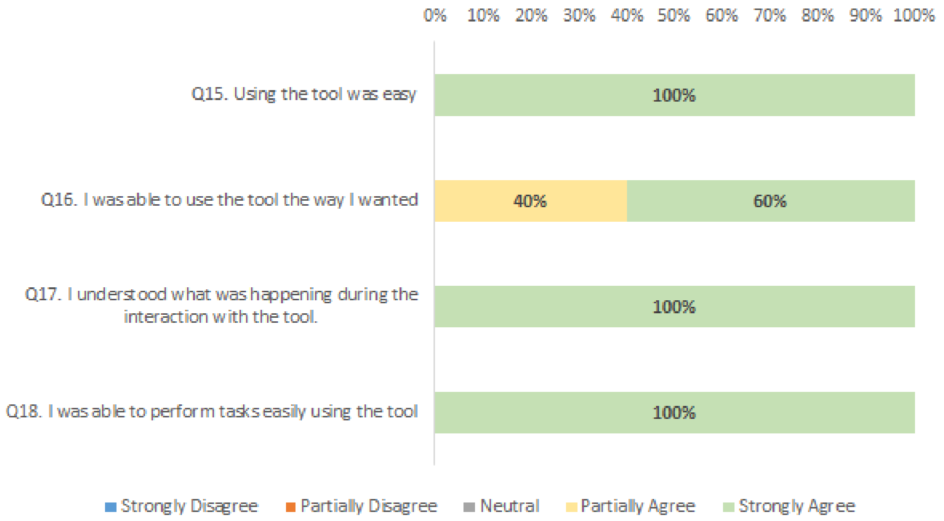


Figure 6.9: PSECO-IM tool regarding the ease-of-use tasks.

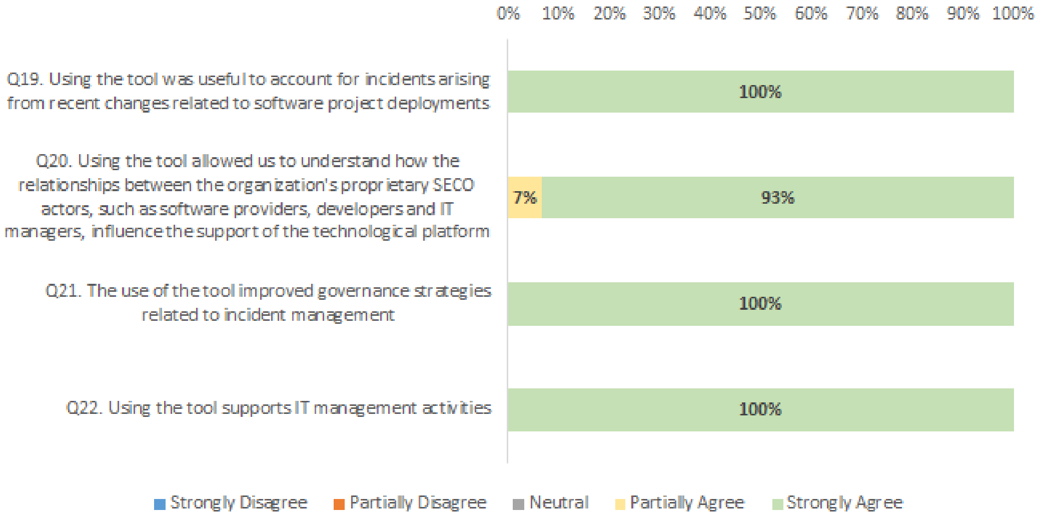


Figure 6.10: PSECO-IM tool regarding the usefulness of tasks.

According to participants, 100% strongly or partially agreed with the **utility** tasks of the PSECO-IM tool. The tool supports the IT management activities, improved governance strategies to incident management and was useful to account the incidents from recent changes. We did not have any disagreements. Several comments congratulated the initiative to develop this tool, as mentioned by participant P8.

> *Congratulations on the initiative. It's something we've wanted to have for a long time.* [Participant #P8]

Participants highlighted the understanding that the organization needs a more robust incident management process as the main point to drive the governance strategy aimed at sustaining the technology platform. Participant P1 considered the opportunity to pay more attention to preventing incidents from being opened rather than reducing inventory, while participant P2 is interested in investigating the productive capacity of each project team.

> *Opportunity to make executives aware of changing the strategic direction for handling incidents...*[Participant #P1]
>
> *The tool will be able to support the investigation of the productive capacity of each project team, as the team of developers may be overloaded.*
>
> [Participant #P2]

Participants P4 and P12 mention that the tool will be able to investigate gaps in software quality control during development, which could be the cause of so many incidents in the production environment right after a deployment. However, participant P4 is also concerned with the way the reports will be shown, as instead of providing alternative solutions, they can only be used to point out the culprits.

> *Positive: possibility to identify the absence of tools to improve the quality of deliveries. Negative: tool can be used to hunt villains.* [Participant #P4]
>
> *Positive: this tool will highlight the gaps in the company's software development in relation to quality.* [Participant #P12]

Participant P8 comments the integration of this tool with the change management process in the future in order to identify the software assets that most cause imbalances in the organization's SECO. This participant also alerted us to the fact that any process change needs a cultural change. People will need to understand the advantages of using a support tool like this.

> *Positive: cross information with the basis of changes and identify the programs that cause the most problems; Negative: process change requires a change in people's culture. Wide dissemination of the advantages of using this tool should be done before updating it into production.*
>
> [Participant #P8]

We consider that constant deployments in the production environment can destabilize the technological platform, causing SECO elements to weaken your relationships. This scenario may result in incidents and trigger factors that have a direct impact on the end-satisfaction user's and the organization's image.

In summary, the process and support tool were well accepted by the public who participated in the studies. The technology platform is an important part of SECO and, if designed correctly, it can bring positive financial results through user loyalty.

6.5 Threats to validity

The validity of the study is closely related to the reliability of the results. Every study involves risks that should be handled and taken into account alongside the findings, according to the classification described in (RUNESON et al., 2012). There are four types of study's validity: internal, external, constructo, and conclusion (TRAVASSOS; GUROV; AMARAL, 2002) (WOHLIN; RUNESON; NETO, et al., 2013). For this study, the following validity threats were identified:

1. **Internal Validity**

   - In the focus group study, the intense involvement of the researcher may have strengthened the threat. To mitigate it, the researcher was careful to provide only the proper amount of guidance without presenting any opinions of their own or suppressing freedom of expression.

2. **External Validity**

   - Focus groups tend to use homogeneous samples of people, which makes generalization difficult. To mitigate the risk, the choice of participants was made in conjunction with an experienced researcher, where the abilities and potential knowledge of each one were observed;
   - The participative case study involved only one organization. Thus, it is not possible to generalize the results to cases without intervention by the researcher or to organizations not similar to the studied organization.

3. **Constructo Validity**

   - The conduct of researchers and participants in the focus group is very germane to the constructo validity. The data that comes out of focus groups are the comments and interactions given by participants. These measures are highly valid as they are free from artificial influences from the environment and the researcher;

- Participants in the opinion survey were the same as those selected in the participative case study, considering the organization's availability and suitability for the desired profile (incident management activities experts). This is a threat to validity as their behavior can be altered to influence the outcome. A random selection of participants was not possible, since participants with an IT manager, developer, or business analyst profile and experience in the industry were required and there were not many possible candidates.

4. **Conclusion Validity**

   - Because the sample size was restricted due to the desired profile, the study's validity may be hampered by the small number of participants. Therefore, the results' interpretation should only be used as a guide;
   - The quantitative analysis was done by direct collecting in the online form during the analysis and interpretation of the data. The remarks mentioned by the participants were grouped for the qualitative analysis;
   - Data was collected directly from the participants in the online form to ensure the accuracy of the measurements.

6.6 Final remarks

In this chapter, details of how the evaluation studies of a process-based approach (PSECO-IM) to incident management to support the IT management team in the governance of a technology platform architecture of a proprietary SECO were presented. We evaluated a process-based approach to support governance of incident management in a proprietary SECO based on the opinions of industry experts (practitioners such as IT managers, developers, and business analysts) who are responsible for decision-making relating to governance strategies and maintaining the IT architecture in the proprietary SECO of the keystone.

The evaluated studies performed a focus group and a participative case study. The focus group was composed of two senior practitioner experts from the software industry with skills in governance and the ITIL framework, and a Ph.D. professor with extensive experience and a specialist in SECO governance. Next, we performed a participative case study. It was composed of participants who belonged to the sustaining team, with the following roles: business analysts, internal and external developers, and IT managers.

Furthermore, the PSECO-IM process was evaluated according to adequacy, control, understanding, and generality based on Strauss and Corbin (STRAUSS; CORBIN, 1998) criteria and the PSECO-IM tool followed the aspects of ease-of-use and utility based on the TAM (Technology Acceptance Model) (DAVIS, 1993). According to percentages results of agreement where no disagreement was highlighted, we concluded that both results were positive, fulfilling the goals they set themselves.

7. Conclusion

This chapter describes the considerations of this Master's dissertation as well as the contributions of this research. Some limitations of this work need to be observed while discussing the results. As form future work, we identified the research areas that can be explored by the scientific community in order to refine the incident management process in the proprietary SECO.

7.1 Implications

We have already presented some empirical findings throughout this Master's thesis. This section highlights the practical implications based on the findings of prior studies in order to develop a research agenda for the academic community and the software industry business. The purpose is to explain the practical consequences of both situations.

For the **academic community**, based on our findings and relevance, we verified that the definition of governance strategies can influence the proprietary SECO health through governance mechanisms. Choosing the right health metrics to provide operational indicators aiming to improve efficiency, support decision making, and increase participants' satisfaction is a challenge because the actions to implement the strategies depend on three pillars: people, process, and technology. There is no point in privileging investments in just one of these pillars. The movement of one pillar impacts the others. If one shifts, the others must also respond to maintain the balance. The keystone must focus on metrics that can help in achieving the most important business objectives.

For the **software industry practitioners**, we have to pay attention in the workforce capacity planning. We noticed that, as a consequence of tacit knowledge concentrated on a few people, it results in low-quality software products and many defects. Workforce capacity planning for the keystones that want to gain competitive advantage in the marketplace is a critical and an essential component of the value creation network.

In order to meet the market pressure from state-of-the-art solutions, IT managers try to manage more software projects than they can. Moreover, software development team turnover is a factor that makes it difficult to meet deadlines. IT managers must address the problem of transferring, hiring, or firing employees among different departments of an organization by implementing a knowledge management culture as one of the most important governance mechanisms within the governance strategy of a proprietary SECO.

The proposed approach for incident management to support governance in proprietary SECO can favor the balance of the technological platform, since it will be possible to identify the projects and software providers that caused the most critical incidents. Metrics and indicators can show the organization that the root causes of instability problems may be linked to low-quality software. Moreover, the support tool may help the decision-making of the IT management team to replace some assets.

Our work indicates an opportunity to meet an increasingly senior executives' demand for understanding of how business and technology can improve operations, enhance managers' decision-making and place the organization in a strong position to compete.

7.2 Contributions

Organizations that produce software systems work cooperatively and competitively to support new products, satisfy customer needs, and incorporate innovations. In this scenario, more attention is being paid to connectivity and dependency in relationships among several actors, such as IT software providers, internal and external developers, and IT managers. The network value creation that is built in this scenario is known as SECO.

The overcrowding of various products, technologies, and architectures from different ecosystems characterizes a proprietary SECO. In this context, concerns are focused on information and knowledge concentrated on a proprietary technological platform. To maintain a sustainable technological platform, the organization must establish governance policies. A sustainable strategy assures the platform's long-term viability.

The challenge of maintaining a sustainable platform is great as business initiatives have been increased in large organizations, according to a report published by Gartner Group. An architecture of a proprietary SECO platform broadly supports the use and development of software artifacts, such as products, applications, and services. However, the artifacts are protected by confidential agreement. They are built using various technologies combined with dozens of integration points, creating a network of dependencies and architectural complexities.

Moreover, the market pressure to deploy frequent software releases makes IT managers avoid sacrificing software project deadlines, affecting the confidence level of deliveries. As noticed in Chapter 5, new software releases usually bring new production defects and stability concerns. As a consequence, the poor quality of the software causes an umbalance in the proprietary SECO and generates unavailability of systems (incidents). This behavior leads to customer dissatisfaction.

Organizations that face high levels of demand consider quality management as a competitive differential. The incidents causes major image and financial upheavals for organizations. The IT management team, in order to mitigate the risks of incidents, should address strategic drivers based on governance mechanisms to sustain the technological platform in the proprietary SECO, as described in Chapter 6.

Therefore, some problems may happen due to the lack of an incident management process: i) preventing the organization from directing right governance strategies to evaluate the replacement of technological platform software assets in the proprietary SECO; and ii) hindering to penalize IT managers who deployed recent software changes with a low confidence level.

As considered in Chapters 1 and 2, the problem of sustaining the technological platform in the proprietary SECO is also a gap found in the literature, since it is not explored much further. Some traditional governance frameworks, such as ITIL, are not mentioned in the literature on proprietary SECO governance.

Important subscriptions of this work are related to the sustaining, quality of service and confidence level of the ecosystem platform. Moreover, the main contribution is to support the IT management team (stakeholders who have authority to make decisions in the organization) in the governance of a technology platform architecture in a proprietary SECO through the development of an incident management process. The following secondary contributions may be highlighted:

- **Exploratory Study:** the governance mechanisms of software assets in a proprietary SECO were identified and relevant correlations based on IT managers' interviews were studied (Chapter 3);
- **Longitudinal Literature Study:** the results represent the contributions on SECO governance mechanisms and SECO health metrics, as well as refined perspectives

on proprietary SECO classifications and the SECO incident management process (Chapter 2 Section 2.3);

- **Participative Case Study (1):** the participants' opinions are very important since they evaluate information collected from the longitudinal study. The participants proposed new governance strategies based on the governance mechanisms and health metrics in a proprietary SECO of a real organization (Chapter 4);
- **Rapid Review Study:** the results reveal the strategic drivers, indicators, and metrics for handling incidents in organizations. The study also provides us with a body of knowledge bound to practical problems relating to incident management strategies (Chapter 2 Section 2.4);
- **Approach for SECO Incident Management Process:** this is a contribution aimed at the support of IT management team in the governance of the architecture of a technology platform in a proprietary SECO. The support tool shows a way to visualize and centralize the data of the incidents due to recent projects changes in a proprietary SECO (Chapter 5); and
- **Evaluation Studies:** the results and protocols are important outcomes of this research since the studies assess the relevance and evaluation of applying the Proprietary SECO Confidence Level tool in a real organization and collect the experience of practitioners through a focus group and participative case study (2) (Chapter 6).

