



Department of Science and Information Technology

Maturity Model of Incident Management

João Filipe Ferreira Aguiar
Nº66810

A Thesis presented in partial fulfillment of the Requirements for the degree of
Master in Information Technology and Management

Supervisor:
Prof. Ph. D. Ruben Pereira
ISCTE-IUL

September, 2017



Department of Science and Information Technology

Maturity Model of Incident Management

João Filipe Ferreira Aguiar
Nº66810

A Thesis presented in partial fulfillment of the Requirements for the degree of
Master in Information Technology and Management

Supervisor:
Prof. Ph. D. Ruben Pereira
ISCTE-IUL

September, 2017

Acknowledgements

Since September of 2016 when I start this thesis, I had the pleasure of learn and collaborate with several people. All of them helped me to develop my skills.

First, I would like to thank to my supervisor, Professor Rúben Pereira, for all the effort and availability dedicated to this thesis. The weekly situation points gave me working guidelines which was very useful. Thank you once again, for all the time you spent with me.

Thanks to all the people of organizations that collaborated with this thesis. The priceless time spent to evaluate their process was very useful to this investigation.

I would also like to thank to my closest family. To my parents, my sisters, my brothers-in-law, nephews and parents-in-law for all the help they gave me and for the moments that I gave up of their company to work on this thesis.

Last but not least, I would like to thank to my fiancée, Ondina Aguiar, who supported me all the time. Without her loving support and help I would have never been able to accomplish this thesis.

Título: Modelo de Maturidade para a Gestão de Incidências

Nome: João Filipe Ferreira Aguiar

Mestrado em: Informática e Gestão

Orientador: Doutor Rúben Filipe de Sousa Pereira

Resumo

Nos últimos 25 anos a preocupação da generalidade das empresas com as Tecnologias da Informação (TI) é claramente exponencial. De tal forma que, para conseguirem organizar, planear, seleccionar, suportar e entregar os serviços de TI, foi necessário implementar *frameworks* de TI. Estas *frameworks* são um conjunto de boas práticas a implementar para gestão de serviços de TI.

Nestas *frameworks* estão incluídos vários processos das diferentes áreas das TI. Este trabalho de investigação focou-se muito concretamente no processo de Gestão de Incidências. Sendo que a operacionalidade da generalidade dos serviços requerer disponibilidade de quase 24/7, a implementação deste processo é fulcral.

Muitas das *frameworks* de TI contem processos similares. Muitas organizações, quando tentam aplicar mais que uma *framework* acabam por fazer trabalho redundante. Assim sendo, a eliminação de sobreposições das atividades torna-se bastante útil para qualquer processo das *frameworks* de IT. Desta forma o processo torna-se mais simples e menos dispendioso para a organização.

Dada a necessidade das organizações de avaliarem a maturidade do seu processo de gestão de incidências e que diferentes organizações têm diferentes *frameworks* de TI, nasceu a necessidade deste trabalho de investigação.

Esta tese propõe um Modelo de Maturidade para o processo de gestão de incidências que abranja as principais e mais utilizadas *frameworks* de TI.

Palavras-Chave: Gestão de Incidências, Modelo de Maturidade, Frameworks de TI, Sobreposição de Frameworks.

Title: Maturity Model of Incident Management

Name: João Filipe Ferreira Aguiar

Master: IT and Management

Supervisor: Doctor Rúben Filipe de Sousa Pereira

Abstract

Over the last 25 years the concern of most organizations with Information Technology (IT) has been clearly exponential. In order to plan, organize, select, support and deliver IT services, it was necessary to implement IT frameworks. These frameworks are a set of the best practices to implement on IT service management.

These frameworks are included in several processes of different areas of IT. This research work is focused very concretely on the Incident Management process. Once the organizations technical consulting services are available 24/7, an implementation of this process is crucial.

Many of the IT frameworks contain similar processes. Many organizations, when trying to apply more than one framework, end up doing redundant work. Therefore, eliminating overlaps of activities becomes very useful for any process of IT frameworks. In this way, the process becomes simpler and less expensive for the organization.

Given the need of the organizations evaluate the maturity of their incident management process and different organizations and different IT frameworks, was born the need for this research.

This thesis proposes a Maturity Model for the incident management process that covers the main and most used IT frameworks.

Keywords: Incident Management, Maturity Model, IT Framework, Overlapping Frameworks.

Table of Contents

Acknowledgements	iii
Resumo	v
Abstract	vi
Table of Contents	vii
List of Tables	ix
List of Figures	x
Chapter 1 – Introduction	11
Chapter 2 – State of the Art	15
2.1. IT Frameworks	16
2.1.1. ITIL.....	17
2.1.2. COBIT	23
2.1.3. CMMI.....	26
2.1.4. Frameworks conclusions and summary.....	29
2.2. Maturity Model Frameworks.....	30
2.2.1. COBIT PAM	32
2.2.2. ISO/IEC 15504	34
2.2.3. CMMI-SVC	36
2.2.4. TIPA	39
2.2.5. AXELOS	41
2.2.6. J. Flores, L. Rusu and P. Johannesson Model	43
2.2.7. R. Pereira, and M. Silva Model	46
2.2.8. M. Vitoriano and J. Neto Model.....	49
2.2.9. M. Simonsson, P. Johnson and H. Hijkstrom Model	51
2.2.10. Comparison Maturity Models Frameworks.....	53
Chapter 3 – Research Methodology	55
3.1. Data collection.....	56
3.2. Data analysis.....	57
Chapter 4 – Proposal	59
Chapter 5 - Analysis and discussion of results	65
Chapter 6 – Conclusions	73
Bibliography	75
Appendix	78
Appendix A	78
Appendix B.....	89
Appendix C.....	101

Appendix D	110
Appendix E	120
Appendix F	126

List of Tables

Table 1- Processes – ITIL.....	19
Table 2- IM Roles – ITIL.....	21
Table 3- DSS Domain – COBIT 5.....	24
Table 4- Activities from COBIT 5.....	25
Table 5 -Process Areas from CMMI SVC.....	27
Table 6- Relationship between IRP Process - CMMI.....	27
Table 7- Specific Goal and Practices – CMMI.....	28
Table 8- Activities – CMMI.....	28
Table 9- Comparison IT Frameworks.....	29
Table 10- Capability Levels – COBIT PAM.....	33
Table 11- Capability Levels- ISO/IEC 15504.....	35
Table 12- Capability Levels – CMMI-SVC.....	36
Table 13- Maturity Levels – CMMI.....	37
Table 14 -Maturity Levels – TIPA.....	39
Table 15- Maturity Levels- Axelos.....	42
Table 16- Proposed Activities.....	43
Table 17- Service Capacity and Service Continuity.....	44
Table 18- Stage Model and Continuous Model.....	47
Table 19- Type of Questions and Answers.....	47
Table 20- Fulfill of Requirements.....	51
Table 21- Comparison Maturity Models Frameworks.....	53
Table 22- Comparison of Maturity Models Levels.....	53
Table 23- Interviewees Profile.....	56
Table 24- Excerpt of CMMI activities.....	59
Table 25- Excerpt of activities merged.....	60
Table 26- Excerpt of applied questionnaire.....	61
Table 27- Questionnaire header.....	62
Table 28- Questionnaire header 2.....	63
Table 29- Organizations Comparison.....	65
Table 30- Activities completed by all organizations.....	69
Table 31 - Interviewees’ opinion about IM process maturity model.....	72

List of Figures

Figure 1- Service Life Cycle - ITIL	18
Figure 2- Incident Management Process - ITIL	20
Figure 3- COBIT Principles	23
Figure 4- Areas from COBIT 5	24
Figure 5- Process DSS02 – Manage Service Requests and Incidents- COBIT 5	25
Figure 6- Process Assessment Model -COBIT PAM.....	32
Figure 7- Part of questionnaire used in IM.....	48
Figure 8- Proposed Maturity Levels.....	52
Figure 9- Research Process Diagram	55
Figure 10- IT Strategy	65
Figure 11- IT Structure	65
Figure 12- Expected and achieved Maturity Level	66
Figure 13- Activities Completed by Maturity Level	66
Figure 14- Average of activities completed	67
Figure 15- IT framework distribution.....	67
Figure 16- Distribution of activities by framework.....	68
Figure 17- Distribution of activities completed by framework.....	68

Chapter 1 – Introduction

The Information Technology (IT) has been growing steadily, and organizations whether they are larger or smaller are totally dependent on it if they intend to succeed and optimize their services. IT has become crucial to the support, sustainability and growth of most businesses [1], by supporting existing business strategies as well as new strategies [2]. IT has ceased to act simply as a supportive role and has taken on a central position within organizations. Currently, having an IT department is not enough to ensure that they are technologically successful.

But the IT-Services relationship has not always been successful. Due to the high number of services and the different types of organizations, IT's had to grow rapidly and widely. IT service managers are under pressure to reduce costs while helping the organization to generate revenue and quickly deliver cost effective services to their customers [3].

Due to this rapid and somewhat unstructured growth, there was a need to plan IT strategies and manage IT processes. To meet this need some organizations have adopted/developed IT frameworks.

Information Technologic Infrastructure Library (ITIL) is the most widely accepted approach to IT service management in the World [4], [5].

Capability Maturity Model Integration (CMMI) is another widely used IT framework. This model, focuses on the activities that are associated with the service provided by the organization, to provide quality of service to customers and final consumers [6]. CMMI provides to organizations a means to achieve service improvement [7].

COBIT is a framework that provides a set of support tools that enable managers to fill gaps with respect to control requirements, technical issues and business risks, and communicate the level of control to stakeholders. It establishes a clear relationship between the governance requirements of IT, IT processes and their control [8].

Many organizations due to being so different in size, objectives and focus found difficulties to implement these frameworks and there was a need to apply maturity models to the different frameworks. Many frameworks overlap each other and tend to propose the same processes with different names [9].

“What you can't measure, you can't control”, the phrase is from a British Physicist and Mathematician Peter Drucker and translates the need to measure performance to control.

Assigning more and more importance to the quality and quantity of information obtained in the IT, a good management of these elements is paramount.

Maturity models in IT management have been proposed since at least 1973 [10]. More than one hundred different maturity models have been proposed [11] but most are too general and, as a result, are not well defined and documented [12].

One of the most common ITIL process and top priority of adoption by organizations, is the Incident Management (IM) process [13]. IM is a key element of supporting [14].

Due to the monetary, operational, and image impact that IM can bring to an organization, it is critical that it is fully implemented and constantly improved. One of the ultimate measures of an IT support organization's success is the amount of time it takes to resolve an incident [5].

This type of coordination of incident management is only possible if the organization has implemented a solid and clear IT framework.

The implementation of the IM process is long, complex and expensive. Failure of properly operate this process may generate monetary losses and tarnish the image of the organization.

More specifically, the failure to implement IM can result in ongoing interruptions by IT Support technicians, poorly defined resolution priorities, poor management information and forgotten, poorly managed events.

The main causes for failure to implement effective IM are [15]:

- Absence of visible management or staff commitment, resulting in non-availability of resources for implementation;
- Lack of clarity about the business/organization's needs;
- Out of date working practices;
- Poorly defined objectives, goals and responsibilities;
- Absence of knowledge for resolving incidents;
- Inadequate staff training;
- Resistance to change;

The reality of IT support organization is much more complicated, with staff working around the clock in the most disparate geographies [5]. When the IM process is done

manually causes a loss of time and degradation of user work performance due to the shutdown of a service and the delay of this service to resumes their operational status [16].

References and guidelines on how to develop and improve the service maturity are foundations to improve service performance and customer satisfaction [17].

After the previous IM contextualization, this thesis will address the following two problems:

P1: Many IT Frameworks overlap each other. [18]

P2: The lack of completeness in the Maturity Models. [12]

These two subproblems are the ones that I will address in this thesis and the ones that our proposal contributes to solve. In order to strengthen our theoretical contribution, I have decided to transform the subproblems in one major hypotheses to be tested.

RQ: Is it possible to develop an overlap less IT Maturity Model?

This work is organized by chapters and subdivided into topics to help its structuring and understanding.

In this chapter, is introduced the research theme and its proposal as well as a brief description of the work structure. The second chapter reflects the theoretical review where I analyse the most relevant research in the main areas covered by this thesis. It's called State of the Art. Third chapter is dedicated to the methodology used in the data collection and the process used as well as the data analysis methods. The fourth chapter reflects the proposal to be tested and how it was reached. The fifth chapter presents the analysis of the results obtained, according to the methodology that was considered appropriate. The final chapter presents the conclusions of this study.

Chapter 2 – State of the Art

This thesis aims to prove that it is possible to develop of a new maturity model mitigate the frameworks overlap problem. Bearing this in mind is important to analyse the current SotA about IT frameworks and IT maturity models.

The SotA contains two major topics:

- IT Frameworks: The most used and famous IT Management frameworks were analyzed. ITIL V3, COBIT5 and CMMI-SVC were the IT frameworks analyzed.
- IT Maturity Models: Some Maturity Models were analysed and it was done a comparison between them at the end in order to choose the best reference to develop our own. The analysed maturity models are COBIT PAM, ISO/IEC 15504, CMMI-SVC, TIPA and AXELOS. It was also performed a research, and we analyzed, reflected and took conclusions about researches/papers done in the area of Maturity Model's in IT Management.

2.1. IT Frameworks

IT frameworks have been created to manage, measure, and align IT objectives with the organization's objectives.

Among the most known, important and used IT management frameworks, ITIL, COBIT and CMMI stand out.

At the next sections, I will provide a short presentation of the main IT Frameworks as well as a comparison between them.

2.1.1. ITIL

The Information Technology Infrastructure Library (ITIL) is a set of publications on best practices for managing IT services [19]. ITIL is the most widely accepted approach to IT service management in the world [20], [21].

It was created in the late 1980s from the need of the English Government to have organized processes in the IT field. ITIL proposes that in order to improve service quality, IT must organize activities around standardized process and perform these activities repeatedly. Since the 1990s, ITIL has been adopted by several European private organizations, mainly due to the great focus on quality, guaranteed by the definition of processes and making ISO 9000 more practicable.

ITIL requires too much change in culture and it is too focused on technology, toolsets and software, it is too high-level to implement, and the organizations usually lacks experienced consultants in ITIL [22].

In 2007, ITIL suffered the biggest update. New models and architectures like outsourcing, cloud, virtualization, web service and mobile were considered. This modernization became known as ITIL V3. In 2011, ITIL V3 2011 was published with the aim of improving consistency between the main publications.

The ultimate goal of ITIL is to improve how IT delivers and supports valued business services. ITIL is not just technology management or process management. ITIL also focuses on improving the capabilities of people, processes, and technology.

Organizational benefits of adopting ITIL best practices may include:

- Stronger alignment between IT and the business;
- Improved service delivery and customer satisfaction;
- Reduced costs through improved use of resources;
- Greater visibility of IT costs and assets;
- Better management of business risk and service disruption or failure;
- More stable service environment to support constant business change.

More detailed benefits and advantages of the ITIL framework are documented in each of the stages and in the 26 ITIL process areas defined in the core books. Essentially, the benefit lies in aligning process area with desired business outcome.

ITIL has been used by organizations in all industries and sectors, including: large, medium, and small organizations, governments and universities. ITIL can benefit any organization that provides an IT service management (ITSM) product or service [23].

Every organization has unique qualities and parameters, therefore it's important for a team who uses ITIL that evaluate and apply the guidelines in a way that fits the needs of its business.

Since ITIL is a set of best practices and not a standard, organizations are free to adopt as much of the ITIL framework as is valuable to them. However, the more ITIL-compliant an organization's processes are, the greater the benefits that organization will realize [24].

ITIL suggests that service management activities should be structured in the service life cycle (Figure 1).

The main content of ITIL is described in 5 books. Each of the 5 books refer to a specific stage of the service life cycle.



Figure 1- Service Life Cycle - ITIL

Since the focus of this thesis is the IM, I have highlighted (Table 1) the process that better match with such topic, which I will further analyze forwardly.

Table 1- Processes – ITIL

Book	Process
Service Strategy	Strategy management for IT services
	Service portfolio management
	Financial management for IT services
	Demand Management
	Business relationship management
Service design	Design Coordination
	Service Catalogue Management
	Service Level Management
	Availability management
	Capacity management
	IT service continuity management
	Information security management
	Supplier Management
Service Transition	Transition planning and support
	Change Management
	Service asset and configuration management
	Release and deployment management
	Service validation and testing
	Change evaluation
	Knowledge management
Service Operations	Event management
	Incident management
	Request fulfillment
	Problem management
	Access management
	Service Desk function
	Technical management function
	IT operations management functions
	Application management function
Continual service improvement	Seven-step improvement process

Service Operation is the phase in the ITIL Lifecycle that is responsible for ‘business-as-usual’ activities. The Service Operation can be viewed as the ‘factory’ of IT. This implies a closer focus on the day-to-day activities and infrastructures that are used to deliver services.

The Service Operations book is where the activities and processes necessary to deliver customer service and business users are coordinated and performed.

Yet, is in the Service Operations that the contact is more direct with the client or user and consequently when the value of the service is more valued.

According to ITIL, IM is the process responsible for managing the life cycle of all incidents. Ensures that normal service is reestablished as quickly as possible while creating the smallest possible impact on the business.

There are some basic things that need to be taken into account and decided when considering IM:

- Timescales – Must be agreed for all incident-handling stages;
- Incident Models – Is a way of predefining the steps that should be taken to handle a process in an agreed way;
- Major Incidents – A separate procedure, with shorter timescales and greater urgency must be used for ‘major’ incidents.

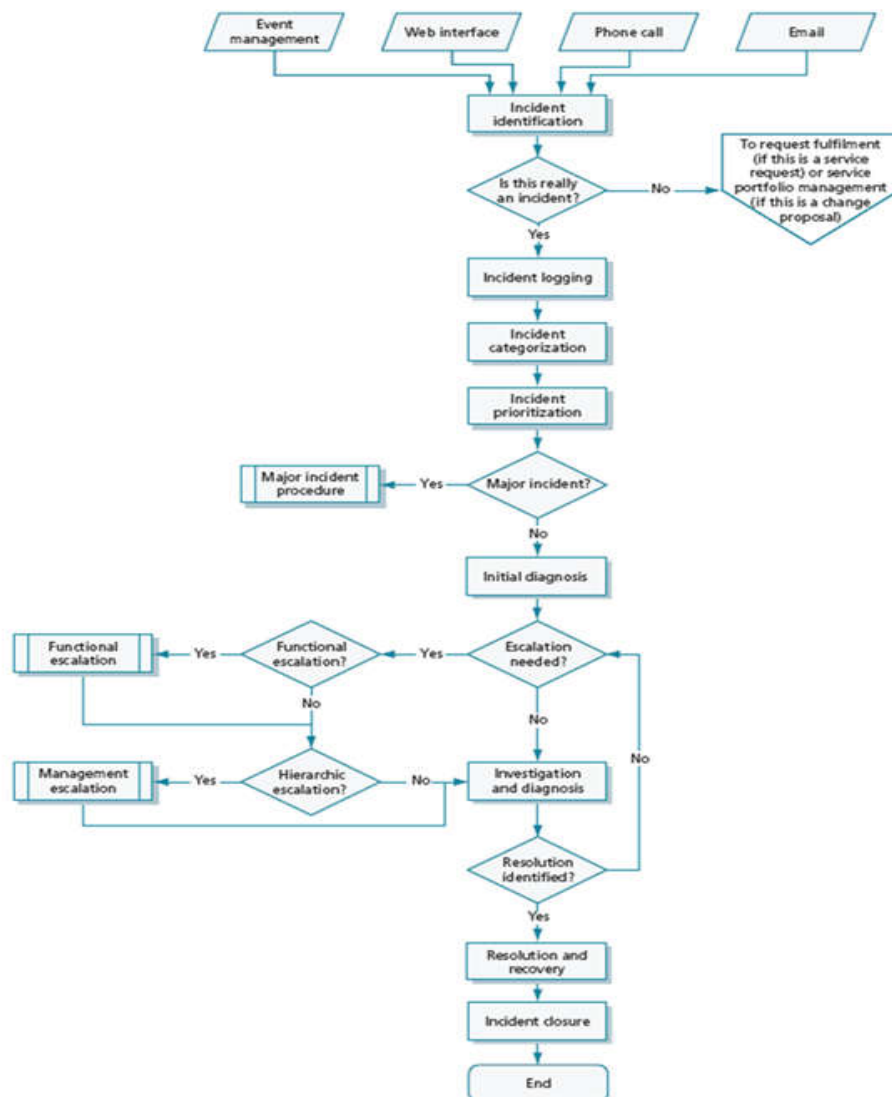


Figure 2- Incident Management Process - ITIL

In ITIL, incidents go through a structured workflow that encourages efficiency and best results for both providers and customers. ITIL recommends the IM process follow on Figure 2.

ITIL roles are used in order to define responsibilities. In particular, they are used to assign process owners to the various ITIL processes, and to illustrate responsibilities for the single activities within the detailed process descriptions. Regarding IM roles, ITIL proposes the following ones in Table 2.

Table 2- IM Roles – ITIL

Roles	Function
Incident Manager	Have the responsibility for, developing and maintaining the IM systems, process and procedures. Managing the work of incident support staff (1 st and 2 nd line) and managing major incidents was their responsibility too. Driving the efficiency and effectiveness of the IM process and making recommendations for improvement.
First Line	Is the primary point of contact for users when there is a service disruption, take the first actions to resolve the issue. If can't resolved, escalate to second level.
Second Line	Made up of staff with greater (though still general) technical skills than the Service Desk and with additional time to devote to incident diagnosis and resolution without interference from telephone interruptions.
Third Line	Will be provided by a number of internal technical groups and/or third-party suppliers. Network, Server, Desktop, Database or Voice Support, Application Management and others are the activities usually use for this support group

IM has close relationships with and dependencies on other service management processes, including:

- Change management. The resolution of an incident may require the raising of a change request. Also, since a large percentage of incidents are known to be caused by implementation of changes, the number of incidents caused by change is a key performance indicator for change management;
- Problem management. An important tool in the diagnosis of incidents is the known error database (KEDB), which is maintained by problem management. Problem management, in turn, depends on the accurate collection of incident data in order to carry out its diagnostic responsibilities;
- Service asset and configuration management. The configuration management system (CMS) is a vital tool for incident resolution because it identifies the relationships among service components and also provides the integration of configuration data with incident and problem data;
- Service level management. The breach of a service level is itself an incident and a trigger to the service level management process. Also, service level agreements (SLAs) may define timescales and escalation procedures for different types of incidents.

In conclusion, ITIL is one of the most used and known IT Framework. Is pointed in the literature as being very complete and organized. The process with interest to this investigation is the Incident Management and is one of the most important. It is inserted in Service Operations book.

2.1.2. COBIT

COBIT is a framework for developing, implementing, monitoring and improving IT governance and its management practices as well as one of the most adopted worldwide for such purpose.

The COBIT framework is published by the IT Governance Institute and the Information Systems Audit and Control Association (ISACA) [24]. The purpose of the framework is to provide a common language for business executives to communicate with each other about goals, objectives and results. The original version, published in 1996, focused largely on auditing. The latest version, published in 2013, COBIT 5, emphasizes the value that information governance can provide to a business' success. It also provides quite a bit of advice about enterprise risk management.

COBIT 5 is based on five key principles for governance and management of enterprise IT as we can see in Figure 3.

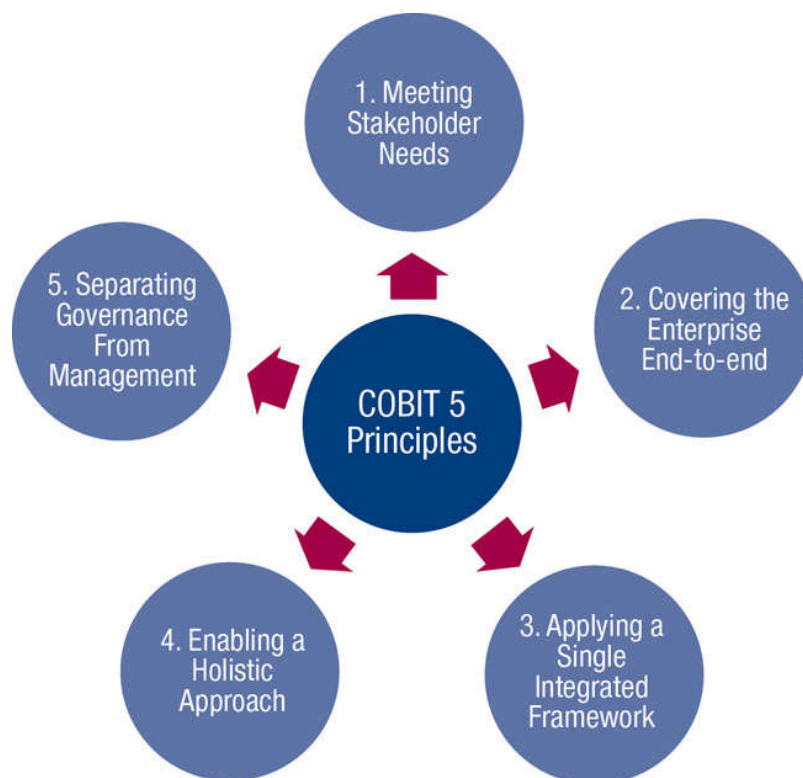


Figure 3- COBIT Principles

The COBIT 5 processes are split into governance and management areas. These two areas contain a total of five domains and thirty-seven processes (Figure 4):

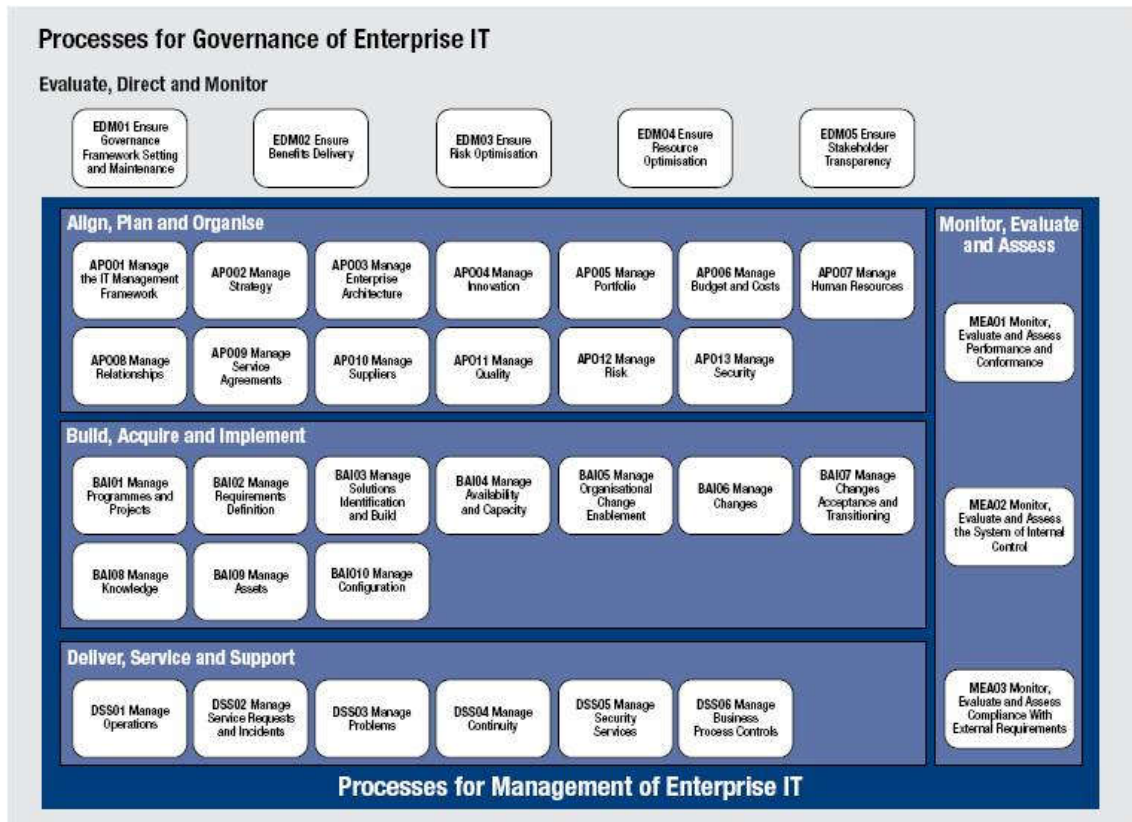


Figure 4- Areas from COBIT 5

Since this thesis focus on IM, I decided to analyze in more detail the process DSS02 Manage Service, Requests and Incidents that is inserted in the domain Deliver, Service and Support (DSS).

The DSS domain center on the delivery aspects of the information technology. It covers areas such as the execution of the applications within the IT system and its results, as well as the support processes that enable the effective and efficient execution of these IT systems. The Table 3 lists the high-level control objectives for the DSS domain.

Table 3- DSS Domain – COBIT 5

Deliver, Service and Support (DSS)	
DSS01	Manage Operations
DSS02	Manage Service Requests and Incidents
DSS03	Manage Problems
DSS04	Manage Continuity
DSS05	Manage Security Services
DSS06	Manage Business Process Controls

The process DSS02, Manage Service Requests and Incidents aims to:

- Record, investigate, diagnose, escalate and resolve incidents;

- Restore normal services;
- Provide timely and effective response to user requests and resolution of all types of incidents.

The Process, DSS02 is described in more detail in Figure 5.

DSS02 Manage Service Requests and Incidents		Area: Management Domain: Deliver, Service and Support
Process Description Provide timely and effective response to user requests and resolution of all types of incidents. Restore normal service; record and fulfil user requests; and record, investigate, diagnose, escalate and resolve incidents.		
Process Purpose Statement Achieve increased productivity and minimise disruptions through quick resolution of user queries and incidents.		
The process supports the achievement of a set of primary IT-related goals:		
IT-related Goal	Related Metrics	
04 Managed IT-related business risk	<ul style="list-style-type: none"> • Percent of critical business processes, IT services and IT-enabled business programmes covered by risk assessment • Number of significant IT-related incidents that were not identified in risk assessment • Percent of enterprise risk assessments including IT-related risk • Frequency of update of risk profile 	
07 Delivery of IT services in line with business requirements	<ul style="list-style-type: none"> • Number of business disruptions due to IT service incidents • Percent of business stakeholders satisfied that IT service delivery meets agreed-on service levels • Percent of users satisfied with the quality of IT service delivery 	
Process Goals and Metrics		
Process Goal	Related Metrics	
1. IT-related services are available for use.	<ul style="list-style-type: none"> • Number and percent of incidents causing disruption to business-critical processes • Mean time between incidents according to IT-enabled service 	
2. Incidents are resolved according to agreed-on service levels.	<ul style="list-style-type: none"> • Percent of incidents resolved within an agreed-on/acceptable period of time 	
3. Service requests are dealt with according to agreed-on service levels and to the satisfaction of users.	<ul style="list-style-type: none"> • Level of user satisfaction with service request fulfilment • Mean elapsed time for handling each type of service request 	

Figure 5- Process DSS02 – Manage Service Requests and Incidents- COBIT 5

COBIT 5 activities provide the ‘how’, ‘why’ and ‘what’ to implement according to each governance or management practice to improve IT performance and/or address IT solution and service delivery risk. The activities of this process are described in Table 4.

Table 4- Activities from COBIT 5

Activities – COBIT	
B1	DSS02.01 Define incident and service request classification schemes
B2	DSS02.02 Record, classify and prioritize requests and incidents
B3	DSS02.03 Verify, approve and fulfil service requests
B4	DSS02.04 Investigate, diagnose and allocate incidents
B5	DSS02.05 Resolve and recover from incidents
B6	DSS02.06 Close service requests and incidents
B7	DSS02.07 Track status and produce reports

2.1.3. CMMI

Capability Maturity Model Integration (CMMI) is a best practice framework [25]. The CMMI model does not describe the processes themselves, it describes the characteristics of good processes, thus providing guidelines for organizations developing or honing their own sets of processes [26].

The first CMMI model (V1.02) was released in 2000 and designed for being used by development organizations in their pursuit of enterprise-wide process improvement.

By the time that version 1.2 was released, two other CMMI models were being planned. Because of this planned expansion, the name of the first CMMI model had to change and became CMMI for Development.

The CMMI for Acquisition model was released in 2007. Two years later, the CMMI-SVC for Services model was released.

In 2008 plans were drawn to begin developing Version 1.3, which would ensure consistency among all three models and improve high maturity material. Version 1.3 of CMMI for Acquisition, CMMI for Development and CMMI for Services were released in November 2009 [27].

CMMI-SVC draws on concepts and practices from CMMI and other service focused standards and models, including the following:

- Information Technology Infrastructure Library (ITIL);
- ISO/IEC 20000: Information Technology – Service Management;
- Control Objectives for Information and related Technology (COBIT);
- Information Technology Services Capability Maturity Model (ITSCMM).

According CMMI-SVC, process areas are a cluster of related practices in an area that, when implemented collectively, satisfy a set of goals considered important for making improvement in that area. CMMI-SVC contains twenty-four process areas (Table 5).