7.3 Publications

The activities performed in the Master's Course produced the following publications:

- **Investigating Asset Governance Mechanisms in a Proprietary Software Ecosystem:** this study was produced in the early stages of the research when the objective was to gain a greater understanding of the governance mechanisms in a proprietary SECO. The study was published in the main track of the XVI Brazilian Symposium on Information Systems (SBSI) (COSTA; FONTÃO; SANTOS, 2020a);
- **Governance Factors in Systems-of-Systems: Analysis of a Brazilian Public Institution:** this study was performed in the early stages of the research when the objective was to gain a greater understanding about factors that influence the governance in complex systems. The study was published at the V Workshop on Social, Human and Economic Aspects of Software (WASHES) (IMAMURA et al., 2020);

- **An Approach to Incident Management in Proprietary Software Ecosystems:** this study was performed in the definition phase of a research proposal. The study was published at the XIII Workshop on Theses and Dissertations in Information Systems (WTDSI) (COSTA; FONTÃO; SANTOS, 2020b);

- **Investigating Proprietary Software Ecosystem Governance and Health: An Update and a Refine Perspective:** this study was produced with the results of the longitudinal literature study conducted to provide an update on SECO governance mechanisms, SECO health metrics, and a refined perspective on the proprietary SECO incident management process. The study was published in the main track of the XVII Brazilian Symposium on Information Systems (SBSI) (COSTA; FONTÃO; SANTOS, 2021b);

- **Towards Proprietary Software Ecosystem Governance Strategies Based On Health Metrics:** this study was produced during the second year of the research throught a participative case study when it was necessary to characterize a real scenario to deal with governance strategies in a proprietary SECO. The study was published for a Special Issue on Collaboration and Innovation Dynamics in Software Ecosystems at IEEE Transactions on Engineering Management Journal (COSTA; FONTÃO; SANTOS, 2021d);

- **Service Management in Practice: Challenges, Opportunities, and Strategies:** this study was produced from the results of a participative case study when it was necessary to investigate keystone's issues with handling incident management and explore strategies to model the incident management process. The study was submitted to the Information and Management Journal (COSTA; FONTÃO; SANTOS, 2021c); and

- **Friendly Fire: An Approach to Reduce Incident Backlog in Proprietary Software Ecosystems:** this study was developed at the stage of modeling a process-based approach to incident management to support the IT management team in the governance of the technology platform in a proprietary SECO, as well as the implementation of the support tool to diagnose the confidence level. The results of the study are in the final stage of submission to the Information Systems Journal (COSTA; FONTÃO; SANTOS, 2021a).

7.4 Limitations

Some limitations were identified considering the execution of the studies of conception (exploratory, longitudinal, rapid review, and participative case), implementation (approach and focus group), and evaluation, as well as the support tool developed. The main limitations are described as follows:

- The survey to evaluate the support tool did not involve a number of participants for robust analysis with statistical tools;
- The results of evaluation studies cannot be generalized because they were not repeated in other organizations of different contexts, such as food, energy, and telecommunications industries;
- The process-based approach to incident management is not a reference model yet, because its definition, refinement and evaluation consider proprietary SECO. There is a need to evaluate the model considering other SECO classifications, such as hybrid and open SECO; and
- The support tool sample selected to carry out the studies had only experts from the same organization, which limits the validity of sustaining team activities related to the process-based approach and support tool.

7.5 Future work

In order to enrich this approach, some suggestions were identified in the longitudinal, survey, participative case, and evaluation studies. The notes can be considered as opportunities in future work, such as:

- Analysing the snowballing on the longitudinal literature and rapid review studies based on selected criteria can be performed;
- Exploring the mining of the organization's software repositories in order to discover standards and rules that can improve the software development quality, anticipate the detection of defects, facilitate evolutionary maintenance and predict the probability of generating an incident;
- Investigating the problem management process and issues in a proprietary SECO context. Problem management works closely with incident management according

to ITIL, but it is not the same. Problem management is tasked with analyzing root causes and preventing incidents from happening in the future.

- Running the same methodology in other organizations that have proprietary SECO and identifying whether the approach and support tool remain with the highest level of agreement;
- Deeping studies into the change management (process involved in Service Transition, one of ITIL library volumes) and software assets involved in incident management process. Incidents resulting from a change are metrics that measure business disruption caused by IT itself. In other words, it is an indicator of "friendly fire".

This research represents only a small contribution that aggregates the specific view of incident management related to governance mechanisms in a proprietary SECO. Through the availability of structured information, the processes that involve decision-making by the IT management team can be facilitated.

References

ADAMS, P; GOVEKAR, M. Hype Cycle for IT Operations Management. **Gartner Technical Professional Advice**, 2012.

ADDY, Rob. **Effective IT service management: to ITIL and beyond!** [S.l.]: Springer-Verlag, 2007.

AGOSTINI, Alessandra et al. Stimulating knowledge discovery and sharing. In: PROCEEDINGS of the 2003 international ACM SIGGROUP conference on Supporting group work. [S.l.: s.n.], 2003. p. 248–257.

ALBERT, B. **SECOGov: Um Modelo de Governança de Ecossistemas de Software para Apoiar Atividades de Arquitetura de TI**. 2014. PhD thesis – Dissertação. COPPE/UFRJ, Rio de Janeiro, Brasil.

ALBERT, Benno E; SANTOS, Rodrigo P dos; WERNER, Cláudia ML. Software ecosystems governance to enable it architecture based on software asset management. In: IEEE. 2013 7th IEEE International Conference on Digital Ecosystems and Technologies (DEST). [S.l.: s.n.], 2013. p. 55–60.

ALVES, Carina; OLIVEIRA, Joyce; JANSEN, Slinger. Understanding governance mechanisms and health in software ecosystems: A systematic literature review. In: SPRINGER. INTERNATIONAL Conference on Enterprise Information Systems. [S.l.: s.n.], 2017. p. 517–542.

ANGEREN, Joey van; ALVES, Carina; JANSEN, Slinger. Can we ask you to collaborate? Analyzing app developer relationships in commercial platform ecosystems. **Journal of Systems and Software**, Elsevier, v. 113, p. 430–445, 2016.

ARNDT, Jens-Magnus; DIBBERN, Jens. Co-innovation in a service oriented strategic network. In: IEEE. 2006 IEEE International Conference on Services Computing (SCC'06). [S.l.: s.n.], 2006. p. 285–288.

ASSINK, Marnix. Inhibitors of disruptive innovation capability: a conceptual model. **European journal of innovation management**, Emerald Group Publishing Limited, 2006.

AVILA, José Coelho; LUCENA FILHO, Gentil José; COSTA FIGUEIREDO, Rejane Maria da. Competências Conversacionais para a Governança Corporativa. **iSys-Revista Brasileira de Sistemas de Informação**, v. 10, n. 2, p. 85–110, 2017.

AYUSO, Silvia et al. Does stakeholder engagement promote sustainable innovation orientation? **Industrial Management & Data Systems**, Emerald Group Publishing Limited, 2011.

BAARS, Alfred; JANSEN, Slinger. A framework for software ecosystem governance. In: SPRINGER. INTERNATIONAL conference of software business. [S.l.: s.n.], 2012. p. 168–180.

BARTHELEMY, Jerome. The hidden costs of IT outsourcing. **MIT Sloan management review**, Massachusetts Institute of Technology, Cambridge, MA, v. 42, n. 3, p. 60, 2001.

BASILI, V. GQM approach has evolved to include models. **IEEE SOFTWARE**, IEEE COMPUTER SOC 10662 LOS VAQUEROS CIRCLE, PO BOX 3014, LOS ALAMITOS, CA ..., v. 11, n. 1, p. 8–8, 1994.

BASKERVILLE, Richard L. Distinguishing action research from participative case studies. **Journal of systems and information technology**, v. 1, n. 1, p. 25–45, 1997.

BASSI, Laurie J; VAN BUREN, Mark E. Valuing investments in intellectual capital. **International Journal of Technology Management**, Inderscience Publishers, v. 18, n. 5-8, p. 414–432, 1999.

BENBASAT, Izak; GOLDSTEIN, David K; MEAD, Melissa. The case research strategy in studies of information systems. **MIS quarterly**, JSTOR, p. 369–386, 1987.

BENESTY, Jacob et al. **Noise reduction in speech processing**. [S.l.]: Springer Science & Business Media, 2009. v. 2.

BETZ, Frederick. **Managing technological innovation: competitive advantage from change**. [S.l.]: John Wiley & Sons, 2003.

BORJESSON, Emil; FELDT, Robert. Automated system testing using visual gui testing tools: A comparative study in industry. In: IEEE. 2012 IEEE Fifth International Conference on Software Testing, Verification and Validation. [S.l.: s.n.], 2012. p. 350–359.

BOSCARIOLI, Clodis; ARAUJO, Renata Mendes de; MACIEL, Rita Suzana Pitangueira. I GranDSI-BR Grand Research Challenges in Information Systems in Brazil 2016-2026. SBC-Sociedade Brasileira de Computação, 2017.

BOSCH, Jan. From software product lines to software ecosystems. In: SPLC. [S.l.: s.n.], 2009. v. 9, p. 111–119.

BOSTOEN, Friso; MÂNDRESCU, Daniel. Assessing abuse of dominance in the platform economy: a case study of app stores. **European Competition Journal**, Taylor & Francis, p. 1–61, 2020.

BOUCHARAS, Vasilis; JANSEN, Slinger; BRINKKEMPER, Sjaak. Formalizing software ecosystem modeling. In: PROCEEDINGS of the 1st international workshop on Open component ecosystems. [S.l.: s.n.], 2009. p. 41–50.

BRAUN, Virginia; CLARKE, Victoria. Using thematic analysis in psychology. **Qualitative research in psychology**, Taylor & Francis, v. 3, n. 2, p. 77–101, 2006.

BRHEL, Manuel et al. Exploring principles of user-centered agile software development: A literature review. **Information and Software Technology**, Elsevier, v. 61, p. 163–181, 2015.

BRINKKEMPER, Sjaak; VAN SOEST, Ivo; JANSEN, Slinger. Modeling of product software businesses: Investigation into industry product and channel typologies. In: INFORMATION Systems Development. [S.l.]: Springer, 2009. p. 307–325.

BROWN, Carol V. The IT organization of the future. **Competing in the Information Age: Align in the Sand (Ed, Luftman, JN). Oxford University Press, New York, NY**, p. 191–207, 2003.

BROWN, Trevor; POTOSKI, Matt. Contracting for management: Assessing management capacity under alternative service delivery arrangements. **Journal of Policy Analysis and Management: The Journal of the Association for Public Policy Analysis and Management**, Wiley Online Library, v. 25, n. 2, p. 323–346, 2006.

CALDIERA, Victor R Basili1 Gianluigi; ROMBACH, H Dieter. The goal question metric approach. **Encyclopedia of software engineering**, p. 528–532, 1994.

CAPILLA, Rafael et al. A web-based tool for managing architectural design decisions. **ACM SIGSOFT software engineering notes**, ACM New York, NY, USA, v. 31, n. 5, 4–es, 2006.

CARTAXO, Bruno; PINTO, Gustavo; SOARES, Sergio. Rapid Reviews in Software Engineering. In: CONTEMPORARY Empirical Methods in Software Engineering. [S.l.]: Springer, 2020. p. 357–384.

CASEY, Thomas F; WARLIN, Karen. Retention and customer satisfaction. **Compensation & Benefits Review**, Sage Publications Sage CA: Thousand Oaks, CA, v. 33, n. 3, p. 27–31, 2001.

CECCAGNOLI, Marco et al. Cocreation of value in a platform ecosystem! The case of enterprise software. **MIS quarterly**, JSTOR, p. 263–290, 2012.

COSTA, Luiz Alexandre; FONTÃO, Awdren; SANTOS, Rodrigo. Friendly Fire: An Approach to Reduce Incident Backlog in Proprietary Software Ecosystems *(under submission)*. In: TECHICAL Report. [S.l.: s.n.], 2021. p. 1–38.

________. Investigating asset governance mechanisms in a proprietary software ecosystem. In: XVI Brazilian Symposium on Information Systems. [S.l.: s.n.], 2020. p. 1–8.

________. Investigating Proprietary Software Ecosystem Governance and Health: An Updated and Refined Perspective. In: XVII Brazilian Symposium on Information Systems. [S.l.: s.n.], 2021. p. 1–8.

________. Service Management in Practice: Challenges and Strategies in Proprietary Software Ecosystem *(submitted)*. In: TECHICAL Report. [S.l.: s.n.], 2021. p. 1–28.

________. Toward Proprietary Software Ecosystem Governance Strategies Based on Health Metrics. **IEEE Transactions on Engineering Management**, IEEE, 2021.

________. Uma Abordagem para Gestão de Incidentes em Ecossistemas de Software Proprietário. In: SBC. ANAIS Estendidos do XVI Simpósio Brasileiro de Sistemas de Informação. [S.l.: s.n.], 2020. p. 52–55.

COZZOLINO, Alessio; VERONA, Gianmario; ROTHAERMEL, Frank T. Unpacking the disruption process: New technology, business models, and incumbent adaptation. **Journal of Management Studies**, Wiley Online Library, v. 55, n. 7, p. 1166–1202, 2018.

CREEDEN, Denis Michael et al. **Methods and systems for managing risk management information**. [S.l.]: Google Patents, Nov. 2013. US Patent 8,589,273.

CRUZES, Daniela S; DYBA, Tore. Recommended steps for thematic synthesis in software engineering. In: IEEE. 2011 International Symposium on Empirical Software Engineering and Measurement. [S.l.: s.n.], 2011. p. 275–284.

CURRIE, Wendy L; SELTSIKAS, Philip. Exploring the supply-side of IT outsourcing: evaluating the emerging role of application service providers. **European Journal of Information Systems**, Taylor & Francis, v. 10, n. 3, p. 123–134, 2001.

CUSICK, James J; MA, Gary. Creating an ITIL inspired Incident Management approach: Roots, response, and results. In: IEEE. 2010 IEEE/IFIP Network Operations and Management Symposium Workshops. [S.l.: s.n.], 2010. p. 142–148.

DAVIS, Fred D. User acceptance of information technology: system characteristics, user perceptions and behavioral impacts. **International journal of man-machine studies**, Elsevier, v. 38, n. 3, p. 475–487, 1993.

DHUNGANA, Deepak et al. Software ecosystems vs. natural ecosystems: learning from the ingenious mind of nature. In: PROCEEDINGS of the Fourth European Conference on Software Architecture: Companion Volume. [S.l.: s.n.], 2010. p. 96–102.

DROST, Ellen A. Validity and reliability in social science research. **Education Research and perspectives**, v. 38, n. 1, p. 105–123, 2011.

DRUCKER, Peter Ferdinand. **People and performance: The best of Peter Drucker on management**. [S.l.]: Routledge, 1995.

ELSAYED, Elsayed A. **Reliability engineering**. [S.l.]: John Wiley & Sons, 2020.

FEILER, Peter H; HUMPHREY, Watts S. Software process development and enactment: Concepts and definitions. In: IEEE. [1993] Proceedings of the Second International Conference on the Software Process-Continuous Software Process Improvement. [S.l.: s.n.], 1993. p. 28–40.

FIGUEIREDO FILHO, Dalson Britto; SILVA JÚNIOR, José Alexandre. Desvendando os Mistérios do Coeficiente de Correlação de Pearson (r). **Revista Polı´tica Hoje**, v. 18, n. 1, p. 115–146, 2009.

FONTÃO, Awdren et al. Supporting governance of mobile application developers from mining and analyzing technical questions in stack overflow. **Journal of Software Engineering Research and Development**, Springer, v. 6, n. 1, p. 8, 2018.

FREIRE, Emerson et al. Inovação e competitividade: o desafio a ser enfrentado pela indústria de software. [sn], 2002.

GALIN, Daniel. **Software quality assurance: from theory to implementation**. [S.l.]: Pearson education, 2004.

GALUP, Stuart D et al. An overview of IT service management. **Communications of the ACM**, ACM New York, NY, USA, v. 52, n. 5, p. 124–127, 2009.

GEFEN, David; WYSS, Simon; LICHTENSTEIN, Yossi. Business familiarity as risk mitigation in software development outsourcing contracts. **MIS quarterly**, JSTOR, p. 531–551, 2008.

GOPAL, Anandasivam; KOKA, Balaji R. The role of contracts on quality and returns to quality in offshore software development outsourcing. **Decision sciences**, Wiley Online Library, v. 41, n. 3, p. 491–516, 2010.

GREINER, Martina E; BÖHMANN, Tilo; KRCMAR, Helmut. A strategy for knowledge management. **Journal of knowledge management**, Emerald Group Publishing Limited, 2007.

GRIEVES, Michael; VICKERS, John. Digital twin: Mitigating unpredictable, undesirable emergent behavior in complex systems. In: TRANSDISCIPLINARY perspectives on complex systems. [S.l.]: Springer, 2017. p. 85–113.

GUPTA, Rajeev; PRASAD, K Hima; MOHANIA, Mukesh. Automating ITSM incident management process. In: IEEE. 2008 International Conference on Autonomic Computing. [S.l.: s.n.], 2008. p. 141–150.

HABY, Michelle M et al. What are the best methodologies for rapid reviews of the research evidence for evidence-informed decision making in health policy and practice: a rapid review. **Health research policy and systems**, BioMed Central, v. 14, n. 1, p. 1–12, 2016.

HAGGIE, Knox; KINGSTON, John. Choosing your knowledge management strategy. **Journal of Knowledge Management Practice**, School of Informatics, University of Edinburgh, v. 4, n. 4, p. 1–20, 2003.

HAGSTROM, Robert G. **The Warren Buffett Way**. [S.l.]: John Wiley & Sons, 2013.

HARTIGH, Erik den; TOL, Michiel; VISSCHER, Wouter. The health measurement of a business ecosystem. In: PROCEEDINGS of the European Network on Chaos and Complexity Research and Management Practice Meeting. [S.l.: s.n.], 2006. p. 1–39.

HATCH, Mary Jo. The dynamics of organizational culture. **Academy of management review**, Academy of Management Briarcliff Manor, NY 10510, v. 18, n. 4, p. 657–693, 1993.

HEVNER, Alan R. A three cycle view of design science research. **Scandinavian journal of information systems**, v. 19, n. 2, p. 4, 2007.

HOCHSTEIN, Axel; ZARNEKOW, Rüdiger; BRENNER, Walter. ITIL as common practice reference model for IT service management: formal assessment and implications for practice. In: IEEE. 2005 IEEE International Conference on e-Technology, e-Commerce and e-Service. [S.l.: s.n.], 2005. p. 704–710.

HSU, Ya-Hui; FANG, Wenchang. Intellectual capital and new product development performance: The mediating role of organizational learning capability. **Technological Forecasting and Social Change**, Elsevier, v. 76, n. 5, p. 664–677, 2009.

HUSSAIN, Azham; RAZAK, Hamidah Abdul; MKPOJIOGU, Emmanuel OC. The perceived usability of automated testing tools for mobile applications. **Journal of Engineering, Science and Technology (JESTEC)**, Taylor's University, v. 12, n. 4, p. 89–97, 2017.

HUTCHESON, Marnie L. **Software testing fundamentals: Methods and metrics**. [S.l.]: John Wiley & Sons, 2003.

IANSITI, Marco; LEVIEN, Roy. Keystones and dominators: Framing operating and technology strategy in a business ecosystem. **Harvard Business School, Boston**, n. 03-061, p. 1–82, 2004.

________. Strategy as ecology. **Harvard business review**, v. 82, n. 3, p. 68–78, 2004.

IANSITI, Marco; RICHARDS, Gregory L. The information technology ecosystem: Structure, health, and performance. **The Antitrust Bulletin**, SAGE Publications Sage CA: Los Angeles, CA, v. 51, n. 1, p. 77–110, 2006.

IDEN, Jon; EIKEBROKK, Tom Roar. Implementing IT Service Management: A systematic literature review. **International Journal of Information Management**, Elsevier, v. 33, n. 3, p. 512–523, 2013.

IMAMURA, Marcio et al. Fatores de Governança em Sistemas-de-Sistemas: Análise de uma Instituição Pública Brasileira. In: SBC. ANAIS do V Workshop sobre Aspectos Sociais, Humanos e Econômicos de Software. [S.l.: s.n.], 2020. p. 31–40.

ISHAK, Zurida; FONG, Sim Liew; SHIN, See Cia. SMART KPI management system framework. In: IEEE. 2019 IEEE 9th International Conference on System Engineering and Technology (ICSET). [S.l.: s.n.], 2019. p. 172–177.

JANSEN, Slinger; BRINKKEMPER, Sjaak; FINKELSTEIN, Anthony. Business Network Management as a Survival Strategy: A Tale of Two Software Ecosystems. **Iwseco@ Icsr**, Citeseer, v. 2009, 2009.

JANSEN, Slinger; BRINKKEMPER, Sjaak; SOUER, Jurriaan, et al. Shades of gray: Opening up a software producing organization with the open software enterprise model. **Journal of Systems and Software**, Elsevier, v. 85, n. 7, p. 1495–1510, 2012.

JANSEN, Slinger; CUSUMANO, Michael A. Defining software ecosystems: a survey of software platforms and business network governance. In: SOFTWARE Ecosystems Analyzing and Managing Business Networks in the Software Industry. [S.l.]: Edward Elgar Publishing, 2013.

KAPPELMAN, Leon A; MCKEEMAN, Robert; ZHANG, Lixuan. Early warning signs of IT project failure: The dominant dozen. **Information systems management**, Taylor & Francis, v. 23, n. 4, p. 31–36, 2006.

KARAMI, Amir; GUO, Zhiling. A fuzzy logic multi-criteria decision framework for selecting it service providers. In: IEEE. 2012 45th Hawaii International Conference on System Sciences. [S.l.: s.n.], 2012. p. 1118–1127.

KAUR, Gurpreet; BAHL, Kailash. Software reliability, metrics, reliability improvement using agile process. **International Journal of Innovative Science, Engineering & Technology**, v. 1, n. 3, p. 143–147, 2014.

KITAY, Jim; WRIGHT, Christopher. Take the money and run? Organisational boundaries and consultants' roles. **The service industries journal**, Taylor & Francis, v. 24, n. 3, p. 1–18, 2004.

KITCHENHAM, Barbara; BRERETON, Pearl. A systematic review of systematic review process research in software engineering. **Information and software technology**, Elsevier, v. 55, n. 12, p. 2049–2075, 2013.

KITCHENHAM, Barbara; CHARTERS, Stuart. Guidelines for performing systematic literature reviews in software engineering. **EBSE Technical Report EBSE-2007-01**, Citeseer, 2007.

KITZINGER, Jenny. Qualitative research: introducing focus groups. **Bmj**, British Medical Journal Publishing Group, v. 311, n. 7000, p. 299–302, 1995.

KLUTKE, Georgia-Ann; KIESSLER, Peter C; WORTMAN, Martin A. A critical look at the bathtub curve. **IEEE Transactions on reliability**, IEEE, v. 52, n. 1, p. 125–129, 2003.

KUDE, Thomas; HUBER, Thomas; DIBBERN, Jens. Successfully Governing Software Ecosystems: Competence Profiles of Partnership Managers. **IEEE Software**, IEEE, v. 36, n. 3, p. 39–44, 2018.

LAANTI, Maarit; SALO, Outi; ABRAHAMSSON, Pekka. Agile methods rapidly replacing traditional methods at Nokia: A survey of opinions on agile transformation. **Information and Software Technology**, Elsevier, v. 53, n. 3, p. 276–290, 2011.

LEWIS, William E. **Software testing and continuous quality improvement**. [S.l.]: CRC press, 2017.

LINÅKER, Johan et al. A survey on the perception of innovation in a large product-focused software organization. In: SPRINGER. INTERNATIONAL Conference of Software Business. [S.l.: s.n.], 2015. p. 66–80.

LO, David; NAGAPPAN, Nachiappan; ZIMMERMANN, Thomas. How practitioners perceive the relevance of software engineering research. In: PROCEEDINGS of the 2015 10th Joint Meeting on Foundations of Software Engineering. [S.l.: s.n.], 2015. p. 415–425.

LONG, John O. **ITIL® 2011 at a Glance**. [S.l.]: Springer Science & Business Media, 2012.

LUCIANO, Edimara Mezzomo; TESTA, Maurı´cio Gregianin; AZEVEDO BRAGANÇA, Carlos Eduardo Barbosa de. Percebendo os benefı´cios e dificuldades da adoção da gestão de serviços de tecnologia da informação. **REGE-Revista de Gestão**, Elsevier, v. 19, n. 1, p. 145–164, 2012.

MAGNANINI, Federico; FERRETTI, Luca; COLAJANNI, Michele. Efficient license management based on smart contracts between software vendors and service providers. In: IEEE. 2019 IEEE 18th International Symposium on Network Computing and Applications (NCA). [S.l.: s.n.], 2019. p. 1–6.

MAHTO, Dalgobind; KUMAR, Anjani. Application of root cause analysis in improvement of product quality and productivity. **Journal of Industrial Engineering and Management (JIEM)**, Barcelona: OmniaScience, v. 1, n. 2, p. 16–53, 2008.

MANIKAS, Konstantinos. Revisiting software ecosystems research: A longitudinal literature study. **Journal of Systems and Software**, Elsevier, v. 117, p. 84–103, 2016.

MANIKAS, Konstantinos; HANSEN, Klaus Marius. Reviewing the health of software ecosystems–a conceptual framework proposal. In: CITESEER. PROCEEDINGS of the 5th international workshop on software ecosystems (IWSECO). [S.l.: s.n.], 2013. p. 33–44.

MANIKAS, Konstantinos; HANSEN, Klaus Marius. Software ecosystems–A systematic literature review. **Journal of Systems and Software**, Elsevier, v. 86, n. 5, p. 1294–1306, 2013.

MANSUR, Ricardo. **Governança de TI: metodologias, frameworks e melhores práticas**. [S.l.]: Brasport, 2007.

MCNAUGHTON, Blake; RAY, Pradeep; LEWIS, Lundy. Designing an evaluation framework for IT service management. **Information & Management**, Elsevier, v. 47, n. 4, p. 219–225, 2010.

MEN, Linjuan Rita. Strategic internal communication: Transformational leadership, communication channels, and employee satisfaction. **Management communication quarterly**, Sage Publications Sage CA: Los Angeles, CA, v. 28, n. 2, p. 264–284, 2014.

MENDES, Emilia et al. When to Update Systematic Literature Reviews in Software Engineering. **Journal of Systems and Software**, Elsevier, p. 110607, 2020.

MOELLER, Robert R. **Executive's guide to IT governance: improving systems processes with service management, COBIT, and ITIL**. [S.l.]: John Wiley & Sons, 2013. v. 637.

MOLLÉRI, Jefferson Seide; PETERSEN, Kai; MENDES, Emilia. Survey guidelines in software engineering: An annotated review. In: ACM. PROCEEDINGS of the 10th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement. [S.l.: s.n.], 2016. p. 58.

MONTEITH, John Yates; MCGREGOR, John D; INGRAM, John E. Proposed metrics on ecosystem health. In: PROCEEDINGS of the 2014 ACM international workshop on Software-defined ecosystems. [S.l.: s.n.], 2014. p. 33–36.

MORGAN, David L; KRUEGER, Richard A. **The focus group guidebook**. [S.l.]: Sage, 1998.

MUNSHI, Jamal. A method for constructing Likert scales. **Available at SSRN 2419366**, 2014.

MUTSAERS, Ernest-Jan; VAN DER ZEE, Han; GIERTZ, Henrik. The evolution of information technology. **Information Management & Computer Security**, MCB UP Ltd, 1998.

NDLELA, Lorna Thembisile; DU TOIT, ASA. Establishing a knowledge management programme for competitive advantage in an enterprise. **International journal of information management**, Elsevier, v. 21, n. 2, p. 151–165, 2001.

NOVAK, Joseph D; CAÑAS, Alberto J. The theory underlying concept maps and how to construct them. **Florida Institute for Human and Machine Cognition**, Citeseer, v. 1, n. 1, p. 1–31, 2006.

NULTY, Duncan D. The adequacy of response rates to online and paper surveys: what can be done? **Assessment & evaluation in higher education**, Routledge, v. 33, n. 3, p. 301–314, 2008.

ORTEGA, Jaime. Job rotation as a learning mechanism. **Management science**, INFORMS, v. 47, n. 10, p. 1361–1370, 2001.

PALILINGAN, Verry Ronny; BATMETAN, Johan Reimon. Incident management in academic information system using ITIL framework. In: IOP PUBLISHING, 1. IOP Conference Series: Materials Science and Engineering. [S.l.: s.n.], 2018. v. 306, p. 012110.

PEE, Loo Geok; KANKANHALLI, Atreyi. A model of organisational knowledge management maturity based on people, process, and technology. **Journal of information & knowledge management**, World Scientific, v. 8, n. 02, p. 79–99, 2009.

PETERSEN, Kai; VAKKALANKA, Sairam; KUZNIARZ, Ludwik. Guidelines for conducting systematic mapping studies in software engineering: An update. **Information and Software Technology**, Elsevier, v. 64, p. 1–18, 2015.

POLISENA, Julie et al. Rapid review summit: an overview and initiation of a research agenda. **Systematic reviews**, Springer, v. 4, n. 1, p. 1–6, 2015.

POWELL, Thomas C. Total quality management as competitive advantage: a review and empirical study. **Strategic management journal**, Wiley Online Library, v. 16, n. 1, p. 15–37, 1995.

PRICE, James H; MURNAN, Judy. Research limitations and the necessity of reporting them. **American Journal of Health Education**, Taylor & Francis Ltd., v. 35, n. 2, p. 66, 2004.

PRICE, Margaret; HANDLEY, Karen, et al. Feedback: all that effort, but what is the effect? **Assessment & Evaluation in Higher Education**, Routledge, v. 35, n. 3, p. 277–289, 2010.

PRODAN, Mircea; PRODAN, Adriana; PURCAREA, Anca Alecandra. Three new dimensions to people, process, technology improvement model. In: NEW contributions in information systems and technologies. [S.l.]: Springer, 2015. p. 481–490.

PURCELL, John et al. **People management and performance**. [S.l.]: Routledge, 2008.

RAMLAOUI, Saı¨d; SEMMA, Alami. Comparative study oComparative of COBIT with other IT Governance Frameworks. **International Journal of Computer Science Issues (IJCSI)**, Int. Journal of Computer Science Issues (IJCSI), v. 11, n. 6, p. 95, 2014.

ROHRBECK, René; HÖLZLE, Katharina; GEMÜNDEN, Hans Georg. Opening up for competitive advantage–How Deutsche Telekom creates an open innovation ecosystem. **R&d Management**, Wiley Online Library, v. 39, n. 4, p. 420–430, 2009.

RUNESON, Per et al. **Case study research in software engineering: Guidelines and examples**. [S.l.]: John Wiley & Sons, 2012.

SADI, Mahsa H; YU, Eric. Designing software ecosystems: How can modeling techniques help? In: ENTERPRISE, Business-Process and Information Systems Modeling. [S.l.]: Springer, 2015. p. 360–375.

SAHIBUDIN, Shamsul; SHARIFI, Mohammad; AYAT, Masarat. Combining ITIL, COBIT and ISO/IEC 27002 in order to design a comprehensive IT framework in organizations. In: IEEE. 2008 Second Asia International Conference on Modelling & Simulation (AMS). [S.l.: s.n.], 2008. p. 749–753.

SANTOS, Rodrigo Pereira. **Managing and monitoring software ecosystem to support demand and solution analysis**. 2016. PhD thesis – COPPE/UFRJ.

SANTOS, Rodrigo Pereira dos et al. ReuseECOS: An approach to support global software development through software ecosystems. In: IEEE. 2012 IEEE Seventh International Conference on Global Software Engineering Workshops. [S.l.: s.n.], 2012. p. 60–65.

SANTOS, Rodrigo Pereira dos; WERNER, Cláudia Maria Lima. A proposal for software ecosystems engineering. In: IWSECO@ ICSOB. [S.l.: s.n.], 2011. p. 40–51.

SCHILIT, Warren Keith. An examination of the influence of middle-level managers in formulating and implementing strategic decisions. **Journal of Management Studies**, Wiley Online Library, v. 24, n. 3, p. 271–293, 1987.