Table 5 -Process Areas from CMMI SVC

Process Areas	
CAM	Capacity and Availability Management
CAR	Causal Analysis and Resolution
CM	Configuration Management
DAR	Decision Analysis and Resolution
IRP	Incident Resolution and Prevention
IWM	Integrated Work Management
MA	Measurement and Analysis
OPD	Organizational Process Definition
OPF	Organizational Process Focus
OPM	Organizational Performance Management
OPP	Organizational Process Performance
OT	Organizational Training
PPQA	Process and Product Quality Assurance
QWM	Quantitative Work Management
REQM	Requirements Management
RSKM	Risk Management
SAM	Supplier Agreement Management
SCON	Service Continuity
SD	Service Delivery
SSD	Service System Development
SST	Service System Transition
STSM	Strategic Service Management
WMC	Work Monitoring and Control
WP	Work Planning

The purpose of Incident Resolution and Prevention (IRP) is to ensure timely and effective resolution of service incidents and prevention of service incidents as appropriate.

Once again, this framework also indicates that this process is one of the most important and most valued.

Some processes are affected by the IRP process which is detailed on Table 6.

Table 6- Relationship between IRP Process - CMMI

Process	Relationship
Capacity and Availability Management	Monitoring and analyzing capacity and availability
Service Delivery	Establishing service agreements
Causal Analysis and Resolution	Determining causes of selected outcomes
Configuration Management	Tracking and controlling changes
Risk Management	Identifying and analyzing risks and mitigating risks
Work Monitoring and Control	Providing an understanding of the ongoing work so that appropriate corrective actions can be taken when the performance deviates significantly from the plan

According to CMMI framework, a specific goal describes the unique characteristics that must be present to satisfy the process area. A specific practice is the description of an activity that is considered important in achieving the associated specific goal. The specific practices describe the activities that are expected to result in achievement of the specific goals of a process area.

The Specific Goals and Specific Practices of this process and the activities were described in Table 7 and Table 8 respectively.

Table 7- Specific Goal and Practices – CMMI

Specific Goals	Specific Practices
SG 1 Preparation for incident resolution and prevention is conducted.	SP 1.1 Establish and maintain an approach to incident resolution and prevention.
	SP 1.2 Establish and maintain an incident management system for processing and tracking incident information.
SG 2 Individual incidents are identified, controlled, and addressed.	SP 2.1 Identify incidents and record information about them.
	SP 2.2 Analyze individual incident data to determine a course of action.
	SP 2.3 Resolve incidents.
	SP 2.4 Manage the status of incidents to closure.
	SP 2.5 Communicate the status of incidents.
SG 3 Causes and Impacts of selected incidents are analyzed and addressed.	SP 3.1 Analyze the underlying causes of selected incidents.
	SP 3.2 Establish and maintain solutions to respond to future incidents.
	SP 3.3 Establish and apply solutions to reduce the occurrence of selected incidents.

Table 8- Activities – CMMI

Activities – CMMI	
C1	Identifying and analyzing service incidents
C2	Initiating specific actions to address incidents
C3	Monitoring the status of incidents, tracking progress of incident status, and escalating as necessary
C4	Identifying and analyzing the underlying causes of incidents
C5	Identifying workarounds that enable service to continue
C6	Initiating specific actions to either address the underlying causes of incidents or to provide workarounds
C7	Communicating the status of incidents to relevant stakeholders
C8	Validating the complete resolution of incidents with relevant stakeholders

In conclusion CMMI is also one of the most used frameworks. This framework contains a process with interest to this investigation, the Incident Resolution and Prevention.

2.1.4. Frameworks conclusions and summary

After describe the most important, used and relevant IT Frameworks, this section intends to present a brief analysis of them (Table 9).

Table 9- Comparison IT Frameworks

	ITIL V3	COBIT 5	CMMI-SVC
Founded	OGC	ISACA	Software Engineering Institute (SEI)
Last Update	July 2011	April 2012	November 2010
Focus	Service	Service	Service
IM	Yes	Yes	Yes
Name of Process	Incident Management	Manage Service Requests and Incidents	Incident Resolution and Prevention
Number of Processes	26	37	24

It's possible to see that the three principal IT frameworks are quite similar in the terms of focus and the last update was recently made. Nevertheless, COBIT 5 has the most recent released version.

The numbers of management processes are similar in ITIL V3 and CMMI-SVC, in the other hand, COBIT 5 have a few more.

All frameworks seem to have information about the IM which make them suitable frameworks to provide inputs to our proposal.

2.2. Maturity Model Frameworks

Maturity models is a measurement of the ability of an organisation for continuous improvement in a particular discipline. Also, is a structured collection of elements that describe characteristics of effective processes. A maturity model provides [50]:

- a place to start;
- the benefit of a community's prior experiences;
- a common language and a shared vision;
- a framework for prioritizing actions;
- a way to define what improvement means for your organization.

A maturity model can be used as a benchmark for assessing different organizations for equivalent comparison. It describes the maturity of the company based upon the project the company is dealing with and the clients.

Maturity models in IT management have been proposed since at least 1973 [10]. More than one hundred different maturity models have been proposed [11] but most are too general and, as a result, not well defined and documented [12].

The use of a maturity model allows an organization to have its methods and processes evaluated in accordance with good management practices and with a set of external parameters. Maturity is indicated by the assignment of a particular "Maturity Level".

When the organization knows the maturity level at the specific process will benefit [30] as follows:

- Knowledge of maturity level with clear recommendations on how to drive improvements;
- Ability to compare itself with other organizations, or with other sectors within the organization;
- Significant progress in self-assessments;
- A consistent set of questionnaires and scores;
- Independent verification and certification;
- A set of independent parameters.

The maturity level evaluation can be supported by certain procedures, including the use of questionnaires.

The advantage of maturity models is their simplicity which facilitates their understanding and communication as well as the fact that they may be used for benchmarking.

Considering the purpose of this thesis, the following sections will analyze the most relevant maturity models and some recent scientific works that propose new IT maturity models. At the end of the chapter comparison between them will be done.

2.2.1. COBIT PAM

Included in COBIT 5 documentation is a maturity model that can be used by organizations to assess COBIT processes maturity [28]. It is called Process Assessment Model (PAM).

COBIT 5 PAM is an evolution from the previous COBIT 4.1 maturity model which is more aligned with a generally accepted process assessment standard.

COBIT PAM was based on the ISO/IEC 15504 standard since it uses the ISO 15504 capability model and the standard's principle of assessment.

Moreover, COBIT PAM is a pillar of COBIT assessment programmed, it provides a base for:

- The process reference model, which defines level 1 base requirements;
- Determining the capability levels (the measurement framework).

As we can see in Figure 6, PAM is a two-dimensional model of process capability. In the process dimension, the processes are defined and classified according of established process categories

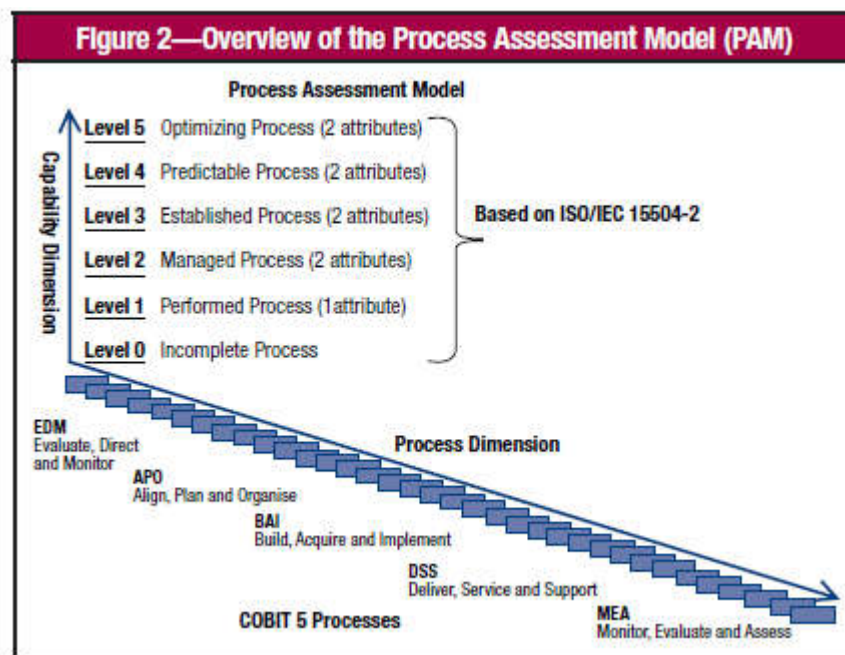


Figure 6- Process Assessment Model -COBIT PAM

In process dimension, the processes are defined and classified into process categories. The process dimension uses COBIT 5 as the process reference model. COBIT 5 provides

definitions of processes in a life cycle, together with an architecture describing the relationships amongst the processes.

In the capability dimension, a set of process attributes grouped into capability levels is defined. The process attributes provide the measurable characteristics of process capability. The capability dimension provides a way to assess the project business goals into organizations.

They have capability levels to classify the processes, as we can see on Table 10.

Table 10- Capability Levels – COBIT PAM

Capability Level	Description
Level 0- Incomplete Process	The process is not implemented or fails to achieve its process purpose
Level 1- Performed Process	The implemented process achieves its process purpose.
Level 2- Managed Process	The previously described performed process is now implemented in a managed fashion (planned, monitored and adjusted) and its work products are appropriately established, controlled and maintained.
Level 3- Established Process	The previously described managed process is now implemented using a defined process that is capable of achieving its process outcomes.
Level 4- Predictable Process	The previously described established process now operates within defined limits to achieve its process outcomes
Level 5- Optimizing Process	The previously described predictable process is continuously improved to meet relevant current and projected business goals

In conclusion, COBIT PAM is one of the most used and important maturity models. It has two dimensions and six maturity levels. As it happens in IT framework, COBIT 5, the maturity model COBIT PAM is more focused in the management level.

2.2.2. ISO/IEC 15504

ISO/IEC 15504 Information Technology – Process Assessment, also termed Software Process Improvement and Capability Determination (SPICE) was developed by the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC).

ISO/IEC 15504 is the international standard for process assessment. It defines a generic way of measuring the effectiveness of processes.

ISO/IEC 15504 has been designed to satisfy the needs of acquirers, suppliers and assessors, and their individual requirements from within a single source [29].

The main objective of IEC/ISO 15504 is to help the software industry to make gains in efficiency and quality and deals with software processes such as development, management, customer support and quality.

Process assessments have two different results:

- Process improvement, current practices in terms of the capability of the selected processes of an organization;
- Capability determination that consists in analyzing the proposed capability of selected processes against a target process capability profile, in order to identify the risks involved in undertaking a project using the selected processes.

As can we see in Table 11 there are six capability levels in the reference model.

Table 11- Capability Levels- ISO/IEC 15504

Level	Description
Level 0 – Incomplete	There is general failure to attain the purpose of the process. There are few or no easily identifiable work products or outputs of the process.
Level 1- Performed	The purpose of the process is generally achieved. The achievement may not be rigorously planned and tracked. Individuals within the organization recognize that an action should be performed, and there is general agreement that this action is performed as and when required. There are identifiable work products for the process, and these testify to the achievement of the purpose.
Level 2- Managed	The process delivers work products according to specified procedures and is planned and tracked. Work products conform to specified standards and requirements. The primary distinction from the Performed Level is that the performance of the process now delivers work products that fulfill expressed quality requirements within defined timescales and resource needs.
Level 3- Established	The process is performed and managed using a defined process based upon good software engineering principles. Individual implementations of the process use approved, tailored versions of standard, documented processes to achieve the process outcomes. The resources necessary to establish the process definition are also in place. The primary distinction from the Managed Level is that the process of the Established Level is using a defined process that is capable of achieving its process outcomes.
Level 4- Predictable	The defined process is performed consistently in practice within defined control limits, to achieve its defined process goals. Detailed measures of performance are collected and analyzed. This leads to a quantitative understanding of process capability and an improved ability to predict and manage performance. Performance is quantitatively managed. The quality of work products is quantitatively known. The primary distinction from the Established Level is that the defined process is now performed consistently within defined limits to achieve its process outcomes.
Level 5- Optimizing	Performance of the process is optimized to meet current and future business needs, and the process achieves repeatability in meeting its defined business goals. Quantitative process effectiveness and efficiency goals (targets) for performance are established, based on the business goals of the organization. Continuous process monitoring against these goals is enabled by obtaining quantitative feedback and improvement is achieved by analysis of the results. Optimizing a process involves piloting innovative ideas and technologies and changing non-effective processes to meet defined goals or objectives. The primary distinction from the Predictable Level is that the defined and standard processes now dynamically change and adapt to effectively meet current and future business goals.

2.2.3. CMMI-SVC

CMMI-SVC use levels to describe an evolutionary path recommended for an organization that wants to improve its processes.

Capability and Maturity are the two levels which reflect two improvement paths, defined as two representations and called Continuous and Staged. Both provide ways to improve processes to achieve business objectives.

The staged representation uses:

- Maturity levels to define the overall state of the organization's processes relative to the model in Staged representation;
- Capability levels used in Continuous representation to define the state of the organization's processes relative to process area.

To support those who use the continuous representation, all CMMI models reflect capability levels in their design and content.

A short description of each capability level follows in Table 12.

Table 12- Capability Levels – CMMI-SVC

Level	Description
Level 0 – Incomplete	An incomplete process is a process that either is not performed or is partially performed. One or more of the specific goals of the process area are not satisfied and no generic goals exist for this level since there is no reason to institutionalize a partially performed process.
Level 1 – Performed	A performed process is a process that accomplishes the needed work to produce work products; the specific goals of the process area are satisfied. Although capability level 1 results in important improvements, those improvements can be lost over time if they are not institutionalized.
Level 2- Managed	A managed process is a performed process that is planned and executed in accordance with policy; employs skilled people having adequate resources to produce controlled outputs; involves relevant stakeholders; is monitored, controlled, and reviewed; and is evaluated for adherence to its process description. The process discipline reflected by capability level 2 helps to ensure that existing practices are retained during times of stress.
Level 3- Defined	A defined process is a managed process that is tailored from the organization's set of standard processes according to the organization's tailoring guidelines; has a maintained process description; and contributes process related assets to the organizational process assets.

In case of Staged representation, CMMI models reflect maturity levels in their design and content.

A maturity level consists of related specific and generic practices for a predefined set of process areas that improve the organization's overall performance. The maturity level of an organization provides a way to characterize its performance.

The five Maturity Levels is describing in Table 13.

Table 13- Maturity Levels – CMMI

Level	Description
Level 1- Initial	Processes are usually ad hoc and chaotic. The organization usually does not provide a stable environment to support processes. Success in these organizations depends on the competence and heroics of the people in the organization and not on the use of proven processes. Organizations on this level provide services that often work, but they frequently exceed the budget and schedule documented in their plans. They are also characterized by a tendency to overcommit, abandon their processes in a time of crisis, and are unable to repeat their successes.
Level 2- Managed	Work groups establish the foundation for an organization to become an effective service provider by institutionalizing selected Project and Work Management, Support, and Service Establishment and Delivery processes. Work groups define a service strategy, create work plans, and monitor and control the work to ensure the service is delivered as planned. The service provider establishes agreements with customers and develops and manages customer and contractual requirements. Configuration management and process and product quality assurance are institutionalized, and the service provider also develops the capability to measure and analyze process performance.
Level 3- Defined	Service providers use defined processes for managing work. They embed tenets of project and work management and services best practices, such as service continuity and incident resolution and prevention, into the standard process set. The service provider verifies that selected work products meet their requirements and validates services to ensure they meet the needs of the customer and end user. These processes are well characterized and understood and are described in standards, procedures, tools, and methods.
Level 4- Quantitatively Managed	Service providers establish quantitative objectives for quality and process performance and use them as criteria in managing processes. Quantitative objectives are based on the needs of the customer, end users, organization, and process implementers. Quality and process performance is understood in statistical terms and is managed throughout the life of processes.
Level 5- Optimizing	An organization continually improves its processes based on a quantitative understanding of its business objectives and performance needs. The organization uses a quantitative approach to understand the variation inherent in the process and the causes of process outcomes.

The maturity levels are measured by the achievement of the specific and generic goals associated with each predefined set of process areas. Each maturity level matures an important subset of the organization's processes, preparing it to move to the next maturity level.

As we can verify, CMMI-SVC have 5 maturity levels. This framework is one of the most used and known among service management community. As the CMMI framework from which it derives, the CMMI-SVC is more focused on operation processes.

2.2.4. TIPA

The Tudor IT Process Assessment (TIPA) is a framework for IT process assessment. It uses the principles of the ISO/IEC 15504-33000 standard to determine the maturity level within an organization.

TIPA has been defined as an interview based assessment methodology. It is considered the most effective way to gather information concerning the process performance and it helps initiate the organizational change required to later improve the processes.

TIPA methodology has six maturity levels that are described in Table 14.

Table 14 -Maturity Levels – TIPA

Levels	Description
Level 1- Incomplete	The process is not implemented or fails to achieve its purpose
Level 2- Performed	The process is implemented and achieves its Process Purpose
Level 3- Managed	The process is managed and work products are established, controlled and maintained
Level – Established	A defined process is used and based on a standard process
Level 5- Predictable	The process is enacted consistently within defined limits
Level 6- Optimizing	The process is continuously improved to meet relevant current and projected business goals.