SELIG, Gad J. **Implementing IT Governance-A Practical Guide to Global Best Practices in IT Management**. [S.l.]: Van Haren, 2008.

SHULL, Forrest; SINGER, Janice; SJØBERG, Dag IK. **Guide to advanced empirical software engineering**. [S.l.]: Springer, 2007.

SHWARTZ, Larisa et al. Service provider considerations for IT service management. In: IEEE. 2007 10th IFIP/IEEE International Symposium on Integrated Network Management. [S.l.: s.n.], 2007. p. 757–760.

SINGH, MD; KANT, R. Knowledge management barriers: An interpretive structural modeling approach. **International Journal of Management Science and Engineering Management**, Taylor & Francis Group, v. 3, n. 2, p. 141–150, 2008.

SMINIA, Harry. Process research in strategy formation: Theory, methodology and relevance. **International Journal of Management Reviews**, Wiley Online Library, v. 11, n. 1, p. 97–125, 2009.

SOMMERVILLE, Ian; SAWYER, Pete. Viewpoints: principles, problems and a practical approach to requirements engineering. **Annals of software engineering**, Springer, v. 3, n. 1, p. 101–130, 1997.

SOOSAY, Claudine A; HYLAND, Paul W; FERRER, Mario. Supply chain collaboration: capabilities for continuous innovation. **Supply chain management: An international journal**, Emerald Group Publishing Limited, 2008.

SOUZA, Mauri´cio; MOREIRA, Renata; FIGUEIREDO, Eduardo. Students perception on the use of project-based learning in software engineering education. In: PROCEEDINGS of the XXXIII Brazilian Symposium on Software Engineering. [S.l.: s.n.], 2019. p. 537–546.

STANK, Theodore P; KELLER, Scott B; DAUGHERTY, Patricia J. Supply chain collaboration and logistical service performance. **Journal of Business logistics**, Wiley Online Library, v. 22, n. 1, p. 29–48, 2001.

STRAUSS, Anselm; CORBIN, Juliet. **Basics of qualitative research techniques**. [S.l.]: Citeseer, 1998.

SWARTZ, Jody; VYSNIAUSKAS, Paulius. Software Asset Management in Large Scale Organizations-Exploring the Challenges and Benefits, 2015.

TALLA, Malleswara; VALVERDE, Raul. An implementation of ITIL guidelines for IT support process in a service organization. **International Journal of Information and Electronics Engineering**, v. 3, n. 3, p. 334–341, 2013.

TIWANA, Amrit; KONSYNSKI, Benn; BUSH, Ashley A. Research commentary—Platform evolution: Coevolution of platform architecture, governance, and environmental dynamics. **Information systems research**, INFORMS, v. 21, n. 4, p. 675–687, 2010.

TONET, Helena Correa; PAZ, Maria das Graças Torres da. Um modelo para o compartilhamento de conhecimento no trabalho. **Revista de Administração Contemporânea**, SciELO Brasil, v. 10, n. 2, p. 75–94, 2006.

TRAVASSOS, Guilherme Horta; GUROV, Dmytro; AMARAL, EAGG. Introdução à engenharia de software experimental. UFRJ, 2002.

TRICCO, Andrea C; ANTONY, Jesmin, et al. A scoping review of rapid review methods. **BMC medicine**, BioMed Central, v. 13, n. 1, p. 1–15, 2015.

TRICCO, Andrea C; LANGLOIS, Etienne, et al. **Rapid reviews to strengthen health policy and systems: a practical guide**. [S.l.]: World Health Organization, 2017.

TRINKENREICH, Bianca et al. Combining GQM+ Strategies and OKR-Preliminary Results from a Participative Case Study in Industry. In: SPRINGER. INTERNATIONAL Conference on Product-Focused Software Process Improvement. [S.l.: s.n.], 2019. p. 103–111.

TUROFF, Murray et al. The design of a dynamic emergency response management information system (DERMIS). **Journal of Information Technology Theory and Application (JITTA)**, v. 5, n. 4, p. 3, 2004.

VAN BON, Jan et al. **Foundations of IT Service Management Based on ITIL®**. [S.l.]: Van Haren, 2008. v. 3.

VAN DER AALST, Wil MP; SCHONENBERG, M Helen; SONG, Minseok. Time prediction based on process mining. **Information systems**, Elsevier, v. 36, n. 2, p. 450–475, 2011.

VAN MARREWIJK, Marcel; TIMMERS, Joanna. Human capital management: New possibilities in people management. **Journal of Business Ethics**, Springer, v. 44, n. 2, p. 171–184, 2003.

WAREHAM, Jonathan; FOX, Paul B; CANO GINER, Josep Lluı´s. Technology ecosystem governance. **Organization Science**, Informs, v. 25, n. 4, p. 1195–1215, 2014.

WATT, Amber et al. Rapid reviews versus full systematic reviews: an inventory of current methods and practice in health technology assessment. Cambridge Univ Press, 2008.

WESTFECHTEL, Bernhard; CONRADI, Reidar. Software architecture and software configuration management. In: SOFTWARE Configuration Management. [S.l.]: Springer, 2001. p. 24–39.

WILLIAMSON, Kirsty. **Research methods for students, academics and professionals: Information management and systems**. [S.l.]: Elsevier, 2002.

WILLIAMSON, Peter James; DE MEYER, Arnoud. Ecosystem advantage: How to successfully harness the power of partners. **California Management Review**, SAGE Publications Sage CA: Los Angeles, CA, v. 55, n. 1, p. 24–46, 2012.

WOHLIN, Claes; RUNESON, Per; HÖST, Martin, et al. **Experimentation in software engineering**. [S.l.]: Springer Science & Business Media, 2012.

WOHLIN, Claes; RUNESON, Per; NETO, Paulo Anselmo da Mota Silveira, et al. On the reliability of mapping studies in software engineering. **Journal of Systems and Software**, Elsevier, v. 86, n. 10, p. 2594–2610, 2013.

YIN, Robert K. **Case study research and applications: Design and methods**. [S.l.]: Sage publications, 2017.

________. **Introducing the world of education: A case study reader**. [S.l.]: Sage, 2005.

ZAPF, Dieter; DORMANN, Christian; FRESE, Michael. Longitudinal studies in organizational stress research: a review of the literature with reference to methodological issues. **Journal of occupational health psychology**, Educational Publishing Foundation, v. 1, n. 2, p. 145, 1996.

Appendices

A. Selected Studies in the Longitudinal Literature

Studies **S1 to S89** were found in the SLR of Alves *et al.* (ALVES; OLIVEIRA; JANSEN, 2017).

S90. Lehtinen, J., Peltokorpi, A., & Artto, K. (2019). Megaprojects as organizational platforms and technology platforms for value creation. International Journal of Project Management, 37(1), 43-58.

S91. Alves, C., Valença, G., & Franch, X. (2018). Exercising power in software ecosystems. IEEE software, 36(3), 50-54.

S92. Wang, L., Wan, J., & Gao, X. (2019). Toward the Health Measure for Open Source Software Ecosystem Via Projection Pursuit and Real-Coded Accelerated Genetic.

S93. Pernpeintner, M. (2019). Collaboration as an emergent property of self-organizing software systems. In 2019 IEEE 4th International Workshops on Foundations and Applications of Self* Systems (FAS* W) (pp. 231-233). IEEE.

S94. Jansen, S. (2020). A focus area maturity model for software ecosystem governance. Information and Software Technology, 118, 106219.

S95. Fontão, A., Bonifácio, B., Santos, R. P., & Dias-Neto, A. C. (2018). Mobile application development training in mobile software ecosystem: Investigating the developer experience. In Proceedings of the 17th Brazilian Symposium on Software Quality (pp. 160-169).

S96. Boshuis, S., Braam, T., Marchena, A. P., & Jansen, S. (2018). The effect of generic strategies on software ecosystem health: the case of cryptocurrency ecosystems. In 2018 IEEE/ACM 1st International Workshop on Software Health (SoHeal) (pp. 10-17). IEEE.

S97. Dijkers, J., Sincic, R., Wasankhasit, N., & Jansen, S. (2018). Exploring the effect

of software ecosystem health on the financial performance of the open source companies. In 2018 IEEE/ACM 1st International Workshop on Software Health (SoHeal) (pp. 48-55). IEEE.

S98. Hyrynsalmi, S., Ruohonen, J., & Seppänen, M. (2018). Healthy until otherwise proven: some proposals for renewing research of software ecosystem health. In 2018 IEEE/ACM 1st International Workshop on Software Health (SoHeal) (pp. 18-24). IEEE.

S99. Fontão, A., Ábia, B., Wiese, I., Estácio, B., Quinta, M., Santos, R. P., & Dias-Neto, A. C. (2018). Supporting governance of mobile application developers from mining and analyzing technical questions in stack overflow. Journal of Software Engineering Research and Development.

S100. Amorim, S. S., McGregor, J. D., de Almeida, E. S., & Chavez, C. F. G. (2017). The Architect's Role in Software Ecosystems Health. In Proceedings of the 2nd Workshop on Social, Human, and Economic Aspects of Software (pp. 1-4).

S101. Ribeiro, M. I. C., & Dias-Neto, A. C. (2017). Company health in mobile software ecosystem (mseco): Research perspectives and challenges. In 2017 IEEE/ACM Joint 5th International Workshop on Software Engineering for Systems-of-Systems and 11th Workshop on Distributed Software Development, Software Ecosystems and Systems-of-Systems (JSOS) (pp. 74-75). IEEE.

S102. Carvalho, I., Campos, F., Braga, R., David, J. M. N., Stroelle, V., & Araújo, M. A. (2017). HEAL ME-An Architecture for Health Software Ecosystem Evaluation. In 2017 IEEE/ACM Joint 5th International Workshop on Software Engineering for Systems-of-Systems and 11th Workshop on Distributed Software Development, Software Ecosystems and Systems-of-Systems (JSOS) (pp. 59-65). IEEE.

S103. Amorim, S. S., McGregor, J. D., de Almeida, E. S., & Chavez, C. F. G. (2017). Understanding the Effects of Practices on KDE Ecosystem Health. In IFIP International Conference on Open Source Systems (pp. 89-100). Springer, Cham.

S104. Amorim, S. S., de Almeida, E. S., McGregor, J. D., & Chavez, C. F. G. (2016). Towards an evaluation method for software ecosystem practices. In Proceedings of the 10th European Conference on Software Architecture Workshops (pp. 1-4).

S105. Bogart, C., Kästner, C., Herbsleb, J., & Thung, F. (2016). How to break an API: cost negotiation and community values in three software ecosystems. In Proceedings of the 2016 24th ACM SIGSOFT International Symposium on Foundations of Software Engineering (pp. 109-120).

S106. Amorim, S. S., McGregor, J. D., de Almeida, E. S., & Chavez, C. F. G. (2016). Software ecosystems architectural health: challenges x practices. In Proceedings of the 10th European Conference on Software Architecture Workshops (pp. 1-7).

S107. Saarni, K., & Kauppinen, M. (2019). Activities and Challenges in the Planning Phase of a Software Ecosystem. In International Conference on Software Business (pp. 71-85). Springer, Cham.

S108. Berkhout, M., van den Brink, F., van Zwienen, M., van Vulpen, P., & Jansen, S. (2018). Software ecosystem health of cryptocurrencies. In International Conference of Software Business (pp. 27-42). Springer, Cham.

S109. Fontão, A., Dias-Neto, A., & Santos, R. (2017). Towards a guideline-based approach to govern developers in mobile software ecosystems. In International Conference on Software Reuse (pp. 208-213). Springer, Cham.

B. Selected Studies in the Rapid Review

R1. Tello-Oquendo, L., Tapia, F., Fuertes, W., Andrade, R., Erazo, N. S., Torres, J., & Cadena, A. (2019). A Structured Approach to Guide the Development of Incident Management Capability for Security and Privacy. In ICEIS (2) (pp. 328-336).

R2. Fuada, S. (2019). Incident management of information technology in the indonesia higher education based on COBIT framework: A review. EAI Endorsed Transactions on Energy Web, 6(21).

R3. Nogueira, A. F., Sergeant, E., Craske, A., Ribeiro, J. C. B., & Zenha-Rela, M. A. (2019). Collecting Data from Continuous Practices: an Infrastructure to Support Team Development. In SEKE (pp. 687-777).

R4. do Amaral, C. A., Fantinato, M., & Peres, S. M. (2018, September). Attribute selection with filter and wrapper: an application on incident management process. In 2018 Federated Conference on Computer Science and Information Systems (FedCSIS) (pp. 679-682). IEEE.

R5. Raharjana, I. K., Ibadillah, I., & Hariyanti, E. (2018, October). Incident and Service Request Management for Academic Information System based on COBIT. In 2018 5th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI) (pp. 421-425). IEEE.

R6. Silva, S., Pereira, R., & Ribeiro, R. (2018, June). Machine learning in incident categorization automation. In 2018 13th Iberian Conference on Information Systems and Technologies (CISTI) (pp. 1-6). IEEE.

R7. Palilingan, V. R., & Batmetan, J. R. (2018, February). Incident management in academic information system using ITIL framework. In IOP Conference Series: Materials Science and Engineering (Vol. 306, No. 1, p. 012110). IOP Publishing.

R8. Belov, A. V., & Ulaeva, E. S. (2017, September). Mathematical model of incident management in the composite applications. In 2017 International Conference" Quality Management, Transport and Information Security, Information Technologies"(IT&QM&IS) (pp. 477-480). IEEE.

R9. Astuti, H. M., Muqtadiroh, F. A., Darmaningrat, E. W. T., & Putri, C. U. (2017). Risks assessment of information technology processes based on COBIT 5 framework: A case study of ITS service desk. Procedia Computer Science, 124, 569-576.

R10. Samopa, F., Astuti, H. M., & Lestari, M. A. (2017). The Development of Work Instruction as a Solution to Handle IT Critical Incidents in Units within an Organization. Procedia Computer Science, 124, 593-600.

R11. Maris, A., Bijvank, R., & Ravesteyn, P. (2016, June). The applicability of Process Mining to determine and align process model descriptions. In Bled eConference (p. 43).

R12. Goby, N., Brandt, T., Feuerriegel, S., & Neumann, D. (2016). Business intelligence for business processes: The case of IT incident management.

R13. Chen, Q., & Wan, X. P. (2014). Research and implementation of event handling of IT service. In Applied Mechanics and Materials (Vol. 513, pp. 2082-2085). Trans Tech Publications Ltd.

R14. Assunçao, M. D., Cavalcante, V. F., Gatti, M. A. D. C., Netto, M. A., Pinhanez, C. S., & de Souza, C. R. (2012, December). Scheduling with preemption for Incident Management: When interrupting tasks is not such a bad idea. In Proceedings of the 2012 Winter Simulation Conference (WSC) (pp. 1-12). IEEE.

R15. Kundu, G. K., Manohar, B. M., & Bairi, J. (2011, December). Incident management process capability: A simulation study. In International Conference on Computing and Communication Systems (pp. 243-255). Springer, Berlin, Heidelberg.

R16. Bartolini, C., Stefanelli, C., Targa, D., & Tortonesi, M. (2012, April). A cloud-based solution for the performance improvement of it support organizations. In 2012 IEEE Network Operations and Management Symposium (pp. 953-960). IEEE.

R17. Tchoffa, D., Duta, L., & El Mhamedi, A. (2012). Decision analysis in management of industrial incidents. IFAC Proceedings Volumes, 45(6), 951-955.

R18. Bartolini, C., Stefanelli, C., Targa, D., & Tortonesi, M. (2011, October). A web-based what-if scenario analysis tool for performance improvement of IT support organizations. In 2011 7th International Conference on Network and Service Management (pp. 1-5). IEEE.

R19 da Silva, R. N., da Silva, M. M., & Gama, N. (2010, October). Using People CMM for Dealing with Resistance on Implementing ITIL. In International Conference on ENTERprise Information Systems (pp. 259-263). Springer, Berlin, Heidelberg.

R20. Pereira, R., & da Silva, M. M. (2010, June). ITIL maturity model. In 5th Iberian Conference on Information Systems and Technologies (pp. 1-6). IEEE.

R21. Muhren, W. J., Van Den Eede, G., & de Walle, B. V. (2007). Organizational learning for the incident management process: Lessons from high reliability organizations.

R22. Van Den Eede, G., Muhren, W., Smals, R., & Van de Walle, B. (2006). IS capability for incident management and the DERMIS design premises. In Proceedings of the 3rd International Conference on Information Systems for Crisis Response and Management (ISCRAM) (May 14–17, Newark, New Jersey) (pp. 251-261).

R23. Bandara, W., Rosemann, M., & Cornes, J. (2005). Business process redesign in information technology incident management: A teaching case. ACIS 2005 Proceedings, 33-40.

C. Informed Consent Form (In Portuguese)

Ao responder a este questionário, você permite que os pesquisadores obtenham, usem e divulguem as informações geradas a partir dos dados agrupados conforme descrito abaixo.

CONDIÇÕES:

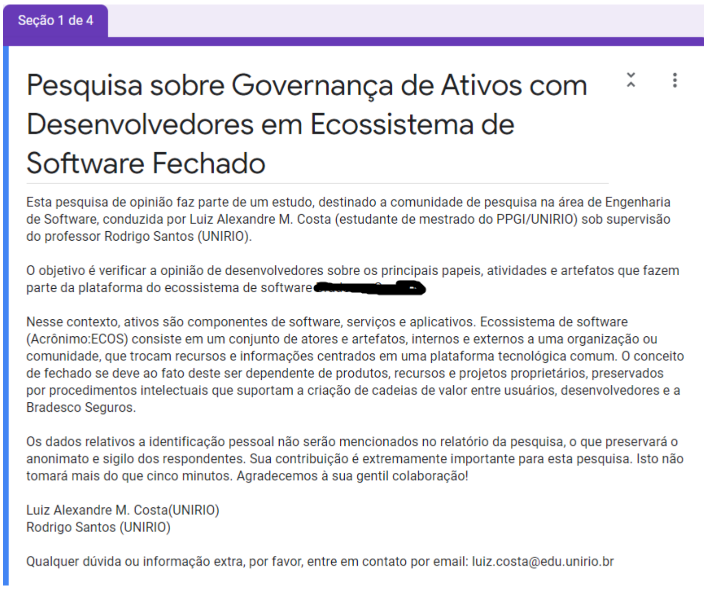
1. Eu entendo que todas as informações são confidenciais. Eu não serei pessoalmente identificado e concordo em concluir o questionário para fins de pesquisa. As informações derivadas dessa pesquisa anônima podem ser publicados em periódicos, conferências e publicações em blogs.

2. Entendo que minha participação nesta pesquisa é totalmente voluntária e que recusar participar não envolverá penalidade ou perda de benefícios. Se eu escolher, posso retirar minha participação a qualquer momento. Eu também entendo que, se eu optar por participar, posso me recusar a responder questões abertas as quais eu não me sinta confortável.

3. Entendo que posso entrar em contato com o pesquisador se tiver alguma dúvida sobre a pesquisa. Estou ciente de que meu consentimento não me beneficiará diretamente. Também estou ciente de que o autor manterá os dados de maneira agrupada, coletados em perpetuidade e poderá utilizá-los para trabalhos acadêmicos futuros.

4. Ao seguir para a próxima seção, eu livremente, reconheço meus direitos como participante voluntário(a) da pesquisa, conforme descrito acima, e forneço consentimento ao pesquisador para usar meus dados na condução de pesquisas sobre a área mencionada acima.

D. Survey on Software Asset Governance with Developers in Proprietary Software Ecosystem (In Portuguese)



Pesquisa sobre Governança de Ativos com Desenvolvedores em Ecossistema de Software Fechado

Esta pesquisa de opinião faz parte de um estudo, destinado a comunidade de pesquisa na área de Engenharia de Software, conduzida por Luiz Alexandre M. Costa (estudante de mestrado do PPGI/UNIRIO) sob supervisão do professor Rodrigo Santos (UNIRIO).

O objetivo é verificar a opinião de desenvolvedores sobre os principais papeis, atividades e artefatos que fazem parte da plataforma do ecossistema de software [redacted]

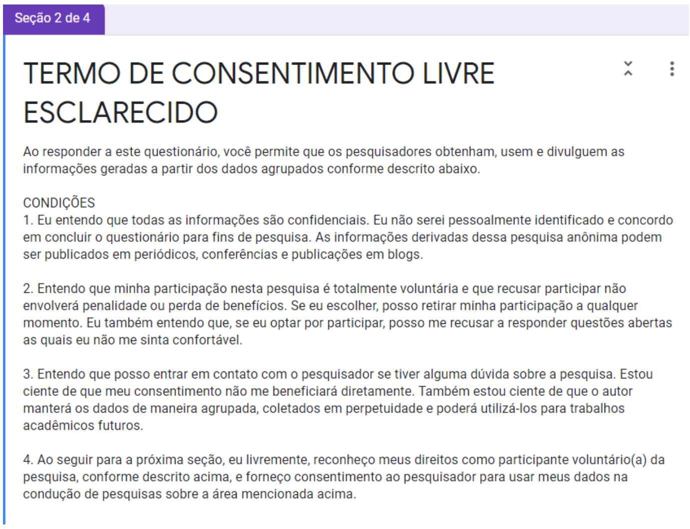
Nesse contexto, ativos são componentes de software, serviços e aplicativos. Ecossistema de software (Acrônimo:ECOS) consiste em um conjunto de atores e artefatos, internos e externos a uma organização ou comunidade, que trocam recursos e informações centrados em uma plataforma tecnológica comum. O conceito de fechado se deve ao fato deste ser dependente de produtos, recursos e projetos proprietários, preservados por procedimentos intelectuais que suportam a criação de cadeias de valor entre usuários, desenvolvedores e a Bradesco Seguros.

Os dados relativos a identificação pessoal não serão mencionados no relatório da pesquisa, o que preservará o anonimato e sigilo dos respondentes. Sua contribuição é extremamente importante para esta pesquisa. Isto não tomará mais do que cinco minutos. Agradecemos à sua gentil colaboração!

Luiz Alexandre M. Costa(UNIRIO)
Rodrigo Santos (UNIRIO)

Qualquer dúvida ou informação extra, por favor, entre em contato por email: luiz.costa@edu.unirio.br

Figure D.1: Introduction to survey *(sensitive data erased)*.



TERMO DE CONSENTIMENTO LIVRE ESCLARECIDO

Ao responder a este questionário, você permite que os pesquisadores obtenham, usem e divulguem as informações geradas a partir dos dados agrupados conforme descrito abaixo.

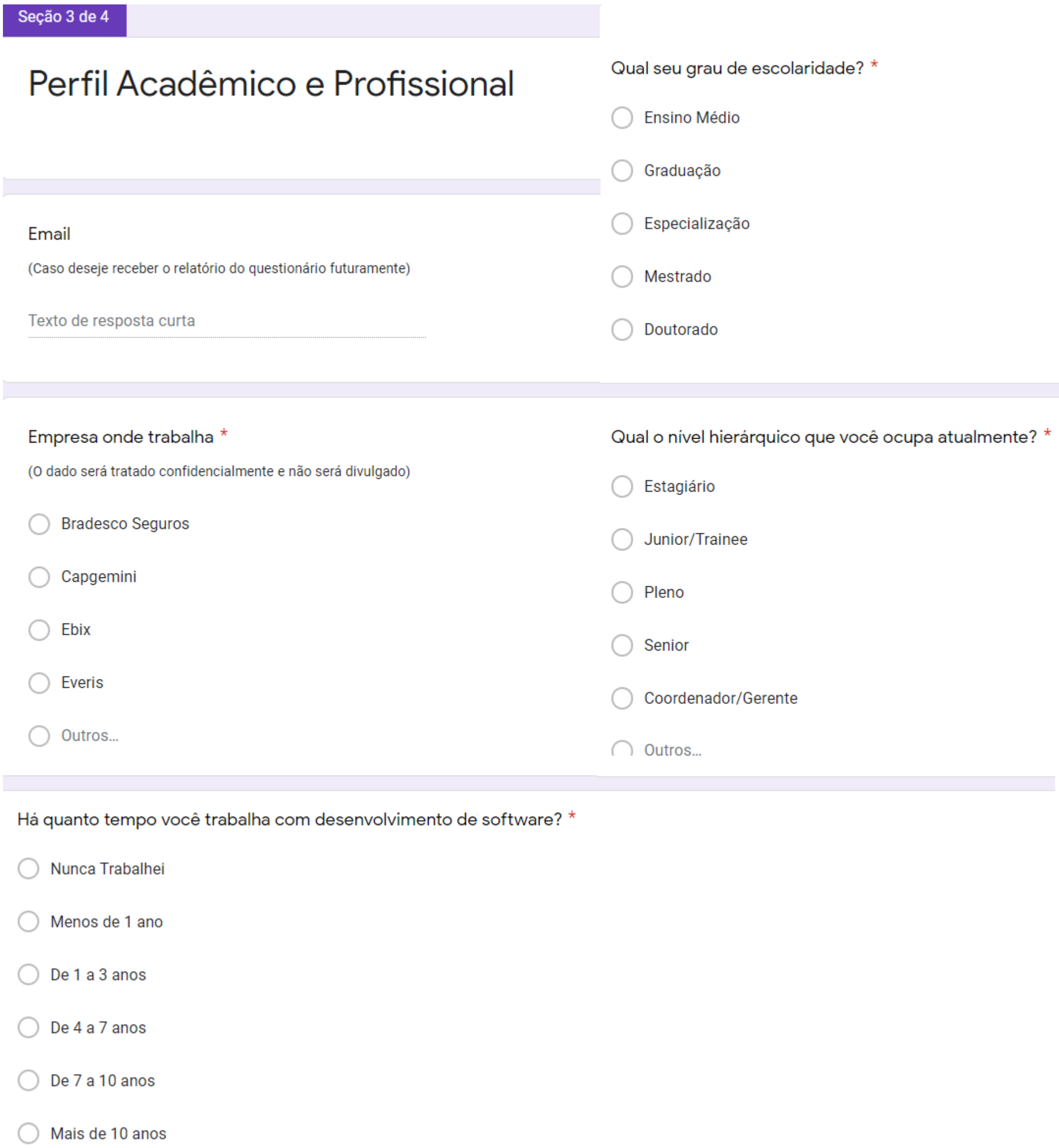
CONDIÇÕES
1. Eu entendo que todas as informações são confidenciais. Eu não serei pessoalmente identificado e concordo em concluir o questionário para fins de pesquisa. As informações derivadas dessa pesquisa anônima podem ser publicados em periódicos, conferências e publicações em blogs.

2. Entendo que minha participação nesta pesquisa é totalmente voluntária e que recusar participar não envolverá penalidade ou perda de benefícios. Se eu escolher, posso retirar minha participação a qualquer momento. Eu também entendo que, se eu optar por participar, posso me recusar a responder questões abertas as quais eu não me sinta confortável.

3. Entendo que posso entrar em contato com o pesquisador se tiver alguma dúvida sobre a pesquisa. Estou ciente de que meu consentimento não me beneficiará diretamente. Também estou ciente de que o autor manterá os dados de maneira agrupada, coletados em perpetuidade e poderá utilizá-los para trabalhos acadêmicos futuros.

4. Ao seguir para a próxima seção, eu livremente, reconheço meus direitos como participante voluntário(a) da pesquisa, conforme descrito acima, e forneço consentimento ao pesquisador para usar meus dados na condução de pesquisas sobre a área mencionada acima.

Figure D.2: Informed Consent Form.



Seção 3 de 4

Perfil Acadêmico e Profissional

Email

(Caso deseje receber o relatório do questionário futuramente)

Texto de resposta curta

Qual seu grau de escolaridade? *

○ Ensino Médio

○ Graduação

○ Especialização

○ Mestrado

○ Doutorado

Empresa onde trabalha *

(O dado será tratado confidencialmente e não será divulgado)

○ Bradesco Seguros

○ Capgemini

○ Ebix

○ Everis

○ Outros...

Qual o nível hierárquico que você ocupa atualmente? *

○ Estagiário

○ Junior/Trainee

○ Pleno

○ Senior

○ Coordenador/Gerente

○ Outros...

Há quanto tempo você trabalha com desenvolvimento de software? *

○ Nunca Trabalhei

○ Menos de 1 ano

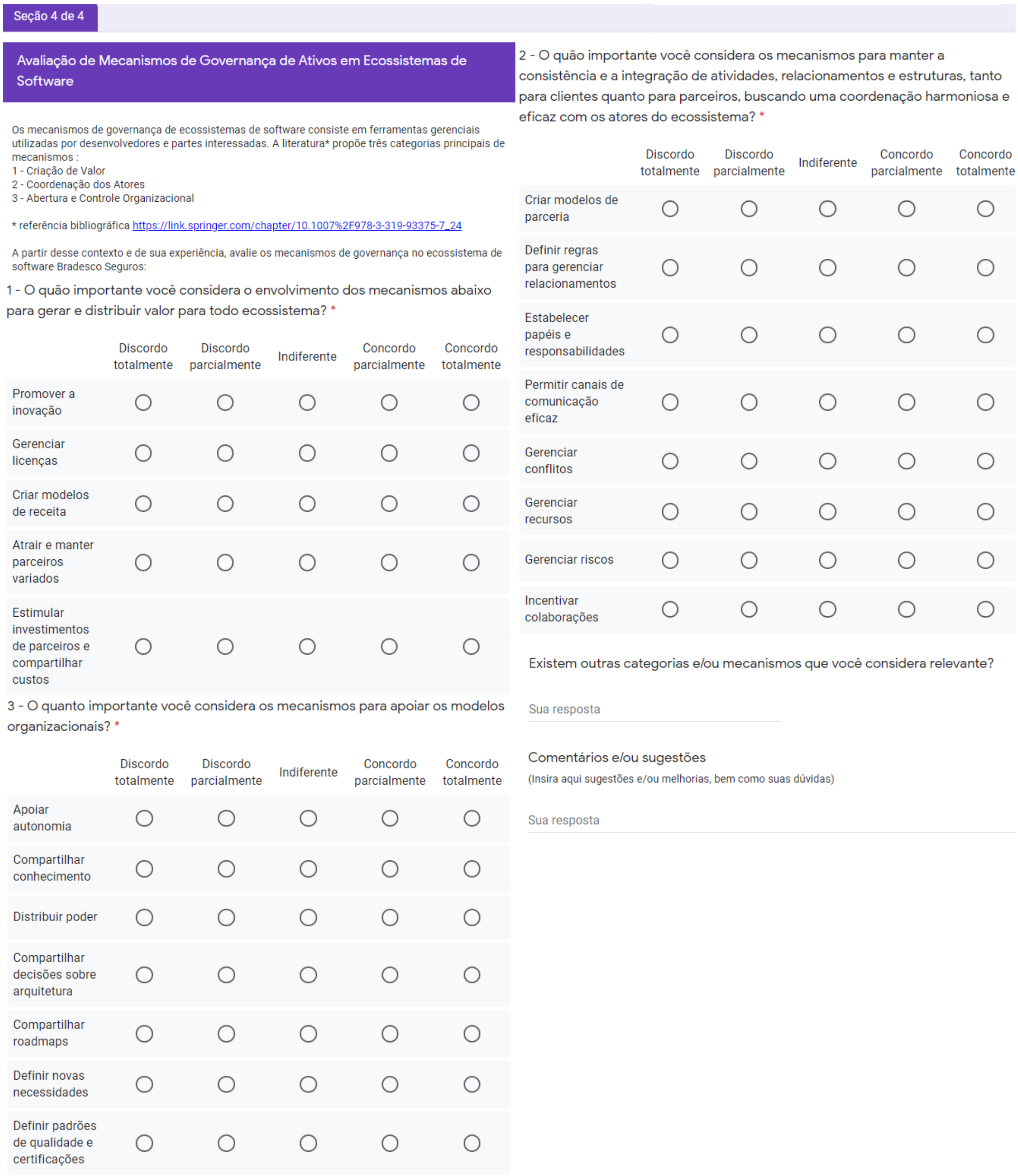
○ De 1 a 3 anos

○ De 4 a 7 anos

○ De 7 a 10 anos

○ Mais de 10 anos

Figure D.3: Professional profile.