The assessment approach used in TIPA delineates an assessment project with six clearly defined phases:

- Definition phase: the main objectives are to set the scope of the assessment, to identify the key actors, to agree on a service offer and concur on the assessment scope agreement;
- Preparation phase: discover the organizational context, and then perform an assessment planning and define the organization (by preparing the Assessment team, the supporting documents used during the assessment and the people who will be interviewed);
- Assessment phase: during which interviews are done and documents reviewed to enable process rating and process capability level determination. This phase is the key of the process assessment;
- Analysis phase: the collected information is evaluated and a SWOT analysis is performed before making improvement recommendations;

- Result presentation phase: the results are presented to the relevant stakeholders, and the detailed assessment report is rendered;
- Assessment closure phase: the assessment project can then be closed.

2.2.5. AXELOS

AXELOS was created in 2013 by the Cabinet Office on behalf of Her Majesty's Government (HMG) in the United Kingdom and Capita, to manage, develop and grow the Global Best Practice portfolio [30].

AXELOS was an evolution of PMF.

Moreover, AXELOS is responsible for developing, enhancing and promoting a number of best practice methodologies used globally by professionals working primarily in project, programming and portfolio management, IT service management and cyber resilience.

AXELOS consists of a set of assessments, in the form of questionnaires, for each process and function across the ITIL service lifecycle.

Each questionnaire comprises:

- Process/function demographic questions;
- Process/function-generic attributes;
- Process/function-specific attributes;
- Process/function outcomes and outputs;
- Interfaces and inputs.

The AXELOS have 5 different maturity levels that are aligned with CMMI and COBIT definitions (Table 15).

Table 15- Maturity Levels- Axelos

Levels	Description
Level 1 – Initial	Processes or functions are ad hoc, disorganized or chaotic. There is evidence that the organization has recognized that the issues exist and need to be addressed. There are, however, no standardized procedures or process/function management activity, and the process/function is regarded as of minor importance, with few resources allocated to it within the organization. There are instead ad hoc approaches that tend to be applied on an individual or case-by-case basis. The overall approach to management is disorganized.
Level 2 – Repeatable	Processes or functions follow a regular pattern. They have developed to the stage where similar procedures are followed by different people undertaking the same task. Training is informal, there is no communication of standard procedures, and responsibility is left to the individual. There is a high degree of reliance on the knowledge of individuals and therefore errors are likely. In general, activities related to the process or function are uncoordinated, irregular and directed towards process or function efficiency.
Level 3- Defined	The process or function has been recognized and procedures have been standardized, documented and communicated through training. The procedures themselves are not sophisticated but are the formalization of existing practices. It is, however, left to the individual to follow these procedures and deviations may occur. The process has a process owner, formal objectives and targets with allocated resources, and is focused on both efficiency and effectiveness. Activities are becoming more proactive and less reactive.
Level 4 – Managed	The process or function has now been fully recognized and accepted throughout IT. It is service-focused and has objectives and targets that are aligned with business objectives and goals. It is fully defined, managed and is becoming pre-emptive, with documented and established interfaces and dependencies with other IT processes. Processes and functions are monitored and measured. Procedures are monitored and measured for compliance and action taken where processes or functions appear not to be working effectively. Processes or functions are under constant improvement and demonstrate good practice. Automation and tools are increasingly used to deliver efficient operations.
Level 5 – Optimized	Leading practices are followed and automated. A self-contained continuous process of improvement is established, which has now resulted in a pre-emptive approach. IT is used in an integrated way to automate the workflow, providing tools to improve quality and effectiveness, making the organization quick to adapt. The process or function has strategic objectives and goals aligned with overall strategic business and IT goals. These have now become ‘institutionalized’ as part of the everyday activity for everyone involved with the process or function.

2.2.6. J. Flores, L. Rusu and P. Johannesson Model

According to A Maturity Model of IT Service Delivery [31], the proposed IT Service Delivery Maturity Model was a mechanism for formalizing and assessing IT Service Delivery Elements.

The authors defined five levels of maturity:

- Level 1 – Initial;
- Level 2 – Repeatable;
- Level 3 – Defined;
- Level 4 – Managed;
- Level 5 – Optimized;

To an agile manipulation of the information the authors score the IT Service delivery element maturity level in a scale of 1 to 5. With the need to differentiate maturity states the authors add a “+” or a “-” if is closer the level up or down respectively.

In order to reduce the complexity, the activities are grouped as in the

Table 16.

Table 16- Proposed Activities

Service Definition Business and technical service information	Service Operation
Negotiation, agreement and maintenance of Service Level Agreement with the customer	Service Achievement
Budgeting, IT accounting and charging	Service Economy
Future business requirements, service performance and resource utilization	Service Capacity
The recovery of required IT technical and service facilities	Service Continuity
Required availability of IT service	Service Availability
Management of a defined level of security	Security Measures

In this particular case is explored in more detail the Service Capacity and Service Continuity activity in order to analyze the areas of IM (Table 17).

Table 17- Service Capacity and Service Continuity

Level	Description	
	Service Capacity	Service Continuity
1	<ul style="list-style-type: none"> - Customer trends are not analyzed - IT service performance is not monitored against Service Level Agreement (SLA) target - Resource utilization is not always analyzed right when an incident occurs 	<ul style="list-style-type: none"> - Personnel are reactive to customer IT service incidents and do not inform customers about the solution in progress
2	<ul style="list-style-type: none"> - Future business requirements are considered for formulating a new service or characterized for the service contracted - IT service performance is analyzed based on customer complaints - Changes of component parts of the IT infrastructure are appropriate to ensure service availability 	<ul style="list-style-type: none"> - Continuity and recovery mechanisms are well known and established through the personnel, who are conscious of the importance of providing good IT service
3	<ul style="list-style-type: none"> - Methods for forecasting future customer requirements have been implemented but their accuracy is not always analyzed - A tool is used to identify and understand IT service performance incidents - A tool is used to monitor and measure components within the IT infrastructure 	<ul style="list-style-type: none"> - Business Impact analysis is used to quantify the loss of the IT services and assess the impact of all changes
4	<ul style="list-style-type: none"> - Forecasted business requirements are accurate and satisfy the customer SLRs - A tool is used to monitor and supervise IT service performance constraints - Current resource utilization trends are produced and future resource requirement estimations are instituted in the organization 	<ul style="list-style-type: none"> - IT recovery plan is implemented and supports critical business processes
5	<ul style="list-style-type: none"> - Future business requirements for IT services are considered and understood, and sufficient capacity to support the services is planned for and implemented in a capacity plan with an appropriate timescale - IT service performance is accurately analyzed, improved and forecasted - Designed, procured or amended configuration of IT infrastructure component is based on capacity and utilization addressed by required response times, expected throughput and usage pattern, and is articulated in the capacity plan 	<ul style="list-style-type: none"> - ITSCM Plan is established and derived from Business Plan Continuity Plan

The Model was applied, and the activities most relevant related to IM are:

- Service performance is reported by customers through a help desk system. When an incident is reported, a ticket is opened in the troubleshooting system until the incident is solved. Is used ORION to monitoring network performance, that

enables quick detection, diagnosis and resolution of network outages and performance issues.

These functionalities score “2+” for service capacity.

- The Service continuity score “2” for the functionalities followed. The personnel are not proactive at preventing customer complaints. The IT staff is reactive and informs the customer of any progress regarding the incident reported. Any incident is recorded and followed up on in a troubleshooting system as knowledge database. The troubleshooting system cannot identify or follow patterns of service performance. The personnel seem to know what to do to keep the continuity and recovery of IT service; their dynamic organization structure promotes personnel commitment.

This article also presents a comparison with the paper *A maturity model for implementing ITIL v3* [32] which will be analyzed in the following sections.

2.2.7. R. Pereira, and M. Silva Model

The authors start by performing a comparison among several maturity models in the market. Rúben Pereira compares different Maturity Models in his work, 'A maturity model of implementing ITIL V3 (2010)'. In this model, the maturity levels used were the same used in CMMI, which can be seen on Table 13.

At the end, the authors chose ITSCMM and CMMI-SVC as a basis to their own model for three main reasons:

- Both focus on service;
- ITSCMM is very well detailed;
- CMM-SVC has Staged Model and Continuous Model, so they decided to design their model following the same rational to give organizations more flexibility in ITIL assessment.

This maturity model was completely different from other models in the market at the time because:

- It was specifically designed to help organizations measure their ITIL maturity;
- Guided them in the implementation of ITIL, in order to reduce risks;
- It was specifically created for ITIL context, as PMF, however PMF was initially designed for ITIL V2 and was too simple in terms of factors.

As we can see in table 18, both models, Staged and Continuous, are connected. While Staged Model provides a global view about the main processes to implement, Continuous Model enables the assessment of each ITIL process.

In order to support the proposed questionnaires, the authors designed and implemented a software prototype that helped organizations to assess their ITIL processes more professionally, easily and efficiently.

In this model, they chose the evaluation of IM, Configuration Management Processes and the Service Desk because they are the most popular in organizations implementing ITIL.

Table 18- Stage Model and Continuous Model

ITIL processes	Stage Model Maturity	Continuous Model Maturity			
		Level 2	Level 3	Level 4	Level 5
Service Catalogue Management	2				
Service Level Management	2				
Supplier Management	2				
Service Asset & Configuration Management	2				
Event Management	2				
Incident Management	2				
Request Fulfillment	2				
Monitoring & Control	2				
Service Desk	2				
Technical Management	2				
Service Generation	3				
Demand Management	3				
IT Financial Management	3				
Service Portfolio Management	3				
Capacity Management	3				
Availability Management	3				
IT Service Continuity Management	3				
Transition Plan & Support	3				
Change Management	3				
Release & Deployment Management	3				
Service Validation & Testing	3				
Problem Management	3				
Access Management	3				
Application Management	3				
Information Security Management	4				
Evaluation	4				
Knowledge Management	4				
Service Report	4				
Service Measurement	4				
Service Improvement	5				

Each questionnaire contains three kinds of questions and four possible answers (Table 19):

Table 19- Type of Questions and Answers

Questions	Answers
Key questions: All these questions are essential for the correct implementation of each specific level of the process, and all must be implemented to reach the level. Basically, they're related with roles, responsibilities, activities, documents, audits, reviews, etc.	Yes: They have the question implemented
Non-key questions: Not all of these questions need to be implemented, just 75 percent of them. Basically, they're related with sub-practices; they are not the main focus.	No: They don't have the question implemented
Dependent key questions: These questions are related to dependencies between processes. If the process that is being assessed depends in some way on other ITIL processes and the organization has those processes implemented too, then the question must be implemented; otherwise, it shouldn't be.	Don't know: They don't understand the question or don't know the answer
	In implementation: If they are already in an implementation phase of that question

Part of the IM questionnaire can be seen in Figure 7. I have chosen this questionnaire since this thesis is also focused on IM process.

Level 3	
Key	Was a policy for the planning and execution of the process established?
Key	Is the policy for the planning and implementation of the process documented?
Key	Was a plan for the implementation of the process defined?
Key	<ul style="list-style-type: none"> Was the plan reviewed by the stakeholders and had their consent?
Key	<ul style="list-style-type: none"> Is the plan revised when necessary?
Key	Is the plan for the execution of the process documented?
Key	Is the description of the incident management documented?
Key	Is there described how the responsibility in the handling incidents are assigned and transferred?
Key	Is there a description of the process that tells the needs and objectives for the implementation of the process?
Key	<ul style="list-style-type: none"> Is it maintained?
Key	<ul style="list-style-type: none"> Is it updated?
Key	<ul style="list-style-type: none"> Is it revised when necessary?
Key	Is there a description of how to notify customers or end users that could be affected by an incident reported? (typically documented in the service agreement). Describes the following parameters:
Non Key	<ul style="list-style-type: none"> Definitions of impact
Non Key	<ul style="list-style-type: none"> Response time
Non Key	<ul style="list-style-type: none"> Resolution time
Non Key	<ul style="list-style-type: none"> Rules for ordering
Non Key	<ul style="list-style-type: none"> Expectations in providing feedback to users
Key	Is the repository audited in accordance with a documented procedure?
Depend Key (Config. M.)	Did it exchanged information with the "Configuration Management" in order to maintain the registry settings?

Figure 7- Part of questionnaire used in IM

After a few interviews, the authors concluded that most organizations failed to implement ITIL properly and remaining at a low maturity level, not because they cannot implement a high percentage of what ITIL proposes, but because they failed to implement specific and crucial details.

2.2.8. M. Vitoriano and J. Neto Model

The methodology used by Vitoriano and Neto was based on the Process Maturity Framework (PMF), a maturity model described in the ITIL's reference model.

In fact, they disagree with Pereira and Silva (2010) who stated that the model was fairly simple and were just described in a few pages in ITIL v2, and little information was provided to help the ITIL's implementation.

PMF was incorporated into ITIL v3, and it can be found in Appendix H of the Design Service book (OGC, 2007a).

To use this maturity model, it is required to perform some interviews with questions related to the five maturity levels, such as: initial, repetitive, defined, managed and optimized; the information was collected on five basic processes of ITSM [33].

In addition to the classification of processes in maturity levels, the interviews gathered information on the possible causes of low process maturity.

As already explained in Table 15, the PMF defines an ITSM maturity model when it comprises five dimensions of organizational evolution.

For each of these dimensions there is a maturity scale, organized in sequential and cumulative stages, from a simple level to a higher level of growth and improvement.

Maturity levels described in the PMF, which follows the same nomenclature used by other maturity models such as ITSCMM, SW-CMM and CMM-SVC are described, as already mentioned, on Table 13.

A method to calculate this maturity has been defined for this purpose, as described below:

1. To find the maturity level in each Dimension, a questionnaire is applied to check if all the requirements indicated in the PMF are met;
2. In order to reach a certain level of maturity in any of the dimensions, all the answers must be positive in the respective level;
3. If there is a negative response, the interview is interrupted at that dimension, the maturity level reached at that point is stored and indications of possible causes for the negative response are presented;

4. At the end of the evaluation, when the level in each dimension has been identified, the process of maturity level may be calculated, as follows:

$$\text{GPM} = \frac{\sum_{N=1}^5 \text{Dimensions}}{5}$$

Where :

GPM- General Process Maturity

Dimensions- Maturity in each dimension

5. If GPM is a real number, truncation is used.

2.2.9. M. Simonsson, P. Johnson and H. Hijkstrom Model

This paper proposed an IT governance maturity assessment method designed to overcome the problems of validity, reliability and cost that are commonly associated with such methods today. One of the major benefits is that the person performing the assessment doesn't necessarily have to be an IT governance expert, since the analysis part is performed automatically [34].

According to the authors, a good IT Governance Maturity Assessment method must have:

- Good Validity:
RQ1: Consistency with common conceptions;
- Good reliability:
RQ2: Descriptive operationalization
RQ3: Normative operationalization;
- Low Cost:
RQ4: Support for efficient data collection
RQ5: Support for efficient analysis.

On the other hand, the authors verified COBIT fulfillment of these requirements (Table 20).

Table 20- Fulfill of Requirements

Requirement	Cobit's Fulfillment
RQ1	Fulfilled
RQ2	Partly Fulfilled
RQ3	Not Fulfilled
RQ4	Not Fulfilled
RQ5	Not Fulfilled

For these reasons, the authors designed their own method based on COBIT, leveraging the benefits and mitigating the weaknesses. It can be described in two parts:

- Modeling Language, to descriptive activities;
- Analysis Framework, to normative activities.

The modeling language was based on what exists in COBIT and allows to identify entities and relations.

The entities identified were: processes, activities, documents, KPI/KGI and Roles.

On the other hand, the relations were:

- Responsible, accountable, consulted or informed, with respect to a role in an activity;
- Input or output with respect to documents;
- Is-a-part, of-relation in respect of activities and processes.

The analysis Framework begins with the disagreement of COBIT metrics. The authors identified four generic metrics. Two of them are assessed for each activity, activity execution and assigned responsibilities. The other two, documents in place and KPI/KGI monitored, are assessed at process level as we can see in the Figure 8.





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

Figure 8- Proposed Maturity Levels

The authors assume that all metrics have the same weight and the aggregation of metrics is done into maturity scores on three different levels:

- Activity Level: the average between two different metrics;
- Process Level: the average of all underlying activities maturities, plus two more metrics;
- Enterprise Level: the average of all underlying activities maturities.

2.2.10. Comparison Maturity Models Frameworks

In this section, a comparison between the different maturity model's frameworks analyzed (Table 21) and the different levels of each maturity model (Table 22) is presented.

The adopted variables were:

- Number of levels: to know how many levels of maturity they have.
- Staged Model / Continuous Model: to understand what kind of model approach is used by each model.
- Scope: to know the area in each model is applicable.
- Based on: to understand if the model was based in other models.