Seção 4 de 4

Avaliação de Mecanismos de Governança de Ativos em Ecossistemas de Software

Os mecanismos de governança de ecossistemas de software consiste em ferramentas gerenciais utilizadas por desenvolvedores e partes interessadas. A literatura* propõe três categorias principais de mecanismos :
1 - Criação de Valor
2 - Coordenação dos Atores
3 - Abertura e Controle Organizacional

* referência bibliográfica https://link.springer.com/chapter/10.1007%2F978-3-319-93375-7_24

A partir desse contexto e de sua experiência, avalie os mecanismos de governança no ecossistema de software Bradesco Seguros:

1 - O quão importante você considera o envolvimento dos mecanismos abaixo para gerar e distribuir valor para todo ecossistema? *

	Discordo totalmente	Discordo parcialmente	Indiferente	Concordo parcialmente	Concordo totalmente
Promover a inovação	○	○	○	○	○
Gerenciar licenças	○	○	○	○	○
Criar modelos de receita	○	○	○	○	○
Atrair e manter parceiros variados	○	○	○	○	○
Estimular investimentos de parceiros e compartilhar custos	○	○	○	○	○

3 - O quanto importante você considera os mecanismos para apoiar os modelos organizacionais? *

	Discordo totalmente	Discordo parcialmente	Indiferente	Concordo parcialmente	Concordo totalmente
Apoiar autonomia	○	○	○	○	○
Compartilhar conhecimento	○	○	○	○	○
Distribuir poder	○	○	○	○	○
Compartilhar decisões sobre arquitetura	○	○	○	○	○
Compartilhar roadmaps	○	○	○	○	○
Definir novas necessidades	○	○	○	○	○
Definir padrões de qualidade e certificações	○	○	○	○	○

2 - O quão importante você considera os mecanismos para manter a consistência e a integração de atividades, relacionamentos e estruturas, tanto para clientes quanto para parceiros, buscando uma coordenação harmoniosa e eficaz com os atores do ecossistema? *

	Discordo totalmente	Discordo parcialmente	Indiferente	Concordo parcialmente	Concordo totalmente
Criar modelos de parceria	○	○	○	○	○
Definir regras para gerenciar relacionamentos	○	○	○	○	○
Estabelecer papéis e responsabilidades	○	○	○	○	○
Permitir canais de comunicação eficaz	○	○	○	○	○
Gerenciar conflitos	○	○	○	○	○
Gerenciar recursos	○	○	○	○	○
Gerenciar riscos	○	○	○	○	○
Incentivar colaborações	○	○	○	○	○

Existem outras categorias e/ou mecanismos que você considera relevante?

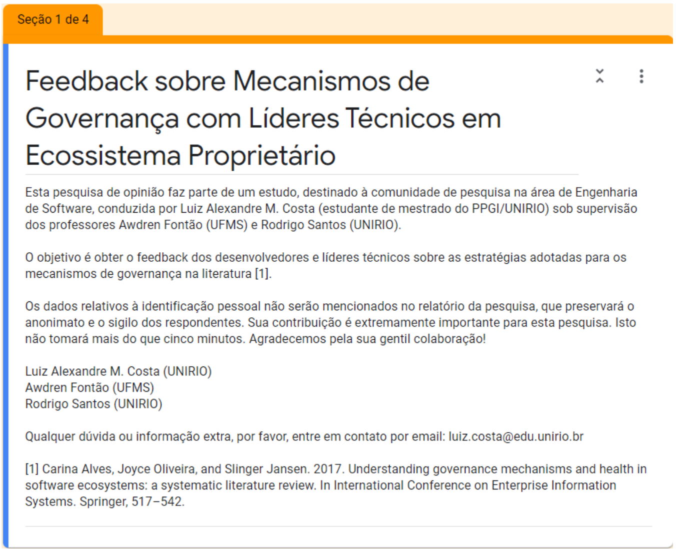
Sua resposta

Comentários e/ou sugestões
(Insira aqui sugestões e/ou melhorias, bem como suas dúvidas)

Sua resposta

Figure D.4: Assessment of asset governance mechanisms in SECO.

E. Feedback Survey on the Governance Mechanisms from Technical Leaders on Proprietary Ecosystem (In Portuguese)



Feedback sobre Mecanismos de Governança com Líderes Técnicos em Ecossistema Proprietário

Esta pesquisa de opinião faz parte de um estudo, destinado à comunidade de pesquisa na área de Engenharia de Software, conduzida por Luiz Alexandre M. Costa (estudante de mestrado do PPGI/UNIRIO) sob supervisão dos professores Awdren Fontão (UFMS) e Rodrigo Santos (UNIRIO).

O objetivo é obter o feedback dos desenvolvedores e líderes técnicos sobre as estratégias adotadas para os mecanismos de governança na literatura [1].

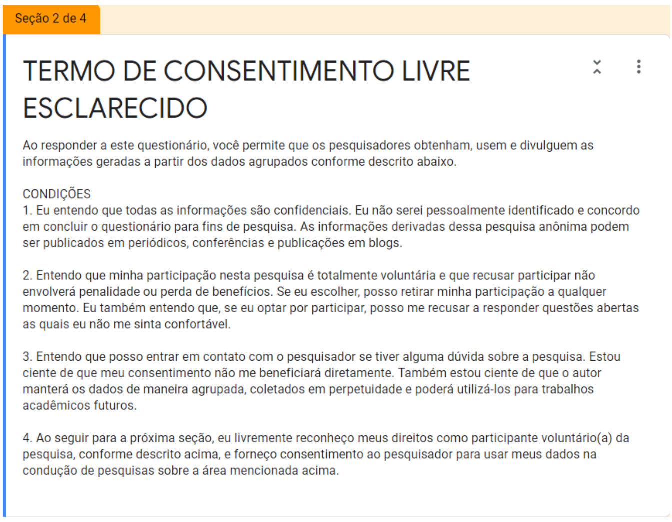
Os dados relativos à identificação pessoal não serão mencionados no relatório da pesquisa, que preservará o anonimato e o sigilo dos respondentes. Sua contribuição é extremamente importante para esta pesquisa. Isto não tomará mais do que cinco minutos. Agradecemos pela sua gentil colaboração!

Luiz Alexandre M. Costa (UNIRIO)
Awdren Fontão (UFMS)
Rodrigo Santos (UNIRIO)

Qualquer dúvida ou informação extra, por favor, entre em contato por email: luiz.costa@edu.unirio.br

[1] Carina Alves, Joyce Oliveira, and Slinger Jansen. 2017. Understanding governance mechanisms and health in software ecosystems: a systematic literature review. In International Conference on Enterprise Information Systems. Springer, 517–542.

Figure E.1: Introduction to survey.



TERMO DE CONSENTIMENTO LIVRE ESCLARECIDO

Ao responder a este questionário, você permite que os pesquisadores obtenham, usem e divulguem as informações geradas a partir dos dados agrupados conforme descrito abaixo.

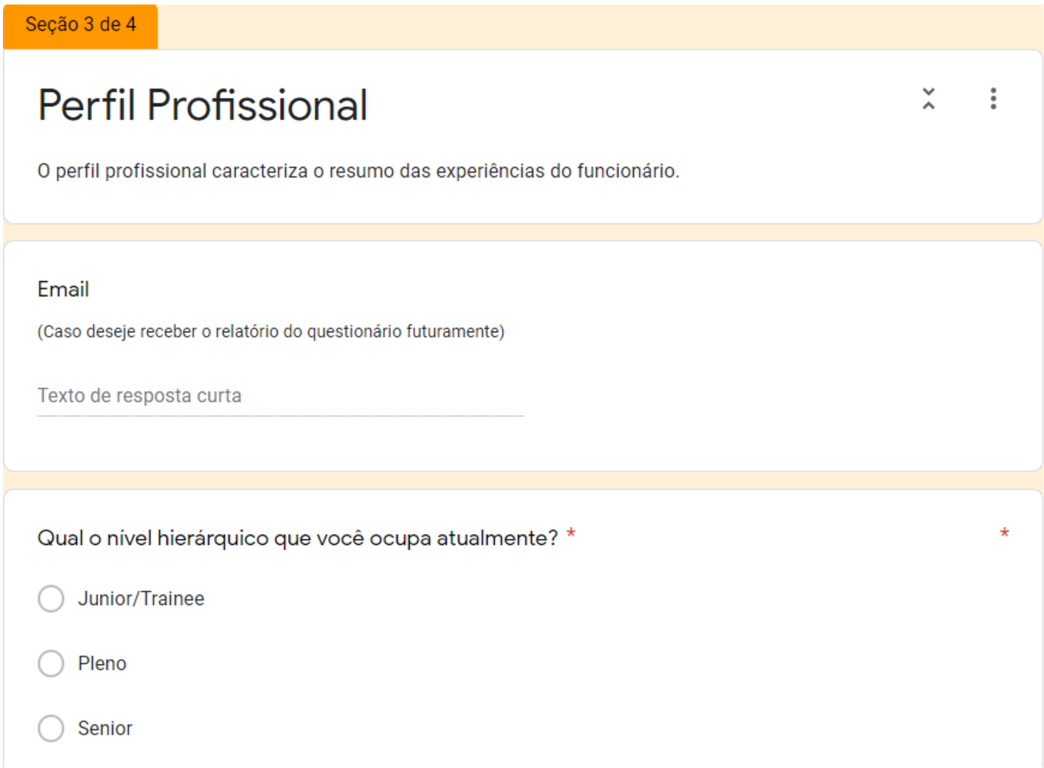
CONDIÇÕES
1. Eu entendo que todas as informações são confidenciais. Eu não serei pessoalmente identificado e concordo em concluir o questionário para fins de pesquisa. As informações derivadas dessa pesquisa anônima podem ser publicados em periódicos, conferências e publicações em blogs.

2. Entendo que minha participação nesta pesquisa é totalmente voluntária e que recusar participar não envolverá penalidade ou perda de benefícios. Se eu escolher, posso retirar minha participação a qualquer momento. Eu também entendo que, se eu optar por participar, posso me recusar a responder questões abertas as quais eu não me sinta confortável.

3. Entendo que posso entrar em contato com o pesquisador se tiver alguma dúvida sobre a pesquisa. Estou ciente de que meu consentimento não me beneficiará diretamente. Também estou ciente de que o autor manterá os dados de maneira agrupada, coletados em perpetuidade e poderá utilizá-los para trabalhos acadêmicos futuros.

4. Ao seguir para a próxima seção, eu livremente reconheço meus direitos como participante voluntário(a) da pesquisa, conforme descrito acima, e forneço consentimento ao pesquisador para usar meus dados na condução de pesquisas sobre a área mencionada acima.

Figure E.2: Informed Consent Form.



Seção 3 de 4

Perfil Profissional

O perfil profissional caracteriza o resumo das experiências do funcionário.

Email

(Caso deseje receber o relatório do questionário futuramente)

Texto de resposta curta

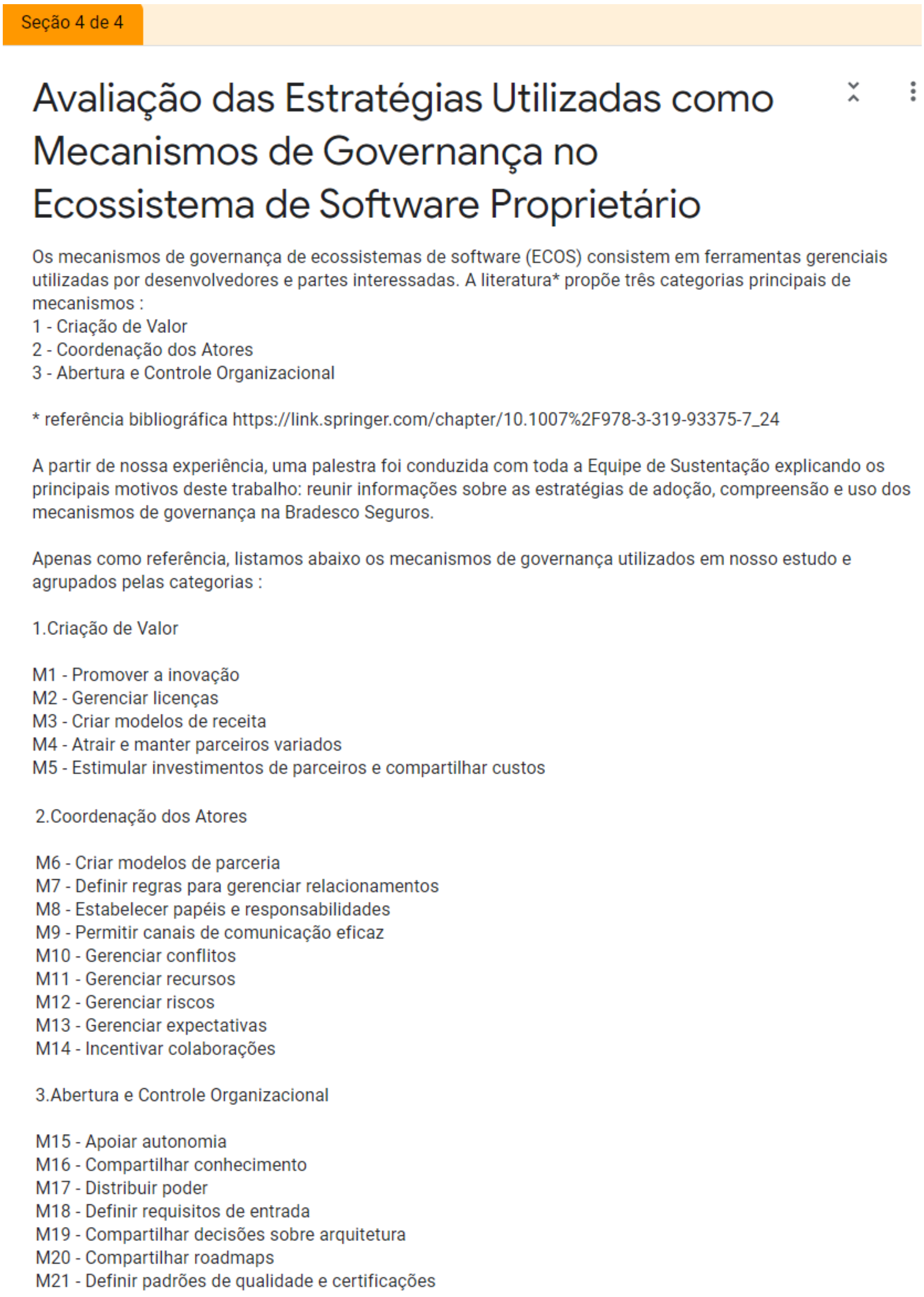
Qual o nível hierárquico que você ocupa atualmente? *

○ Junior/Trainee

○ Pleno

○ Senior

Figure E.3: Professional profile.



Avaliação das Estratégias Utilizadas como Mecanismos de Governança no Ecossistema de Software Proprietário

Os mecanismos de governança de ecossistemas de software (ECOS) consistem em ferramentas gerenciais utilizadas por desenvolvedores e partes interessadas. A literatura* propõe três categorias principais de mecanismos :
1 - Criação de Valor
2 - Coordenação dos Atores
3 - Abertura e Controle Organizacional

* referência bibliográfica https://link.springer.com/chapter/10.1007%2F978-3-319-93375-7_24

A partir de nossa experiência, uma palestra foi conduzida com toda a Equipe de Sustentação explicando os principais motivos deste trabalho: reunir informações sobre as estratégias de adoção, compreensão e uso dos mecanismos de governança na Bradesco Seguros.

Apenas como referência, listamos abaixo os mecanismos de governança utilizados em nosso estudo e agrupados pelas categorias :

1.Criação de Valor

M1 - Promover a inovação
M2 - Gerenciar licenças
M3 - Criar modelos de receita
M4 - Atrair e manter parceiros variados
M5 - Estimular investimentos de parceiros e compartilhar custos

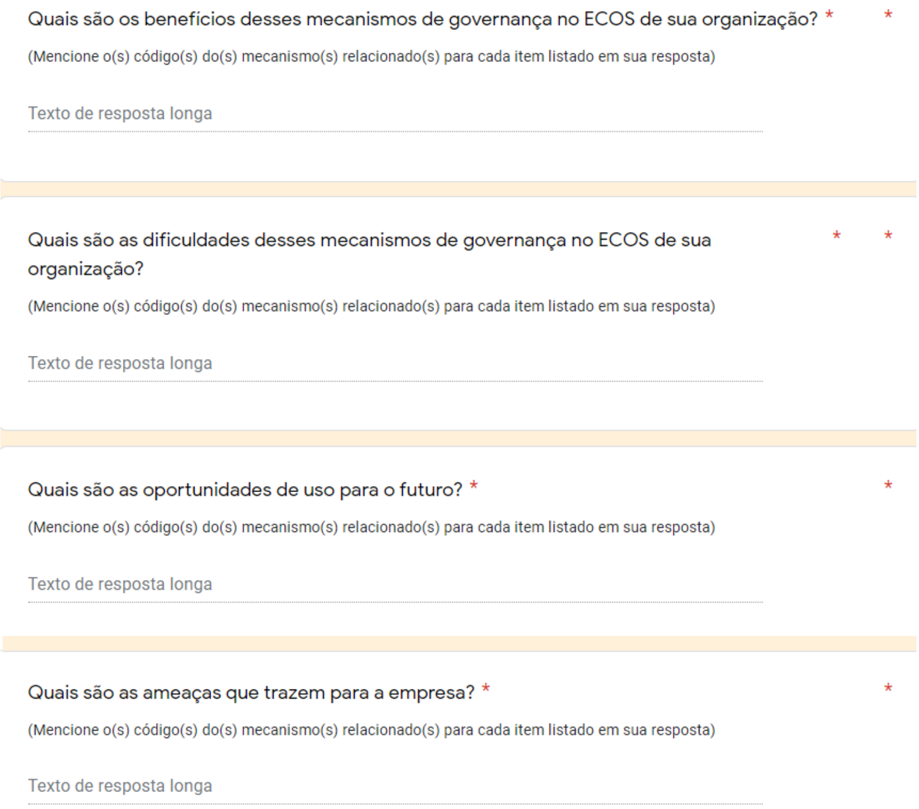
2.Coordenação dos Atores

M6 - Criar modelos de parceria
M7 - Definir regras para gerenciar relacionamentos
M8 - Estabelecer papéis e responsabilidades
M9 - Permitir canais de comunicação eficaz
M10 - Gerenciar conflitos
M11 - Gerenciar recursos
M12 - Gerenciar riscos
M13 - Gerenciar expectativas
M14 - Incentivar colaborações

3.Abertura e Controle Organizacional

M15 - Apoiar autonomia
M16 - Compartilhar conhecimento
M17 - Distribuir poder
M18 - Definir requisitos de entrada
M19 - Compartilhar decisões sobre arquitetura
M20 - Compartilhar roadmaps
M21 - Definir padrões de qualidade e certificações

Figure E.4: Assessment of strategies used as governance mechanisms in the proprietary SECO.



Quais são os benefícios desses mecanismos de governança no ECOS de sua organização? * *

(Mencione o(s) código(s) do(s) mecanismo(s) relacionado(s) para cada item listado em sua resposta)

Texto de resposta longa

Quais são as dificuldades desses mecanismos de governança no ECOS de sua organização? * *

(Mencione o(s) código(s) do(s) mecanismo(s) relacionado(s) para cada item listado em sua resposta)

Texto de resposta longa

Quais são as oportunidades de uso para o futuro? * *

(Mencione o(s) código(s) do(s) mecanismo(s) relacionado(s) para cada item listado em sua resposta)

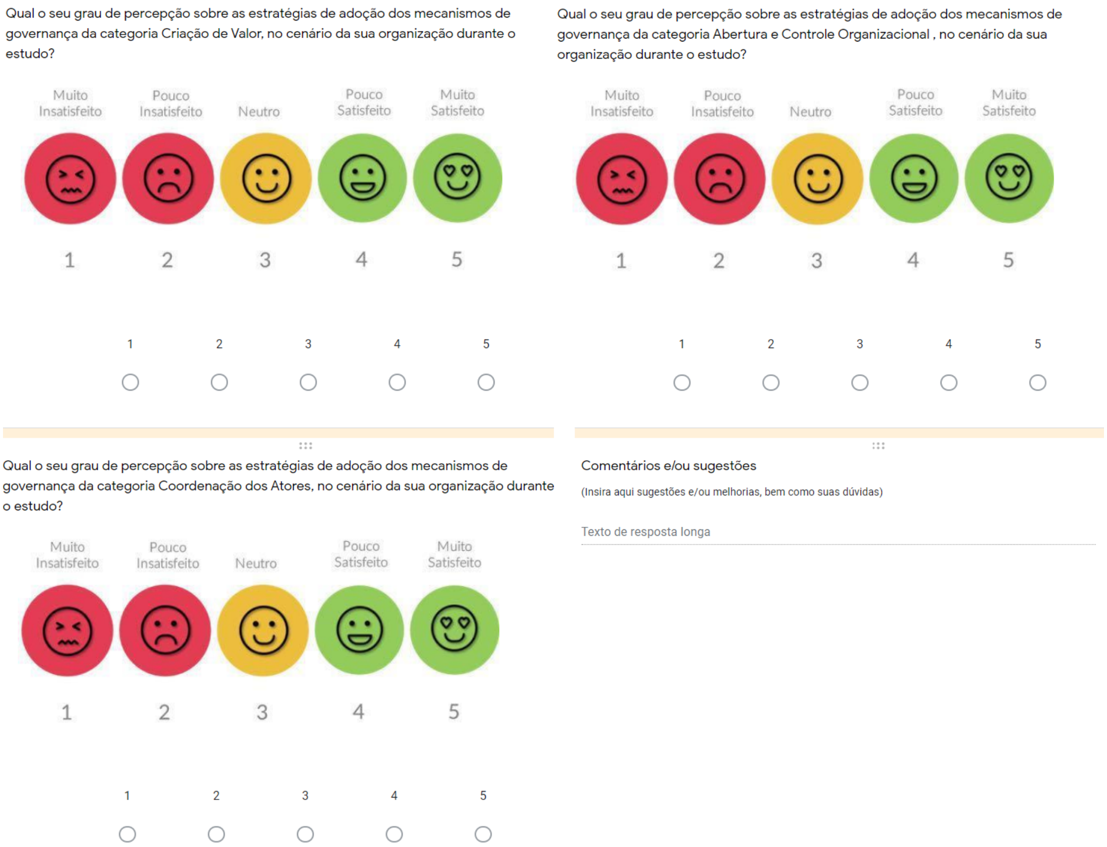
Texto de resposta longa

Quais são as ameaças que trazem para a empresa? * *

(Mencione o(s) código(s) do(s) mecanismo(s) relacionado(s) para cada item listado em sua resposta)

Texto de resposta longa

Figure E.5: Open questions about strategies used.



Qual o seu grau de percepção sobre as estratégias de adoção dos mecanismos de governança da categoria Criação de Valor, no cenário da sua organização durante o estudo?

1	2	3	4	5
○	○	○	○	○

Qual o seu grau de percepção sobre as estratégias de adoção dos mecanismos de governança da categoria Abertura e Controle Organizacional , no cenário da sua organização durante o estudo?

1	2	3	4	5
○	○	○	○	○

Qual o seu grau de percepção sobre as estratégias de adoção dos mecanismos de governança da categoria Coordenação dos Atores, no cenário da sua organização durante o estudo?

1	2	3	4	5
○	○	○	○	○

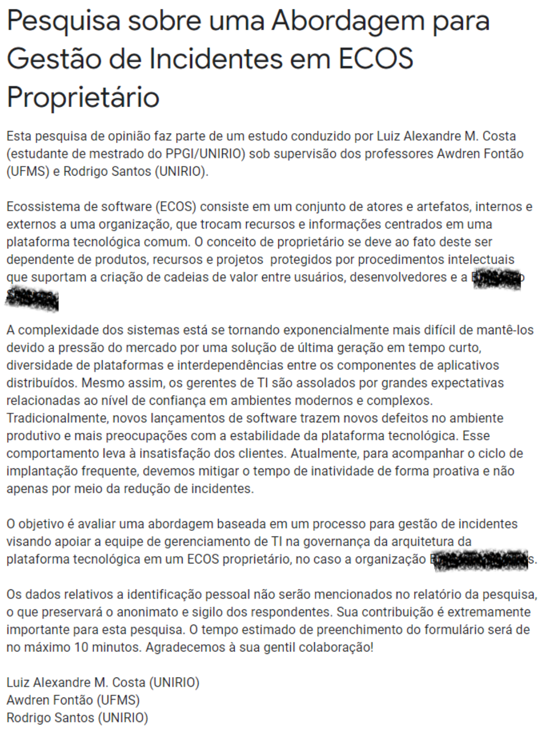
Comentários e/ou sugestões

(Insira aqui sugestões e/ou melhorias, bem como suas dúvidas)

Texto de resposta longa

Figure E.6: Visual Analogue Scale.

F. Feedback survey on the Approach to Incident Management in Proprietary SECO (In Portuguese)



Pesquisa sobre uma Abordagem para Gestão de Incidentes em ECOS Proprietário

Esta pesquisa de opinião faz parte de um estudo conduzido por Luiz Alexandre M. Costa (estudante de mestrado do PPGI/UNIRIO) sob supervisão dos professores Awdren Fontão (UFMS) e Rodrigo Santos (UNIRIO).

Ecossistema de software (ECOS) consiste em um conjunto de atores e artefatos, internos e externos a uma organização, que trocam recursos e informações centrados em uma plataforma tecnológica comum. O conceito de proprietário se deve ao fato deste ser dependente de produtos, recursos e projetos protegidos por procedimentos intelectuais que suportam a criação de cadeias de valor entre usuários, desenvolvedores e a [redacted]

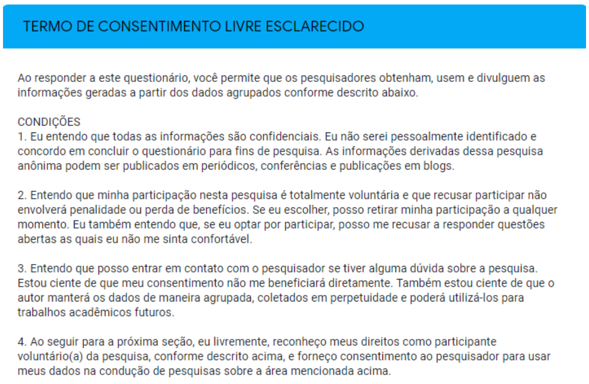
A complexidade dos sistemas está se tornando exponencialmente mais difícil de mantê-los devido a pressão do mercado por uma solução de última geração em tempo curto, diversidade de plataformas e interdependências entre os componentes de aplicativos distribuídos. Mesmo assim, os gerentes de TI são assolados por grandes expectativas relacionadas ao nível de confiança em ambientes modernos e complexos. Tradicionalmente, novos lançamentos de software trazem novos defeitos no ambiente produtivo e mais preocupações com a estabilidade da plataforma tecnológica. Esse comportamento leva à insatisfação dos clientes. Atualmente, para acompanhar o ciclo de implantação frequente, devemos mitigar o tempo de inatividade de forma proativa e não apenas por meio da redução de incidentes.

O objetivo é avaliar uma abordagem baseada em um processo para gestão de incidentes visando apoiar a equipe de gerenciamento de TI na governança da arquitetura da plataforma tecnológica em um ECOS proprietário, no caso a organização [redacted]s.

Os dados relativos a identificação pessoal não serão mencionados no relatório da pesquisa, o que preservará o anonimato e sigilo dos respondentes. Sua contribuição é extremamente importante para esta pesquisa. O tempo estimado de preenchimento do formulário será de no máximo 10 minutos. Agradecemos à sua gentil colaboração!

Luiz Alexandre M. Costa (UNIRIO)
Awdren Fontão (UFMS)
Rodrigo Santos (UNIRIO)

Figure F.1: Introduction to survey *(sensitive data erased).*



TERMO DE CONSENTIMENTO LIVRE ESCLARECIDO

Ao responder a este questionário, você permite que os pesquisadores obtenham, usem e divulguem as informações geradas a partir dos dados agrupados conforme descrito abaixo.

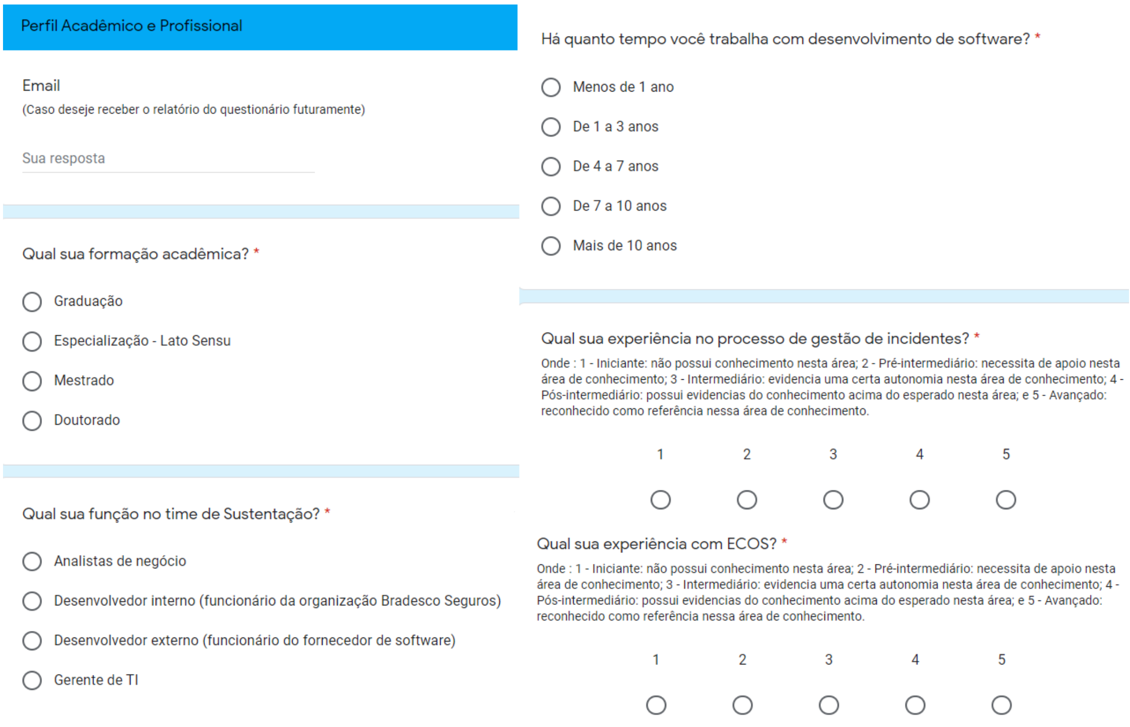
CONDIÇÕES
1. Eu entendo que todas as informações são confidenciais. Eu não serei pessoalmente identificado e concordo em concluir o questionário para fins de pesquisa. As informações derivadas dessa pesquisa anônima podem ser publicados em periódicos, conferências e publicações em blogs.