Table 21- Comparison Maturity Models Frameworks

	COBIT PAM	ISO/IEC 15504	CMMI- SVC	TIPA	AXELOS
Number of levels	0-5	0-5	SM:1-5 CM:0-5	1-6	1-5
Scope	Services	Services	Services	Services	Services
Based on	ISO/IEC 15504	-----	-----	ISO/IEC 15504	-----

Table 22- Comparison of Maturity Models Levels

Level	COBIT PAM	ISO/IEC 15504	CMMI – SVC	TIPA	AXELOS
Level 0	Incomplete	Incomplete	-----	-----	-----
Level 1	Performed	Performed	Initial	Incomplete	Initial
Level 2	Managed	Managed	Managed	Performed	Repeatable
Level 3	Established	Established	Defined	Managed	Defined
Level 4	Predictable	Predictable	Quantitatively Managed	Established	Managed
Level 5	Optimizing	Optimizing	Optimizing	Predictable	Optimizing
Level 6	-----	-----	-----	Optimizing	-----

These variables certainly are important to consider when comparing the models. To measure these variables, it's necessary to read documentation about the models.

Chapter 3 – Research Methodology

Research Methodology implies more than simply the methods you intend to use to collect data [35]. The methodology may include publication research, interviews, surveys and others, and could include both present and historical information.

The focus of this thesis begins with three major points: IT Frameworks, Maturity Models and Incident Management. After all the research work, it became evident that there was a gap in the scientific community that touched all three points simultaneously. There was a need in organizations to apply a maturity model to the IM process that was transverse to the three main IT Frameworks.

The diagram of the research process can be seen at Figure 9.

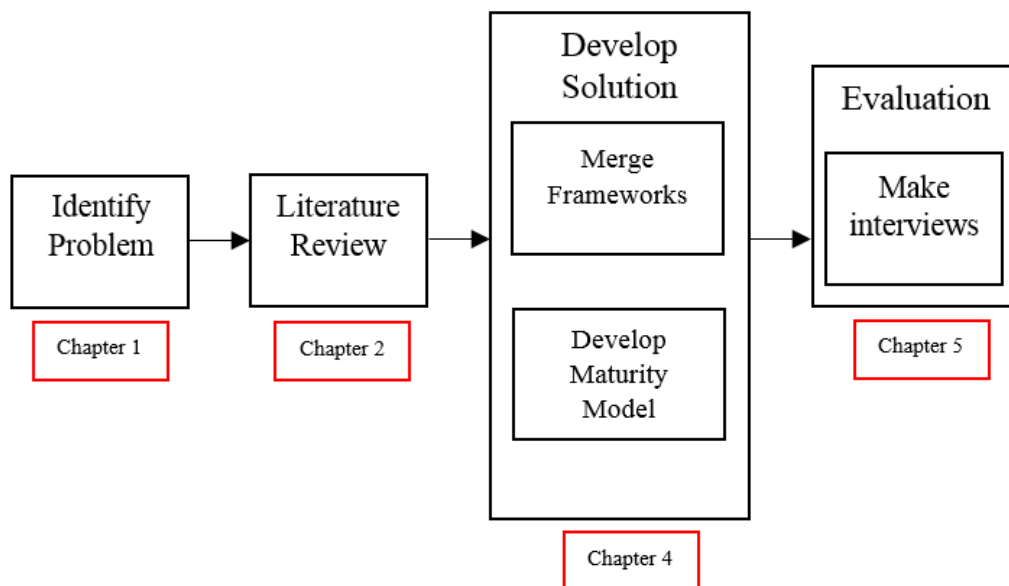


Figure 9- Research Process Diagram

After eliminating the overlap of the frameworks, the second step was to construct a questionnaire with all the activities of the process of IM divided by the five maturity levels. The questionnaire was applied to seven different organizations in order to assess the maturity of the process.

In the third step, the results of the questionnaire were analyzed. After evaluating the various interviews and comparing them, the patterns and trend verified were considered of great relevance. Even considering organizations of different industries and different sizes, it is quite interesting to verify their homogeneity.

3.1. Data collection

In order to assess the proposed IM maturity model, I chose 7 major organizations to interview. I carried out the interviews with CIOs, IT Coordinators and IT Directors since they were, at the time, the most suitable decision-makers responsible for the IM process. It's possible to see the profile of each interviewee in Table 23.

Table 23- Interviewees Profile

Country	Position	Experience in IT (years)	Duration of interview	Interview form
Portugal	Director of Infrastructure Computing and Communications Services	18	1h35m	Presential
Portugal	IT Director	15	1h	Presential
Portugal	IT Operations Manager	10	50m	Presential
Portugal	IT Director	18	1h10m	Presential
Portugal	IT Director	30	45m	Presential
Portugal	Area Manager Support Field Services	23	1h30m	Presential
U.S.A	APP Support Lead	25	1h	Skype

Only organizations already performing the IM process were selected to ensure scientific rigor and better results. It was important to approach different industries to understand how the activities applied to each of them. The responsible for the process was contacted by email in order to participate in this investigation. An invitation was sent to that person to schedule the interview. Six of that interviews were presential and the seventh was performed by Skype because it was an American company.

A copy of the questionnaire was delivered to the interviewees before the beginning of the interview. So, the interviewee could be able to follow it. In the case of the American company, the questionnaire was sent by email. During the interview, specific explanations of the activities were given to clarify any interviewees' doubts.

The questionnaire was divided in three main sections:

- Header, containing questions to collect information about the interviewee, industry and the IT department/team.
- Main body, containing questions about the execution of the activities Four possible answers could be provided: "Yes", "No", "In implementation", "Not applicable".

- Feedback, containing questions about the perception and opinion of the interviewee about the maturity model.

The interviews were conducted between April and June of 2017.

3.2. Data analysis

Each interview was analyzed on average, one week after it was performed.

It was important to identify the maturity level of IM process. But most important was the identification of gaps in the process and alert the organizations about the importance of implement such activities.

The analysis was done in two major phases:

- Individual, where was analyzed the interview of the organizations, identified the maturity level of the process, activities missing and done/sent a report to each company. These reports have information and recommendations about their process. It is possible to see one example of report in Appendix E.
- General, where was done a comparison between all organizations, identified correspondences, patterns and trends. I also elaborated a general report with these comparisons which was sent to all organizations. It is possible to see it in Appendix F.

Chapter 4 – Proposal

This thesis proposes a maturity model focus in IM based on different IT frameworks with the aim of improving this process in organizations.

After a deeply analyzing of the process of IRP of CMMI framework, it was possible to identify 108 activities.

The activities are described in Appendix A with the corresponding specific goal and specific practices. An ID match has been assigned to each activity to be easier to identify and use on the future chapters.

In the ITIL framework the same lifting was done of the all activities from the IM process (Appendix A). They are divided by different areas. About 134 activities were identified in the process of IM.

Yet, on COBIT framework on the manage service requests and incidents process (Appendix A), several activities were also identified and an ID assigned. In this framework 37 activities were identified from the process of Management Service Request and Incidents.

In Table 24 is possible to check an excerpt from the CMMI activities.

Table 24- Excerpt of CMMI activities

CMMI				
Specific Goals	Specific Practices	Activities	ID	
SG 2 Identify, Control and Address Incidents	SP 2.2 Analyze Incident Data	Is Analyzed incident data?	A21	
		Is determined which group is best suited to take action to address the incident?	A22	
		Is a determined action that must be taken to address the incident?	A23	
		Actions to be taken are planed?	A24	
	SP 2.3 Apply Workarounds to selected Incidents.	The incident is addressed using the workaround?	A25	
		Are managed the actions until the impact of the incident is at an acceptable level?	A26	
		Are recorded the actions and results for apply workarounds to selected incidents?	A27	
		SP 2.4 Address Underlying causes of selected Incidents	Are addressed the underlying causes using the action proposal that resulted from the analysis of the incidents underlying causes?	A28
			Are manager the actions until the underlying causes is addressed?	A29
			Are recorded the actions and results for address underlying causes of selected incidents?	A30

The activities were put in question form to facilitate their application in the interview.

After identify all activities from the IM process from the three Frameworks, I merged all of them (Appendix B). This made possible the elimination of overlaps.

In Table 25 is possible to check an excerpt from the activities merged.

Table 25- Excerpt of activities merged

Activities	CMMI	ITIL	COBIT	Maturity Level	Type
Is define criteria for determining what an incident is?	A1			2	O
For determining which categories an incident belong to is defined:					
• Categories?	A2			2	O
• Criteria?	A3			2	O
Is describe how responsibility for processing incidents is assigned and transferred?	A4	B8		2	O
Costumer and end users have mechanisms to report incidents?	A5			2	O
Are defined methods and secure tools to use for incident management?	A6			2	O
Are defined criteria for determining categories of actions and responses to be taken based on severity and priority levels?	A8			2	O
Are identified and monitored incidents that are in scope?	A18	B16		2	O
Does your organization have channels in place to receive incidents notifications?		B17		2	O
How can received incidents notifications:					
• By phone?		B18		2	O
• Other?				2	O
Detail:		B19			
Does your organization have mechanisms in place to automatically detect incidents?		B20		2	O
Are incidents reported and/or detected logged?		B21	C10	2	O
If support staff visit the customers:					
• They ask for further incidents?		B22		2	O
• A separate incident record is logged for each additional incident?		B23		2	O
To ensure consistent approaches for handling incidents is define criteria for problem registration?			C2	2	O
Are define incident models for known errors?			C4	2	O

Merging the activities led to a decrease from 279 to 207 activities. This made the questionnaire more concise and reliable.

For easier interpretation of all this information, after doing the merge, the activities were separated by maturity level (Appendix C). These maturity levels were assigned following the CMMI-SVC maturity model levels description, considering 5 maturity levels.

After all this theoretical work of elicitation of the activities, elimination of overlaps and maturity levels assignment, the questionnaire was ready to be applied.

The order of the questions was selected by area of the IM process (log in, closer, metrics, etc.). This was done to make the interview more fluid and easy to be followed by the interviewee.

On the other hand, there was no order by maturity level to avoid bias responses.

The completed questionnaire is available in the Appendix D, but is also available an excerpt in Table 26.

Table 26- Excerpt of applied questionnaire

Activities	Yes	No	In Implementation
Is defined a criterion for determining what an incident is?			
Are defined methods and secure tools to execute incident management process? Which ones:			
For determining which incidents belong to is defined categories?			
Is described how responsibility for processing incidents is assigned and transferred?			
Customer and end users have mechanisms to report incidents? Which ones:			
How?			
Is a criterion defined for determining categories of actions and responses to be taken based on severity and priority levels?			
Are defined the minimum and maximum amounts of time needed to resolve an incident?			
Does your organization have mechanisms in place to automatically detect incidents?			
If support staff visit the customers during the resolution of an incident:			
• They ask for further incidents?			
• A separate incident record is logged for each additional incident?			
Are defined incident models for known errors?			

The answers available were “Yes”, “No”, “in implementation” and “not applicable” (N/A). The N/A response was given in cases where the activity had no business sense to the organization. For example:

- Which of the following aspects contribute to define the incident priority:
Risk to life?

Risk to life is a concern that does not apply to all kind of organizations and industries. It makes sense to some industries but is N/A to others.

The header of the questionnaire has some generic questions about the company and the interviewee (Table 27).

Table 27- Questionnaire header

<u>Interviewee</u>	
Name	
Post	
Years of experience	
<u>Company</u>	
Name	
Industry	
Number of employees	
Number of IT employees	
Multinational	

Yet, since different organizations have different contexts and such context identification is crucial for future results generalization [18] I also included some questions like the IT Strategy and IT Structure of the organization, the IT framework used and what maturity level of IM process they think that have (Table 28).

Table 28- Questionnaire header 2

Regarding the IT Strategy, what kind(s) of IT strategy is(are) used? (Note: More than 1 (one) option can be chosen)	
• IT for comprehensiveness	
• IT for flexibility	
• IT for efficiency	
Regarding the IT structure what is the structure used in the organization? (Note: Only 1 (one) answer is available)	
• Centralized	
• Decentralized	
• Federal	
What maturity level do you think your organization is regarding incident management process?	
• 1?	
• 2?	
• 3?	
• 4?	
• 5?	
Did you perform an official implementation of incident management process adopting some of the following IT frameworks?	
• CMMI?	
• COBIT?	
• ITIL?	
• None?	

These questions were not randomly chosen. They have a clear and defined purpose. Some have been referred in various thesis and research articles in this area. In this particular case, I have:

- **Industry**

IT has a wide range of applicability across almost all industries [36], [37]. IM process is present in different and almost all type of industries.

- **Number of employees**

The size of the company influences IT Governance [37], [38]. In this way, that's important to have different sizes of organizations in order to test our proposal. There are also evidences that many small organizations lack standardized project management practices [37], [38], [39].

- **Number of IT employees**

In order to analyse the capacity of their IT Department to implement all IM process. Probably a larger department will have greater capacity and time to analyses metrics and do a predictive analysis.

- **Multinational**
An important factor to understand how the process of IM behaves in exclusively national or multinational organizations.
- **Culture**
Each organizational culture is a set of habits, values, thoughts and beliefs. In organization-level development areas such as health, safety, quality and environment, the habits are the keystones that affect the culture the most [40]. An organizational culture that prioritizes coordinated response to incidents is vital for monitoring and managing an IT infrastructure [41].
- **IT Strategy**
Some research projects focus on how strategic alignment impacts business performance [37], [42]. With different IT strategies will be different the approach of the IM process and use that will give the metrics.
- **IT Structure**
The structure of IT is one of the major recurring issues in the literature [37], [38], [43], [44], [45], [46], [47]. Organization structure is the necessary condition to the achievement of business goals by organizations [37], [48].
- **Maturity Level**
It is useful to compare the maturity level expected by the organizations and the effective level of maturity in IM process.
- **IT Framework**
In order to understand if the organization implements some IT framework. This information is used to compare with the activities they implemented and with their framework. It is also useful to understand if the process is more operational or management.

This information can be very useful to generalize conclusions/results in further researches [18].

Chapter 5 - Analysis and discussion of results

The interviews were applied in 7 organizations from various industries, sizes and IT Strategies. In Table 29 it is possible to see such heterogeneity.

Table 29- Organizations Comparison

Industry	Size	IT employees	Multinational	IT Strategy	IT Structure	Culture
Education	1.287	20	No	Flexibility and Efficiency	Centralized	The pyramidal organization
Retailing	6.000	4	Yes	Efficiency	Federal	The pyramidal organization
Conglomerate	360.000	7500	Yes	Efficiency	Decentralized	Well oiled machine
Electricity, Telecommunications and Automation	1.300	9	Yes	Flexibility	Decentralized	The pyramidal organization
Health	2.700	9	No	Flexibility and Comprehensiveness	Centralized	The pyramidal organization
Telecommunications	-----	-----	No	Comprehensiveness and Efficiency	Decentralized	The pyramidal organization
Pharmaceuticals	42.000	1320	Yes	Efficiency	Federal	Contest

The duration of the interviews also varied considerably. The longest took 1h35m and the shortest one took 45m. At the end, we had 470 minutes of interviews (8 hours approximately).

It is possible that the interviewed organizations have considerable dimensions. All of them have more than 1000 employees and considerable IT Departments. In the case of telecommunications organization, it will not possible to obtain the dimension until the conclusion of the thesis. However, they indicated that it would be of a considerable size.

The IT Strategy changes, with a little focus on efficiency, as can be seen in Figure 10. The IT Structure have more incidence in a Decentralized Structure but I have a Centralized and Federal Structure too (Figure 11).

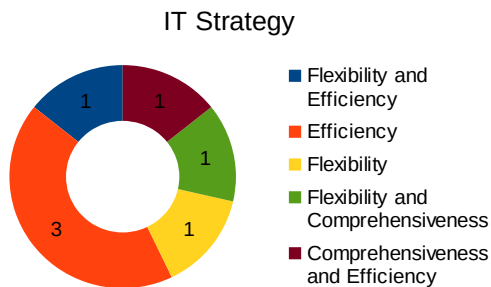


Figure 10- IT Strategy

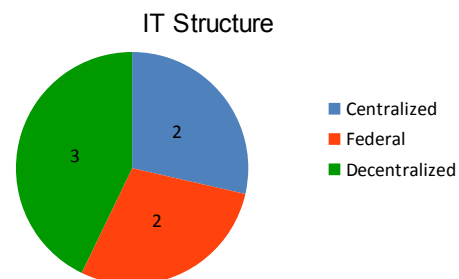


Figure 11- IT Structure

Relatively to the culture of each organizations, this designation was made through what is defined by Matthyssens and Wursten. [49]

From Figure 12 it's possible to conclude the maturity level expected for each company and the final result.

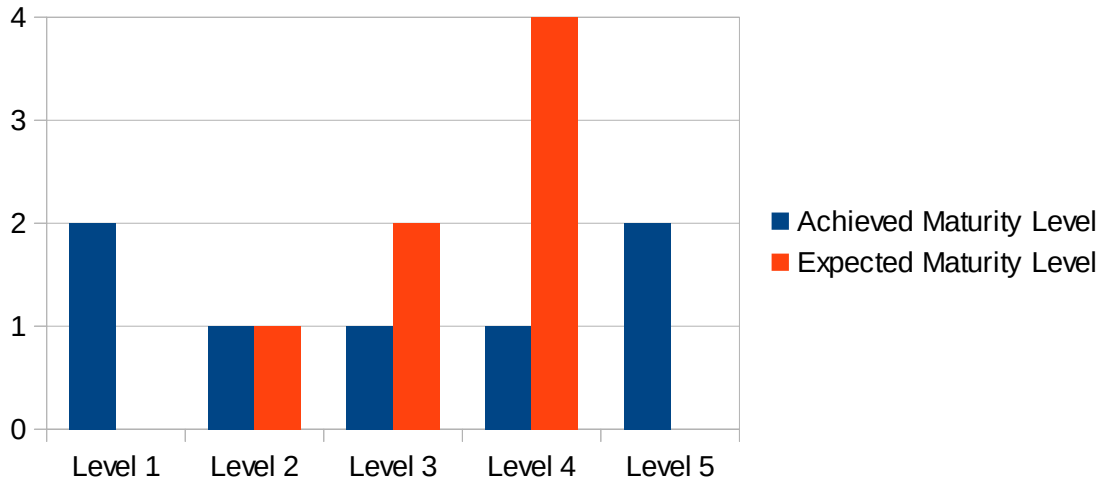


Figure 12- Expected and achieved Maturity Level

In order to achieve a more global vision, in Figure 13 it is possible to see the percentage of complete activities in each level of maturity per company.

Based on the information in this figure, it was possible to conclude that maturity level 4 was the lowest in general.

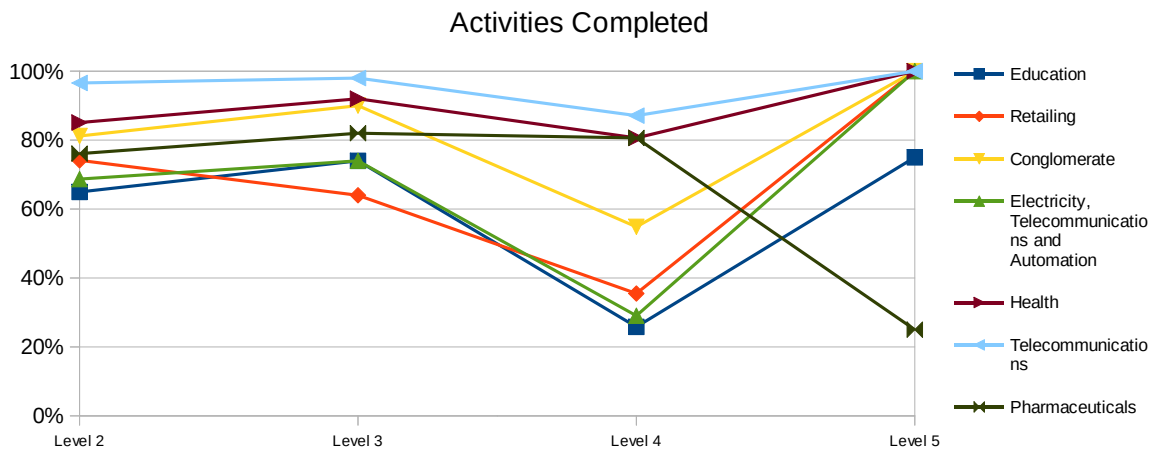


Figure 13- Activities Completed by Maturity Level

In Figure 14 is shown the average of activities by of all organizations per maturity level.

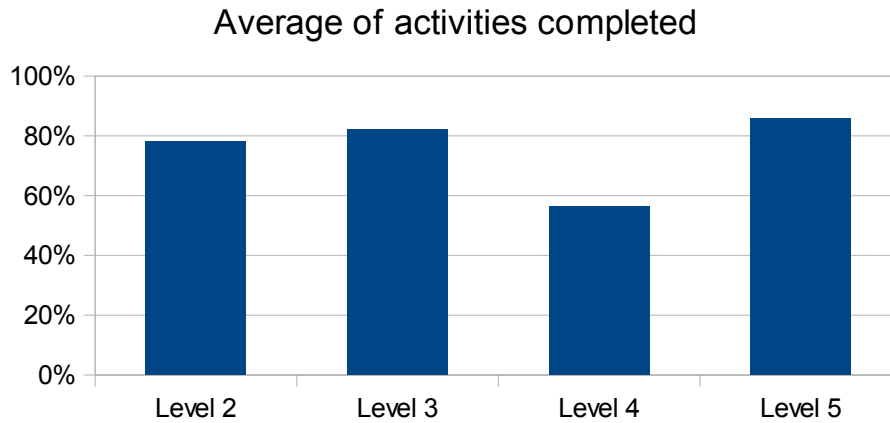


Figure 14- Average of activities completed

I can conclude that in average the levels 2, 3 and 5 are greater than the limited defined to reach the next level of maturity (75%). On the other hand, the level of maturity 4 was the most lower and the average didn't reach 60%.

In an evaluation of higher level, it's possible to conclude that the organizations apply most of the activities of planning and execution but don't analyze metrics and measures for continuous improvement and predictive analysis.

On the other hand, it was possible to make an analysis of the interview from the point of view of the frameworks. From all organizations interviewed most use the best known and used worldwide ITIL. On the other hand, the remaining organizations do not use any framework for management of IT processes (Figure 15).

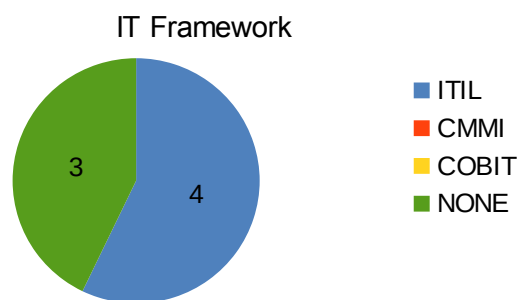


Figure 15- IT framework distribution

It is possible to see the distribution of the 207 activities by framework in Figure 16.

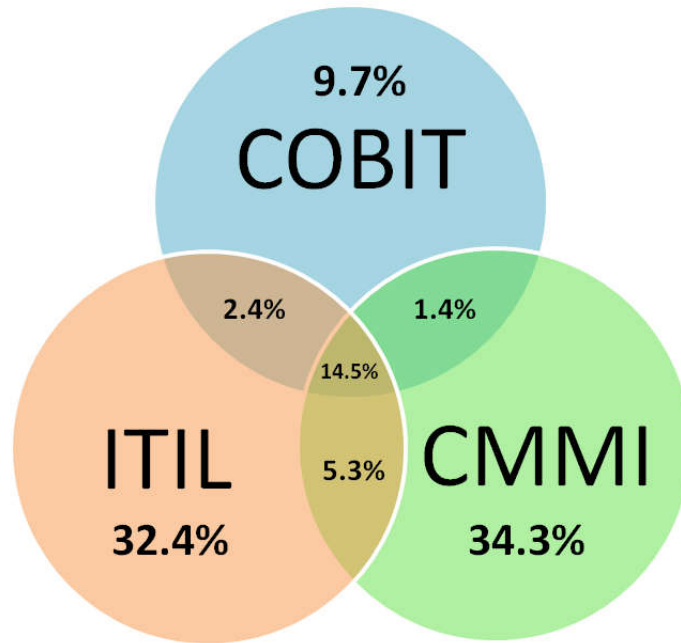


Figure 16- Distribution of activities by framework

In Figure 16 is possible to verify that the distribution of activities is similar in ITIL and CMMI framework. The total of activities that includes ITIL framework is 54,6%, 55,5% for CMMI and 28% for COBIT.

The distribution of the activities carried out by the 7 organizations was also average (Figure 15).

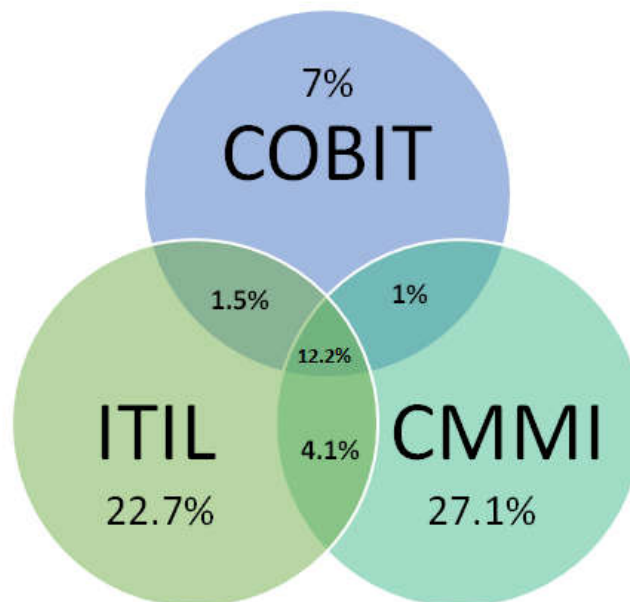


Figure 17- Distribution of activities completed by framework

Figure 17 shows us that the most used framework, in average is CMMI. Exclusive activities used by CMMI framework represent 27,1% in a total of 34,3%. On the other hand, the total of activities that includes CMMI framework represent 44,4% and 40,5% to ITIL. This means a percentage drop in ITIL relative to CMMI. In other words, CMMI is the framework most used by organizations, although none of them have mentioned that it uses it.

From possible 9,7% of COBIT framework was completed on 7%. On the other hand, the total of activities completed that includes this framework was 21,7% in comparison of the total of 28%.

In a total of 207 activities, only 1 wasn't implemented by the 7 organizations. The activity, is level 4 of maturity and is exclusive of CMMI framework.

The activity is:

- Number of times the IM system is accessed and for what purpose.

At first glance, this metric may seem futile and inappropriate. But from the point of view of IT security and audit can become relevant.

Moreover, there are some activities that are completed by all organizations. Most of them are level 2 of maturity model. They are all listed in Table 30.

Table 30- Activities completed by all organizations

Activities	Maturity Level	Framework
Are defined methods and secure tools to execute incident management process?	2	C
How many categorization levels are use:		
· One?	2	I
· Two?		
· Four?		
· Other?		
Costumer and end users have mechanisms to report incidents?	2	CI
To ensure consistent approaches for handling incidents is defined criteria for problem registration?	2	Co
Does the incident management tool allow the escalation and transfer of incidents among groups?	2	I
Incident knowledge sources are defined?	2	Co
Are determined actions that must be taken to address the incident?	2	C
Is an initial diagnosis made?	2	I

If a related problem or know error does not already exist and if the incident satisfies agreed-on criteria for problem registration, is a new problem logged?	2	C
Which of the following activities are performed during the investigation:		
· Understand the chronological order of events?	2	I
· Confirm the full impact of the incident:		
-Number of users affected?	2	I
-Range of users affected?	2	I
· Identify any events that could have triggered the incident?	2	I
Which of the following aspects contribute to define the incident priority:		
· The number of services affected?	2	CI
· Effect on business reputation?	2	CI
Is it possible to override normal priority levels?	2	I
Incident's priority can change if:		
· Circumstances change?	2	I
Is there a second line support?	2	I
Is the incident addressed using a workaround?	2	C
Are identified underlying causes of incidents?	2	C
Are incidents escalated until the underlying causes be discovered?	2	C
Is the action proposal communicated to relevant stakeholders?	2	C
Is the workaround communicated to relevant stakeholders?	2	C
If required are performed recovery actions?	2	Co
When a possible resolution is identified, the actions undertaken involve:		
· Asking the user to undertake directed activities	2	I
· The Service Desk implementing the resolution remotely or centrally	2	I
· Specialist support groups being asked to implement a resolution	2	I
When a resolution is found, is done a testing to ensure that recovery action is complete?	2	I
Are the incidents that meet the criteria for closure closed?	2	CICo
Exist a pre-defined 'standard' Incident Models?	2	I
Are provided adequate resources for:		
· Performing the process	2	C
The resources provided are:		
· Help desk tools?	2	C
· Incident management systems?	2	C
Are people trained for performing or supporting the process?	2	C
Incident Records include the following data:		
· Unique reference number?	3	CICo
· Incident classification?	3	CICo
· Data and time of recording?	3	CICo
· Name and identity of the person recording the incident record?	3	CICo

· Name and identity of the person updating the incident record?	3	CICo
· Method of notifications?	3	CICo
· Description of incident symptoms?	3	CICo
· Support group/person to which incident is allocated?	3	CICo
· Incident Status?	3	CICo
· Incident category?	3	CICo
· Incident urgency?	3	CICo
· Incident priority?	3	CICo
· Closure details including:		
-Time?	3	CICo
-Action taken?	3	CICo
-Person of closing the record?	3	CICo
· Details of any actions taken to try to:		
-Diagnose incident?	3	CICo
-Resolve incident?	3	CICo
A full historical record is maintained?	3	Co
The workaround is:		
· Planed?	3	C
If the resolution can be used as future knowledge sources, are incident resolution:		
· Documented?	3	Co
· Assessed?	3	Co
The communication with customers and end users are recorded?	3	C
Incidents are analyzed by category?	4	Ico
Is the integrity of the incident management tools and its contents maintained?	3	C
Are timely reports:		
· Produced?	4	Co
Which of the following measures and work products are used in monitoring and controlling:		
· Total number of incidents	4	CI
Are identified and corrected the root causes of defects and other problems in the process?	5	C

It's possible to see what maturity level corresponds to each activity, and what frameworks are included. It can be just CMMI I, ITIL (I) or COBIT (Co). It also can be a merge of frameworks like CMMI and ITIL (CI) or all 3(CICo).

The authors also asked a few questions to collect the opinion of the interviewees about the maturity model. These questions are important to assess the validity of our proposal and consequently the research question under study. As can be seen at Table 31, interviewees' opinion about the proposed IM maturity model is positive.

Table 31 - Interviewees' opinion about IM process maturity model

	Completeness	Missing activities	Usefulness
Interview 1	Exhausting	No	Yes
Interview 2	Very	No	Yes
Interview 3	Yes	Differentiate the 2 nd from the 3 rd line	Very
Interview 4	Very	No	Yes
Interview 5	Yes	No	Yes
Interview 6	Yes	No	Yes
Interview 7	Yes	No	Yes, very curious about the result

Chapter 6 – Conclusions

The main objective of this thesis is to solve the problems presented in the Chapter 1 and to elicit conclusions about the validity of the formulated research question.

Remember that P1: Many IT Frameworks overlap each other, which was the first problem identified. In fact, this problem is verified through the State of the Art and the survey of the different IT Frameworks. The most used in the business world were analyzed and the overlap exists in the most diverse process. With this thesis, it is not only possible to strengthen such statement from the peers as well as to solve P1 with our proposal by eliminating the IT frameworks overlap regarding IM process.

Relative to P2: The lack of completeness in the Maturity Models, once again was proved in theoretical and practical way. In fact, after the questionnaire, everyone found it useful, complete and came up with new ideas to improve their IM process. It's clear that implementing an IT framework is not easy. Several organizations fail it and something that could help them is still missing. If is difficult to an organization that uses a single IT Framework, how difficult can it be to different organizations that have not defined one yet? The maturity models assess the actual maturity and identify what is missing. Not a single interviewee stated that his organization use maturity models but all agreed on their importance.

It is also curious to notice that 6 of the 7 organizations were not at the level of maturity they expected. These misalignment expectations of the state of this particular process can be risky.

In conclusion, the research question, “RQ: Is it possible to develop an overlap less IT Maturity Model?” was answered with all the previously described. This thesis proves that such artefact can be developed and remain useful and complete as pointed by the interviewees. In this case, was done to one of the most important (argued as being a quick-win of ITIL framework) of any IT Framework in order to test its credibility.

Although the final results of maturity levels are different, the variations within the levels are quite similar.

One of the more obvious conclusions is that in average, the level 4 of maturity is the lowest. Even the organizations that have level 5 of maturity in IM process are at the limit in level 4, what obviously lows their maturity. That means the organizations, even

implementing policies, documenting and planning procedures and measuring metrics don't use them it to improve their performance.

Other main conclusion is about the activity's level. In average, are done more activities from level 3 of maturity than from level 2. As level 2 is the one that corresponds to the lowest maturity of the activities it should be, in average the more complete. However, this does not happen. As a consequence, this fact lowers the efficiency of the activities implemented in the other higher levels.

In the case of the frameworks, even though none of the organizations indicated that they use the CMMI framework, they all carry out, in average, more exclusive activities of this framework. This is also influenced by the fact that the total amount of activities is higher in CMMI. In fact, the distribution of completed activities is most similar to the distribution of total activities by framework.