2. Entendo que minha participação nesta pesquisa é totalmente voluntária e que recusar participar não envolverá penalidade ou perda de benefícios. Se eu escolher, posso retirar minha participação a qualquer momento. Eu também entendo que, se eu optar por participar, posso me recusar a responder questões abertas as quais eu não me sinta confortável.

3. Entendo que posso entrar em contato com o pesquisador se tiver alguma dúvida sobre a pesquisa. Estou ciente de que meu consentimento não me beneficiará diretamente. Também estou ciente de que o autor manterá os dados de maneira agrupada, coletados em perpetuidade e poderá utilizá-los para trabalhos acadêmicos futuros.

4. Ao seguir para a próxima seção, eu livremente, reconheço meus direitos como participante voluntário(a) da pesquisa, conforme descrito acima, e forneço consentimento ao pesquisador para usar meus dados na condução de pesquisas sobre a área mencionada acima.

Figure F.2: Informed Consent Form.



Perfil Acadêmico e Profissional

Email
(Caso deseje receber o relatório do questionário futuramente)

Sua resposta

Qual sua formação acadêmica? *

○ Graduação
○ Especialização - Lato Sensu
○ Mestrado
○ Doutorado

Qual sua função no time de Sustentação? *

○ Analistas de negócio
○ Desenvolvedor interno (funcionário da organização Bradesco Seguros)
○ Desenvolvedor externo (funcionário do fornecedor de software)
○ Gerente de TI

Há quanto tempo você trabalha com desenvolvimento de software? *

○ Menos de 1 ano
○ De 1 a 3 anos
○ De 4 a 7 anos
○ De 7 a 10 anos
○ Mais de 10 anos

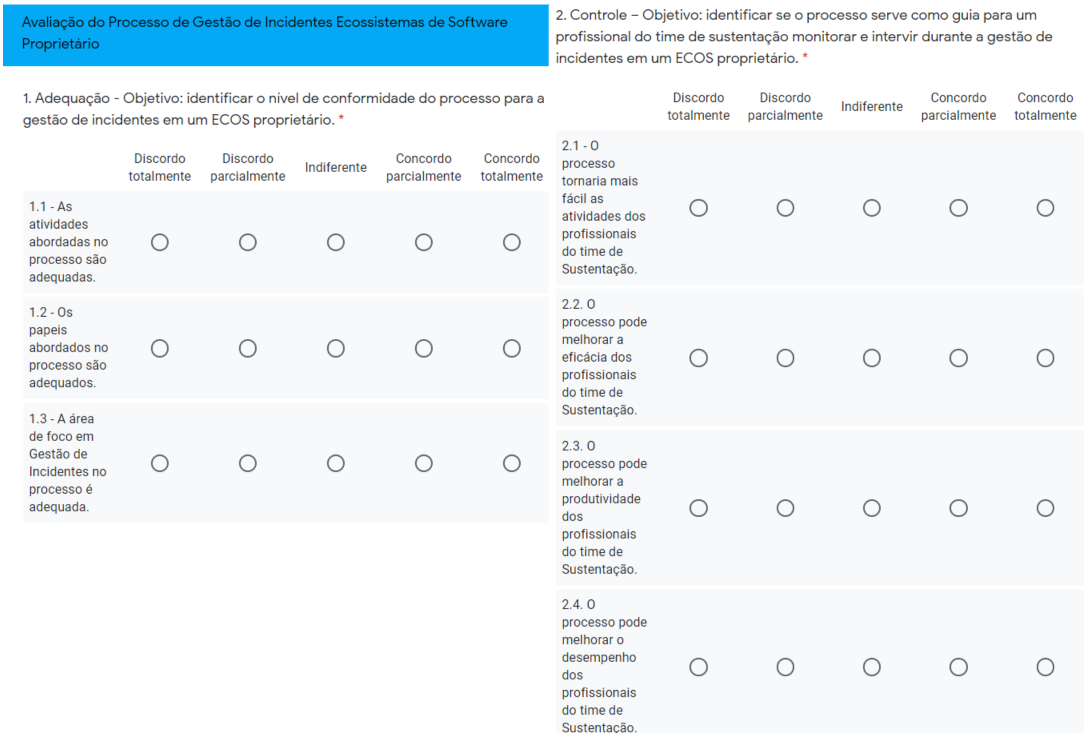
Qual sua experiência no processo de gestão de incidentes? *
Onde : 1 - Iniciante: não possui conhecimento nesta área; 2 - Pré-intermediário: necessita de apoio nesta área de conhecimento; 3 - Intermediário: evidencia uma certa autonomia nesta área de conhecimento; 4 - Pós-intermediário: possui evidencias do conhecimento acima do esperado nesta área; e 5 - Avançado: reconhecido como referência nessa área de conhecimento.

1	2	3	4	5
○	○	○	○	○

Qual sua experiência com ECOS? *
Onde : 1 - Iniciante: não possui conhecimento nesta área; 2 - Pré-intermediário: necessita de apoio nesta área de conhecimento; 3 - Intermediário: evidencia uma certa autonomia nesta área de conhecimento; 4 - Pós-intermediário: possui evidencias do conhecimento acima do esperado nesta área; e 5 - Avançado: reconhecido como referência nessa área de conhecimento.

1	2	3	4	5
○	○	○	○	○

Figure F.3: Professional profile.



Avaliação do Processo de Gestão de Incidentes Ecossistemas de Software Proprietário

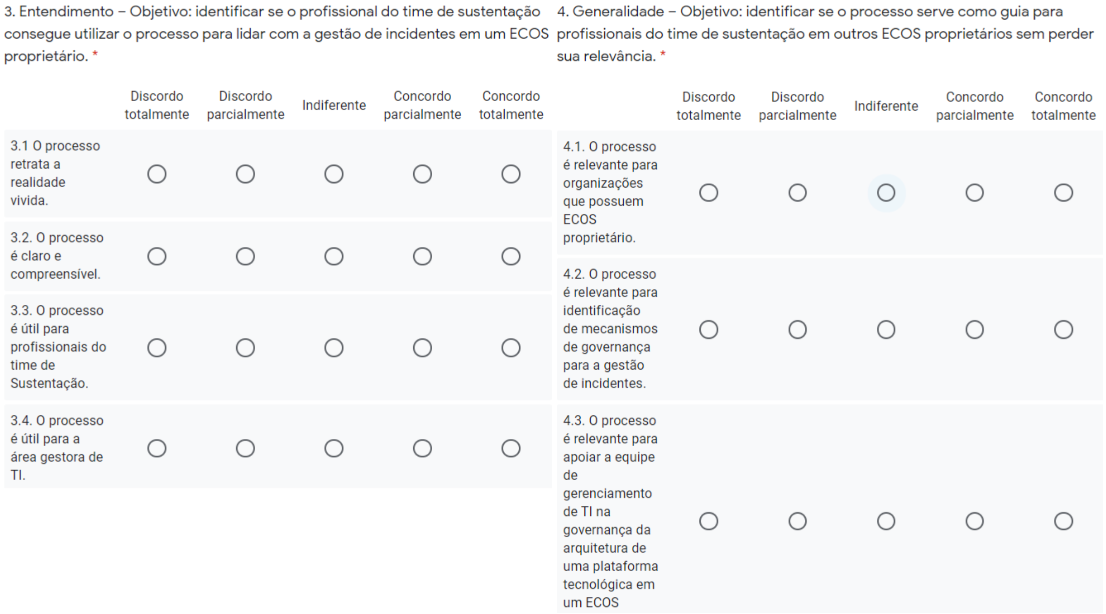
1. Adequação - Objetivo: identificar o nivel de conformidade do processo para a gestão de incidentes em um ECOS proprietário. *

	Discordo totalmente	Discordo parcialmente	Indiferente	Concordo parcialmente	Concordo totalmente
1.1 - As atividades abordadas no processo são adequadas.	○	○	○	○	○
1.2 - Os papeis abordados no processo são adequados.	○	○	○	○	○
1.3 - A área de foco em Gestão de Incidentes no processo é adequada.	○	○	○	○	○

2. Controle – Objetivo: identificar se o processo serve como guia para um profissional do time de sustentação monitorar e intervir durante a gestão de incidentes em um ECOS proprietário. *

	Discordo totalmente	Discordo parcialmente	Indiferente	Concordo parcialmente	Concordo totalmente
2.1 - O processo tornaria mais fácil as atividades dos profissionais do time de Sustentação.	○	○	○	○	○
2.2. O processo pode melhorar a eficácia dos profissionais do time de Sustentação.	○	○	○	○	○
2.3. O processo pode melhorar a produtividade dos profissionais do time de Sustentação.	○	○	○	○	○
2.4. O processo pode melhorar o desempenho dos profissionais do time de Sustentação.	○	○	○	○	○

Figure F.4: Incident management process assessment in proprietary SECO.



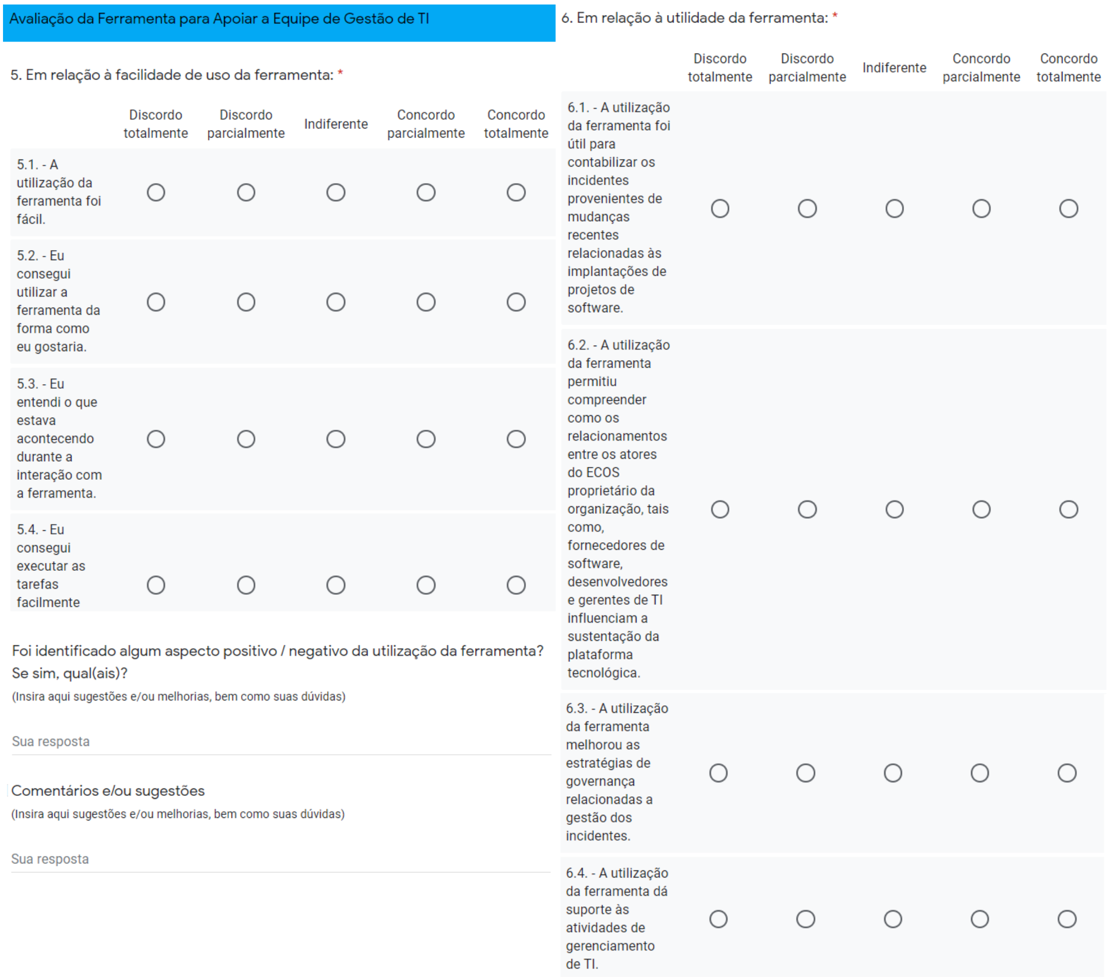
3. Entendimento – Objetivo: identificar se o profissional do time de sustentação consegue utilizar o processo para lidar com a gestão de incidentes em um ECOS proprietário. *

	Discordo totalmente	Discordo parcialmente	Indiferente	Concordo parcialmente	Concordo totalmente
3.1 O processo retrata a realidade vivida.	○	○	○	○	○
3.2. O processo é claro e compreensível.	○	○	○	○	○
3.3. O processo é útil para profissionais do time de Sustentação.	○	○	○	○	○
3.4. O processo é útil para a área gestora de TI.	○	○	○	○	○

4. Generalidade – Objetivo: identificar se o processo serve como guia para profissionais do time de sustentação em outros ECOS proprietários sem perder sua relevância. *

	Discordo totalmente	Discordo parcialmente	Indiferente	Concordo parcialmente	Concordo totalmente
4.1. O processo é relevante para organizações que possuem ECOS proprietário.	○	○	○	○	○
4.2. O processo é relevante para identificação de mecanismos de governança para a gestão de incidentes.	○	○	○	○	○
4.3. O processo é relevante para apoiar a equipe de gerenciamento de TI na governança da arquitetura de uma plataforma tecnológica em um ECOS	○	○	○	○	○

Figure F.5: Incident management process assessment in proprietary SECO.



Avaliação da Ferramenta para Apoiar a Equipe de Gestão de TI

5. Em relação à facilidade de uso da ferramenta: *

	Discordo totalmente	Discordo parcialmente	Indiferente	Concordo parcialmente	Concordo totalmente
5.1. - A utilização da ferramenta foi fácil.	○	○	○	○	○
5.2. - Eu consegui utilizar a ferramenta da forma como eu gostaria.	○	○	○	○	○
5.3. - Eu entendi o que estava acontecendo durante a interação com a ferramenta.	○	○	○	○	○
5.4. - Eu consegui executar as tarefas facilmente	○	○	○	○	○

Foi identificado algum aspecto positivo / negativo da utilização da ferramenta? Se sim, qual(ais)?

(Insira aqui sugestões e/ou melhorias, bem como suas dúvidas)

Sua resposta

Comentários e/ou sugestões

(Insira aqui sugestões e/ou melhorias, bem como suas dúvidas)

Sua resposta

6. Em relação à utilidade da ferramenta: *

	Discordo totalmente	Discordo parcialmente	Indiferente	Concordo parcialmente	Concordo totalmente
6.1. - A utilização da ferramenta foi útil para contabilizar os incidentes provenientes de mudanças recentes relacionadas às implantações de projetos de software.	○	○	○	○	○
6.2. - A utilização da ferramenta permitiu compreender como os relacionamentos entre os atores do ECOS proprietário da organização, tais como, fornecedores de software, desenvolvedores e gerentes de TI influenciam a sustentação da plataforma tecnológica.	○	○	○	○	○
6.3. - A utilização da ferramenta melhorou as estratégias de governança relacionadas a gestão dos incidentes.	○	○	○	○	○
6.4. - A utilização da ferramenta dá suporte às atividades de gerenciamento de TI.	○	○	○	○	○

Figure F.6: Assessment of the tool to support the IT management team.