Is proposed a Maturity Model for IM process. However, it is not clear that the same conclusion elicited in this research for the IM process can be automatically generalized to the remaining processes. Therefore, future research can pass by develop similar maturity models for the remaining processes of IT Framework's. The need of organizations has in assess the entire spectrum of processes is crucial to any IT framework implementation or even for a process evolution.

The proposed IM Maturity Model can be used as a foundation for future research. In fact, to give a widespread and realistic support to this Maturity Model, is fundamental complement it with knowledge from others researches.

In this thesis, is performed a set of quantitative interviews, however more but more interviews must be performed not only to leverage conclusions about other organizations contexts, but also to reinforce the ones presented in this thesis.

A unique Maturity Model that could be applied by any organization to any IT Framework can represent a huge challenge, but would be extremely interesting to study its advantages.

Bibliography

1. Pereira, R., Silva, M., Lapão, L., 2014, Business/IT Alignment through IT Governance Patterns in Portuguese Healthcare
2. Henderson, J.C., & Venkatraman, N., 1993, Strategic Alignment: Leveraging Information Technology for Transforming Organizations. *IBM Systems Journal*, 32(1), 4-16.
3. Gacenga, F., Cater-Steel A., Toleman, M., 2014, An International Analysis of IT Service Management Benefits and Performance Measurement.
4. Y. Sekhara, H. Medromi, A. Sayouti, 2014, Multi-Agent Architecture for implementation of ITIL Processes: Case of IM Process
5. Barash, G., Bartolini, C., Wu, L., 2007, Measuring and Improving the Performance of an IT Support Organization in Managing Service Incidents
6. SEI, S. E. I., CMMI® for Services, Version 1.3., 2010
7. Yoo, C. et al., 2006, A unified model for the implementation of both ISO 9001:2000 and CMMI by ISO-certified organizations. *The Journal of Systems and Software*, Volume 79, pp. 954 - 961.
8. Institute, I. G., COBIT 4.1. USA: IT Governance Institute, 2007
9. Sahibudin, S., Sharifi, M., & Ayat, M., 2008, Combining ITIL, COBIT and ISO/IEC27002 in Order to Design a Comprehensive IT Framework in Organizations. In: *Proceedings of the Second Asia International Conference on Modeling & Simulation*, AMS, IEEE, Kuala Lumpur, Malaysia, pp. 749-753
10. Rocha, A., Vasconcelos, J, 2004, “Maturity models for information systems management. (Os modelos de maturidade na gestão de sistemas de informação, in Portuguese),” in: *Journal of the Faculty of Sciences and Technology at University Fernando Pessoa*, N° 1, pp. 93-107
11. Bruin, T., Rosemann, M., Freeze, R., KulKarni, U., 2005, “Understanding the main phases of developing a maturity assessment model,” in: *16th Australian Conference on Information Systems (ACIS)*, Sydney
12. Becker, J., Knackstedt, R., Pöppelbuß, J, 2009, “Developing maturity models for IT management – A procedure model and its application,” in: *Journal Business & Information Systems Engineering (BISE)*, Volume 1, Number 3. B&ISE
13. Alshathry O., 2016, Maturity Status of ITIL IM Process among Saudi Arabian Organizations
14. James J. Cusick & Gary M., 2010, *Creating an ITIL Inspired Incident Management Approach: Roots, Response and Results*
15. UCISA, 2016, *A guide to Incident Management*
<https://www.ucisa.ac.uk/representation/activities/ITIL/serviceoperation>
16. I. Ghrab, M. Ketata, Z. Loukil, F. Gargouri, 2016, Using constraint programming techniques to improve incident management process in ITIL
17. Trinkenreich B., Santos G., 2015, Avaliação da Gerência de Incidentes sob a Luz do MR-MPS-SV e Medição para Apoiar a Melhoria da Qualidade do Serviço de TI
18. Pereira, R., Silva, M., 2012, Designing a new Integrated IT Governance and IT Management Framework Based on Both Scientific and Practitioner Viewpoint
19. OGC, ITIL V3 - Service Operation, 2007
20. Kari Saarelainen, Marko Jantti, 2015, *Quality and Human Errors in IT Service Infrastructures*
21. OGC, ITIL V3 - Service Design, 2007
22. A. Bovim, K. Johnston, S. Kabanda, M. Tanner and A. Stander, 2014, ITIL adoption in South African: A capability Maturity view

23. BMC, 2017, ITIL Processes & Best Practices, <http://www.bmc.com/guides/itil-introduction.html>
24. COBIT 5: Enabling Processes, 2012
25. CMMI for Services V1.3, 2010
26. CIO, 12/2016, Capability Maturity Model Integration, Definition and Solutions, <http://www.cio.com/article/2437864/process-improvement/capability-maturity-model-integration--cmmi--definition-and-solutions.html>, 12/2016
27. CMMI for Development, Version 1.3, 2010
28. COBIT 5: Process Assessment Model (PAM), 2013
29. ISO, 11/2016, IT – Process assessment- Part 4: Guidance on use for process improvement and process capability determination, <https://www.iso.org/obp/ui/#iso:std:iso-iec:15504:-4:ed-1:v1:en>
30. AXELOS - ITIL® Service Design. TSO (The Stationery Office), 2007
31. J. Flores, L. Rusu and P. Johannesson, 2011, A Maturity Model of IT Service Delivery
32. Pereira R., Silva M., 2010, A maturity Model for Implementing ITIL V3
33. M. Vitoriano and J. Neto, 2015, Information Technology Service Management Processes Maturity in the Brazilian Federal Direct Administration
34. M. Simonsson, P. Johnson and H. Wijkstrom, 2007, Model-Based IT Governance Maturity Assessments with COBIT
35. The University of Manchester, 2017, Research Methodology, http://www.humanities.manchester.ac.uk/studyskills/assessment_evaluation/dissertations/methodology.html
36. Tanriverdi, H., 2006. Performance Effects of Information Technology Synergies in Multibusiness Firms. *Management Information Systems Quarterly*, MISQ, 30(1), 57-77.
37. Pereira, R., 2014, A Framework for Implementing IT Governance
38. Sambamurthy, V., Zmud, R.W., 1999, Arrangements for Information Technology Governance: A Theory of Multiple Contingencies. *Management Information Systems Quarterly*, MISQ, 23(2), 261-290
39. Cochran, M., 2010, Proposal of an Operations Department Model to Provide IT Governance In Organizations that Don't have IT C-Level Executives. In: *Proceedings of the 43rd Hawaii International Conference on System Sciences*, HICSS, IEEE, Honolulu, HI, pp.1-10.
40. Vesterinen, A., 2017, <https://blog.planbrothers.io/en/why-incident-reporting-is-indispensable>
41. Tozzi, C., 2017, A Coordinated Response Culture for Incident Management, <https://www.pagerduty.com/blog/coordinated-response-culture-incident-management/>
42. Simonsson, M., Johnson, P., & Ekstedt, M., 2008, IT Governance Decision Support Using the IT Organization Modeling and Assessment Tool. In: *Proceedings of the Management of Engineering & Technology*, Cape Town, South Africa, pp. 802-810
43. Adams, C.R., Larson, E.C., & Xia, W., 2007, IS/IT Governance Structure and Alignment: An Apparent Paradox. In: *Proceedings of the 2007 Society for Information Management Academic Work-Shop (SIM Academic Workshop)*, Montreal, Canada.
44. Gallagher, K.P., Worrel, J.L., 2008, Organizing IT to Promote Agility. *Information Technology Management*, 9(1), 71-88

45. Goeken, M., Alter, S., 2008, Representing IT Governance Frameworks as Metamodels. In: Proceedings of the International Conference on E-Business, Enterprise Information Systems, E-Government, and Outsourcing, ICEE, IEEE, Nevada, USA, pp.48-54.
46. King, J.L., 1983, Centralized versus Decentralized Computing: Organizational Considerations and Management Options. *Computing Survey*, 15, 320-349.
47. Peak, D.A., Azadmanesh, M.H., 1997, Centralization/Decentralization Cycles in Computing: Market Evidence. *Information & Management*, 31, 303-317.
48. Gao, S., Chen, J., & Fang, D., 2009, The Influence of the Capability on Dimensions of Organization Structure. In: Proceedings of the Second International Conference on Future Information Technology and Management Engineering, FITME, IEEE, Sanya, China, pp. 269-273.
49. Matthyssens, P., Wursten, H., 2003, Internal marketing in: Rugimbana, R., Nwankwo, S. (Eds.), *Cross-Cultural Marketing*, Thomson Learning, Australia.
50. Select – Business Solutions, 2017, What is a Maturity Model, <http://www.selectbs.com/process-maturity/what-is-the-capability-maturity-model>

Appendix

Appendix A

CMMI			
Specific Goals	Specific Practices	Activities	ID
SG 1 Prepare for Incident Resolution and Prevention	SP 1.1 Establish an approach to Incident Resolution and Prevention	Is define criteria for determining what an incident is?	A1
		For determining which categories an incident belongs to is defined:	
		• Categories?	A2
		• Criteria?	A3
		Is described how responsibility for processing incidents is assigned and transferred?	A4
		Customer and end users have mechanisms to report incidents?	A5
		Are defined methods and secure tools to use for incident management?	A6
		All relevant customers and end users who may be affected by a report incident are notified? How?	A7
		Are defined criteria for determining categories of actions and responses to be taken based on severity and priority levels?	A8
		Are defined criteria for determining severity and priority levels?	A9
		Is identify requirements on the amount of time defined for the resolution of incidents in the service agreement?	A10
	Are documented criteria that define when an incident should be closed?	A11	
	SP 1.2 Establish an Incident Management System	Is ensured that the incident management system allows the escalation and transfer of incidents among groups?	A12
		Is ensured, in incident management system, that incident information that is useful to the resolution and prevention of incidents is:	
		• Storage?	A13
		• Update?	A14
		• Retrieval?	A15
• Reporting?		A16	
Is maintained the integrity of the incident management system and its contents?	A17		
SP 2.1 Identify and Record Incidents	Are identified incidents that are in scope?	A18	
	Is recorded information about the incident?	A19	
	Is categorized the incident?	A20	

SG 2 Identify, Control and Address Incidents	SP 2.2 Analyze Incident Data	Is Analyzed incident data?	A21	
		Is determined which group is best suited to take action to address the incident?	A22	
		Is a determined action that must be taken to address the incident?	A23	
		Actions to be taken are planed?	A24	
	SP 2.3 Apply Workarounds to selected Incidents.	The incident is addressed using the workaround?	A25	
		Are managed the actions until the impact of the incident is at an acceptable level?	A26	
		Are recorded the actions and results for apply workarounds to selected incidents?	A27	
	SP 2.4 Address Underlying causes of selected Incidents	Are addressed the underlying causes using the action proposal that resulted from the analysis of the incidents underlying causes?	A28	
		Are manager the actions until the underlying causes is addressed?	A29	
		Are recorded the actions and results for address underlying causes of selected incidents?	A30	
	SP 2.5 Monitor the status of incident to closure	Until they meet the terms of the service agreement and satisfy the incident submitter as appropriate, incidents are:		
		• Documented actions?	A31	
		• Monitored and tracked?	A32	
		Is reviewed the resolution of the incident?	A33	
		Is confirmed the results with relevant stakeholders?	A34	
		Are closed incidents that meet the criteria for closure?	A35	
	SP 2.6 Communicate the Status of Incidents	The communication with customers and end users are recorded?	A36	
	SG 3 Define Approaches to Address Selected Incidents	SP 3.1 Analyze Selected Incident Data	Are identified underlying causes of incidents?	A37
			Is recorded information about the underlying causes of an incident or group of incidents?	A38
			Are conduct causal analysis with the people who are responsible for performing related tasks?	A39
SP 3.2 Plan actions to address underlying causes of selected incidents		Is determined which group is best suited to address the underlying cause?	A40	
		Is determined the actions to be taken to address the underlying cause?	A41	
		Is documented the actions to be taken in an action proposal?	A42	
		Is verified and validated the action proposal to ensure that it effectively addresses the incident?	A43	

		Is communicated the action proposal to relevant stakeholders?	A44	
	SP 3.3 Establish Workarounds for selected incidents	Is determine which group is best suited to establish and maintain a workaround?	A45	
		The workaround is:		
		• Planed?	A46	
		• Documented?	A47	
		Is verified and validate the workaround to ensure that it effectively addresses the incident?	A48	
			Is communicated the workaround to relevant stakeholders?	A49
	GG 2 The process is institutionalized as a managed process.	GG 2 The process is institutionalized as a managed process.	GP 2.1 Is establishes and maintains an organizational policy for planning and performing the process?	A51
			Incidents are:	
			• Identified?	A52
			• Controlled?	A53
			• Addressed?	A54
			For selected incidents is determined:	
			• Workarounds?	A55
			• Underlying causes?	A56
			GP 2.2 Is established and maintains the plan for performing the process based on volume and type of service incidents?	A57
			GP 2.3 Are provided adequate resources for performing the process, developing the work products, and providing the services of the process?	A58
			The resources provided are:	
			• Help desk tools?	A59
			• Remote analysis tools?	A60
• Automated monitoring tools?			A61	
• Incident management systems?	A62			
		GP 2.4 Responsibility and authority is assigned for:		
		• Performing the process?	A63	
		• Developing the work products?	A64	
		• Providing the services of the process?	A65	
		GP 2.5 Are people trained for performing or supporting the process?	A66	
		The topics included in training people are:		
		• Service incident criteria?	A67	
		• Interacting with those who report service incidents and those who are affected by them?	A68	
		• Incident management system?	A69	
• Analysis techniques?	A70			

		GP 2.6 Are place designated work products of the process under appropriate levels of control?	A71
		The work products under control are:	
		• Incident management records?	A72
		• Incident resolution and prevention reports?	A73
		• Action proposals?	A74
		• Workaround description and instructions?	A75
		• Incident database copies?	A76
		GP 2.7 Are identified and involved the relevant stakeholders of the process as planned?	A77
		Stakeholders are involved in the activities:	
		• Establishing an approach to incident resolution and prevention?	A78
		• Identifying service incidents and recording information about them?	A79
		• Analyzing service incidents to determine the best course of action?	A80
		• Reviewing the result of actions for resolving service incidents?	A81
		GP 2.8 Are monitored and controlled the process against the plan for performing the process and take appropriate corrective action?	A82
		The measures and work products used in monitoring and controlling are:	
		• Capacity, performance, and availability data that signal potential service incidents?	A83
		• Number of service incidents received?	A84
		• Lead time for resolving service incidents compared to the lead times defined in the service level agreement?	A85
		• Number of transfers between support groups before a service incident is resolved?	A86
		Is scheduled for implementing an action proposal to prevent a class of service incidents from reoccurring?	A87
		GP 2.9 Is objectively evaluated the adherence of the process against its process description, standards, and procedures, and address noncompliance?	A88
		The activities reviewed are:	

	<ul style="list-style-type: none"> Establishing an approach to incident resolution and prevention? 	A89
	<ul style="list-style-type: none"> Identifying service incidents and recording information about them? 	A90
	<ul style="list-style-type: none"> Communicating the status of service incidents? 	A91
	The work products reviewed are:	
	<ul style="list-style-type: none"> Service incident database? 	A92
	<ul style="list-style-type: none"> Workarounds? 	A93
	<ul style="list-style-type: none"> Action proposals? 	A94
	<ul style="list-style-type: none"> Service incident records? 	A95
	GP 2.10 Are reviewed with higher level management:	
	<ul style="list-style-type: none"> Activities? 	A96
	<ul style="list-style-type: none"> Status? 	A97
	<ul style="list-style-type: none"> Results? 	A98
ITIL		
Area	Activities	ID
Timescales	Support groups are fully aware of timescales?	B1
	Service Management tools are used to automate timescales?	B2
	Service Management tools are used to automate escalate the incident?	B3
Incident Models	Is used a pre-defined 'standard' Incident Models?	B4
	The incident Model includes:	
	<ul style="list-style-type: none"> The steps that should be taken to handle the incident? 	B5
	<ul style="list-style-type: none"> The chronological order of these steps should be taken in? 	B6
	<ul style="list-style-type: none"> Timescales and thresholds for completion of the actions is define? 	B7
	<ul style="list-style-type: none"> Escalation procedures are set? 	B8
	The incident model is input to the incident-handling support tools?	B9
	The support tools automated:	
	<ul style="list-style-type: none"> Handling of the process? 	B10
	<ul style="list-style-type: none"> Management of the process? 	B11
Major Incidents	Is a separated procedure used for major incidents?	B13
	A definition of what constitutes a major incident is agreed and mapped on the incident prioritization system?	B14
	If necessary, separated major incident team, under the direct leadership of Incident Manager, is create to concentrate on this incident alone to ensure that adequate resources and focus?	B15
Incident Identification	Key components are monitored?	B16
Incident Logging	Does your organization have channels in place to receive incidents notifications?	B17
	How can received incidents notifications:	

	<ul style="list-style-type: none"> • By phone? 	B18
	<ul style="list-style-type: none"> • Other? 	
	Detail:	B19
	Does your organization have mechanisms in place to automatically detect incidents?	B20
	Are incidents reported and/or detected logged?	B21
	If support staff visit the customers:	
	<ul style="list-style-type: none"> • They ask for further incidents? 	B22
	<ul style="list-style-type: none"> • A separate incident record is logged for each additional incident? 	B23
	Each incident includes the information:	
	<ul style="list-style-type: none"> • Unique reference number? 	B24
	<ul style="list-style-type: none"> • Categorization? 	B25
	<ul style="list-style-type: none"> • Urgency? 	B26
	<ul style="list-style-type: none"> • Impact? 	B27
	<ul style="list-style-type: none"> • Priorization? 	B28
	<ul style="list-style-type: none"> • Date/Time record? 	B29
	<ul style="list-style-type: none"> • Name/ID of the person and/or group recording the incident? 	B30
	<ul style="list-style-type: none"> • Method of notification? 	B31
	<ul style="list-style-type: none"> • Name/department/phone/location of user? 	B32
	<ul style="list-style-type: none"> • Call-back method? 	B33
	<ul style="list-style-type: none"> • Description of symptoms? 	B34
	<ul style="list-style-type: none"> • Incident Status? 	B35
	<ul style="list-style-type: none"> • Related Configuration item? 	B36
	<ul style="list-style-type: none"> • Support group/person to which the incident is allocated? 	B37
	<ul style="list-style-type: none"> • Related Know Error? 	B38
	<ul style="list-style-type: none"> • Activities undertaken to resolve the incident? 	B39
	<ul style="list-style-type: none"> • Resolution Date and time? 	B40
	<ul style="list-style-type: none"> • Closure category? 	B41
	If Service Desk does not work 24/7 and the responsibility for the first-line passes to another group, they have equally rigorous about logging and incident details?	B42
Incident Categorization	How many categorization levels are user: <ul style="list-style-type: none"> • One? • Two? • Three? • Four? • Five or more? 	B43
Incident Priorization	Is there a criterion that defines the priority of the incidents and the actions that must be taken according to the priority in question?	B44
	Which of these aspects incident priorization is based on:	
	<ul style="list-style-type: none"> • Risk to life? 	B45
	<ul style="list-style-type: none"> • The number of services affected? 	B46
	<ul style="list-style-type: none"> • The level of financial losses? 	B47

	<ul style="list-style-type: none"> • Effect on business reputation? 	B48
	<ul style="list-style-type: none"> • Regulatory or legislative breaches? 	B49
	Clear guidance is provided for all support staff to enable them to determine the correct urgency and impact levels?	B50
	At no time, the normal priority levels are overridden?	B51
	Is define a priority level for VIPs?	B52
	Incident's priority can change if:	
	<ul style="list-style-type: none"> • Circumstances change? 	B53
	<ul style="list-style-type: none"> • Is not resolved within SLA target times? 	B54
Initial Diagnosis	In the initial diagnosis are use:	
	<ul style="list-style-type: none"> • Diagnostic scripts? 	B55
	<ul style="list-style-type: none"> • Know error information? 	B56
	If is possible and the incident was reported by telephone, Service Desk Analyst will resolve the incident while the user still on the telephone?	B57
	If is not possible to the Service Desk Analyst resolve a reported telephone incident, it:	
	<ul style="list-style-type: none"> • Inform the user of their intentions? 	B58
	<ul style="list-style-type: none"> • Give the user the reference number? 	B59
Incident Escalation	Attempt to resolve the maximum number of incidents in the first line of support?	B60
	Is there a second line support?	B61
	Is there a third line support?	B62
	If there is a second line and /or third line, is this requested when the first line is not capable of resolving the incident?	B63
	If multiple incidents have the same type of priority, is define which incident should be pick up and actively worked on?	B64
Investigation and Diagnosis	All activities of investigate and diagnose are documented in the incident record?	B65
	During the investigation is caring out:	
	<ul style="list-style-type: none"> • Establishing exactly what has gone wrong or being sought by the user? 	B66
	<ul style="list-style-type: none"> • Understanding the chronological order of events? 	B67
	<ul style="list-style-type: none"> • Confirming the full impact of the incident (number and range of users affected)? 	B68
	<ul style="list-style-type: none"> • Identifying any events that could have triggered the incident? 	B69
	<ul style="list-style-type: none"> • Knowledge searches looking for previous occurrences by searching: 	
	-Incident/Problem Record?	B70
	-Know Error Database?	B71
	-Knowledge Databases?	B72
-Manufactures/suppliers Error Logs?	B73	
Resolution and Recovery	When a potential resolution has been identified the actions undertaken involve:	
	<ul style="list-style-type: none"> • Asking the user to undertake directed activities? 	B74
	<ul style="list-style-type: none"> • The Service Desk implementing the resolution remotely or centrally? 	B75

	<ul style="list-style-type: none"> Specialist support groups being asked to implement a resolution? 	B76
	<ul style="list-style-type: none"> A third-party supplier or maintainer being asked to resolve the fault? 	B77
	When a resolution has been found, is done a testing to ensure that recovery action is complete?	B78
	If is necessary two or more groups take recovery actions in the same incident, Incident Management coordinate the activities and liaise with all parties involved?	B79
	When incident is resolved, the resolving group pass the incident back to Service Desk for closure action?	B80
Incident Closure	When the Service Desk check that incident is fully resolved, it verify:	
	<ul style="list-style-type: none"> That user is satisfied? 	B81
	<ul style="list-style-type: none"> That user agrees the incident can be closed? 	B82
	<ul style="list-style-type: none"> That closure categorization is correct or if it changes from the initial incident categorization? 	B83
	<ul style="list-style-type: none"> A user satisfaction call-back or e-mail survey for the agreed percentage of incidents is done? 	B84
	<ul style="list-style-type: none"> If is a recurring problem and decide to take any preventive action? 	B85
	<ul style="list-style-type: none"> If incident is formally close? 	B86
	Automatic closure period its applied to:	
	<ul style="list-style-type: none"> All incidents? 	B87
	<ul style="list-style-type: none"> Specific Incidents? 	B88
	<ul style="list-style-type: none"> None? 	B89
	An incident can be re-open after closure?	B90
	If a problem recurs from a close incident, how many work days, can be possible re-open: <ul style="list-style-type: none"> One? Two? Three? More? 	B91
	If a problem recurs from a closure incident and it can't be re-open, a new incident is open and linked to the previous incident?	B92
Information Management	The incident management tools contain information about:	
	<ul style="list-style-type: none"> Incident and problem history? 	B93
	<ul style="list-style-type: none"> Incident categories? 	B94
	<ul style="list-style-type: none"> Action taken to resolve incidents? 	B95
	<ul style="list-style-type: none"> Diagnostic scripts? 	B96
	Incident Records include the following data:	
	<ul style="list-style-type: none"> Unique reference number? 	B97
	<ul style="list-style-type: none"> Incident classification? 	B98
	<ul style="list-style-type: none"> Data and time of recording? 	B99
	<ul style="list-style-type: none"> Name and identity of the person recording the incident record? 	B100

	<ul style="list-style-type: none"> Name and identity of the person updating the incident record? 	B101
	<ul style="list-style-type: none"> Name/organization/contact details of affected users? 	B102
	<ul style="list-style-type: none"> Description of incident symptoms? 	B103
	<ul style="list-style-type: none"> Incident category? 	B104
	<ul style="list-style-type: none"> Incident Impact? 	B105
	<ul style="list-style-type: none"> Incident urgency? 	B106
	<ul style="list-style-type: none"> Incident priority? 	B107
	<ul style="list-style-type: none"> Closure details including: 	
	<ul style="list-style-type: none"> -Time? 	B108
	<ul style="list-style-type: none"> -Category? 	B109
	<ul style="list-style-type: none"> -Action taken? 	B110
	<ul style="list-style-type: none"> -Person of closing the record? 	B111
	<ul style="list-style-type: none"> Relationship with other: 	
	<ul style="list-style-type: none"> -Incidents? 	B112
	<ul style="list-style-type: none"> -Problems? 	B113
	<ul style="list-style-type: none"> -Changes? 	B114
	<ul style="list-style-type: none"> -Know error? 	B115
	<ul style="list-style-type: none"> Details of any actions taken to try to: 	
	<ul style="list-style-type: none"> -Diagnose incident? 	B116
	<ul style="list-style-type: none"> -Resolve incident? 	B117
	<ul style="list-style-type: none"> -Re-create incident? 	B118
Metrics	Is the performance of Incident Management measured according to what is described in the execution plan?	B119
	With which data of the following:	
	<ul style="list-style-type: none"> Total number of incidents? 	B120
	<ul style="list-style-type: none"> Breakdown of incidents at each stage? 	B121
	<ul style="list-style-type: none"> Number and percentage of major incidents? 	B122
	<ul style="list-style-type: none"> Percentage of incidents handled within agreed response time? 	B123
	<ul style="list-style-type: none"> Size of the current incident backlog? 	B124
	<ul style="list-style-type: none"> Average cost per incident? 	B125
	<ul style="list-style-type: none"> Number of incidents re-open and as a percentage of the total? 	B126
	<ul style="list-style-type: none"> Number and percentage of incidents incorrectly assigned? 	B127
	<ul style="list-style-type: none"> Number and percentage of incidents incorrectly categorized? 	B128
	<ul style="list-style-type: none"> Percentage of incidents closes by the Service Desk? 	B129
	<ul style="list-style-type: none"> Number and percentage of the incidents processed per Service Desk agent? 	B130
	<ul style="list-style-type: none"> Number and percentage of incidents resolved remotely, without the need for a visit? 	B131
	<ul style="list-style-type: none"> Number of incidents handled by each Incident Model? 	B132

	<ul style="list-style-type: none"> Breakdown of incidents by time of the day, to help pinpoint peaks and ensure matching of resources? 	B133
	Is done a statistical management of the performance of one or more sub-processes that are critical to the performance of Incident Management?	B134

COBIT		
Management Practice	Activities	ID
DSS02.01 Define incident classification schemes.	Incident classification and prioritization schemes are defined?	C1
	To ensure consistent approaches for handling incidents is define criteria for problem registration?	C2
	The users are informed about and conducting trend analysis?	C3
	Are define incident models for known errors?	C4
	Are define incident escalation rules and procedures:	
	<ul style="list-style-type: none"> For major incidents? 	C5
	<ul style="list-style-type: none"> For security incidents? 	C6
	<ul style="list-style-type: none"> For all? 	C7
	Incident knowledge sources are defined?	C8
Incident knowledge use is defined?	C9	
DSS02.02 Record, classify and prioritize incidents	All incidents are log?	C10
	All relevant information is recorded?	C11
	A full historical record is maintained?	C12
	All incidents are classifying by:	
	<ul style="list-style-type: none"> Type? 	C13
	<ul style="list-style-type: none"> Category? 	C14
	Are incidents prioritized based on SLA service definition of business impact and urgency?	C15
DSS02.04 Investigate, diagnose and allocate incidents	Are identified and describe relevant symptoms of incident?	C16
	Are available knowledge resources to identify possible incident resolution?	C17
	If a related problem or know error does not already exist and if the incident satisfies agreed-on criteria for problem registration, is log a new problem?	C18
	Are incidents assigned to specialist functions if deeper expertise is need?	C19
DSS02.05 Resolve and recover from incidents	Are selected and applied the most appropriate incident resolutions?	C20
	When workarounds were used for incident resolution are record?	C21
	If required are performed recovery actions?	C22
	If the resolution can be used as future knowledge sources, are incident resolution documented and assess?	C23
DSS02.06 Close incidents	Is verify with the affected users that the incident has been satisfactory resolved?	C24
	Incidents are closed?	C25
	Are escalated incident:	

DSS02.07 Track status and produce reports	• Monitored?	C26
	• Request handling procedures?	C27
	Stakeholders are identifying?	C28
	Stakeholders needs for data or reports are identify?	C29
	Reporting frequency and medium to stakeholders are identify?	C30
	Incidents are analyzing by category and type?	C31
	In Incidents analysis are identify:	
	• Trends?	C32
	• Patterns of recurring issues?	C33
	• SLA breaches?	C34
	The information of incidents is used to continual improvement planning?	C35
	Is produced and distributed timely reports?	C36
	Is provided controlled access to online data?	C37

Appendix B

Activities	CMMI	ITIL	COBIT	Maturity Level	Type
Is define criteria for determining what an incident is?	A1			2	O
For determining which categories an incident belong to is defined:					
• Categories?	A2			2	O
• Criteria?	A3			2	O
Is describe how responsibility for processing incidents is assigned and transferred?	A4	B8		2	O
Costumer and end users have mechanisms to report incidents?	A5			2	O
Are defined methods and secure tools to use for incident management?	A6			2	O
All relevant customers and end users who may be affected by a report incident are notified? How?	A7			2	O
Are defined criteria for determining categories of actions and responses to be taken based on severity and priority levels?	A8			2	O
Is identify requirements on the amount of time defined for the resolution of incidents in the service agreement?	A10			2	O
Are identified and monitored incidents that are in scope?	A18	B16		2	O
Does your organization have channels in place to receive incidents notifications?		B17		2	O
How can received incidents notifications:					
• By phone?		B18		2	O
• Other?				2	O
Detail: _____		B19			
Does your organization have mechanisms in place to automatically detect incidents?		B20		2	O
Are incidents reported and/or detected logged?		B21	C10	2	O
If support staff visit the customers:					
• They ask for further incidents?		B22		2	O
• A separate incident record is logged for each additional incident?		B23		2	O

To ensure consistent approaches for handling incidents is define criteria for problem registration?			C2	2	O
The users are informed about and conducting trend analysis?			C3	2	O
Are define incident models for known errors?			C4	2	O
Are define incident escalation rules and procedures:					
• For major incidents?			C5	2	O
• For security incidents?			C6	2	O
• For all?			C7	2	O
Incident knowledge sources are defined?			C8	2	O
Incident knowledge use is defined?			C9	2	O
Each incident includes the information:					
• Unique reference number?		B24		2	O
• Categorization?	A20	B25	C14	2	O
• Urgency?		B26		2	O
• Impact?		B27		2	O
• Priorization?		B28		2	O
• Date/Time record?		B29		2	O
• Name/ID of the person and/or group recording the incident?		B30		2	O
• Method of notification?		B31		2	O
• Name/department/phone/location of user?		B32		2	O
• Call-back method?		B33		2	O
• Description of symptoms?		B34		2	O
• Incident Status?		B35		2	O
• Related Configuration item?		B36		2	O
• Support group/person to which the incident is allocated?		B37		2	O
• Related Know Error?		B38		2	O
• Activities undertaken to resolve the incident?		B39		2	O
• Resolution Date and time?		B40		2	O
• Closure category?		B41		2	O
• Type?			C13	2	O
If Service Desk does not work 24/7 and the responsibility for the first-line passes to another group, they have equally rigorous about logging and incident details?		B42		2	O
Incident Records include the following data:					
• Unique reference number?	A19	B97	C11	3	
• Incident classification?	A19	B98	C11	3	

• Data and time of recording?	A19	B99	C11	3	
• Name and identity of the person recording the incident record?	A19	B100	C11	3	
• Name and identity of the person updating the incident record?	A19	B101	C11	3	
• Name/organization/contact details of affected users?	A19	B102	C11	3	
• Description of incident symptoms?	A19	B103	C11	3	
• Incident category?	A19	B104	C11	3	
• Incident Impact?	A19	B105	C11	3	
• Incident urgency?	A19	B106	C11	3	
• Incident priority?	A19	B107	C11	3	
• Closure details including:					
-Time?	A19	B108	C11	3	
-Category?	A19	B109	C11	3	
-Action taken?	A19	B110	C11	3	
-Person of closing the record?	A19	B111	C11	3	
• Relationship with other:					
-Incidents?	A19	B112	C11	3	
-Problems?	A19	B113	C11	3	
-Changes?	A19	B114	C11	3	
-Know error?	A19	B115	C11	3	
• Details of any actions taken to try to:					
-Diagnose incident?	A19	B116	C11	3	
-Resolve incident?	A19	B117	C11	3	
-Re-create incident?	A19	B118	C11	3	
A full historical record is maintained?			C12	3	
Is analyzed incident data?	A21			3	O
Is determined which group is best suited to take action to address the incident?	A22	B63	C19	2	O
Is a determined action that must be taken to address the incident?	A23			2	O
Actions to be taken are planed?	A24			3	O
In the initial diagnosis are use:					
• Diagnostic scripts?		B55		2	O
• Know error information?		B56		2	O
If is possible and the incident was reported by telephone, Service Desk Analyst will resolve the incident while the user still on the telephone?		B57		2	O
If is not possible to the Service Desk Analyst resolve a reported telephone incident, it:					
• Inform the user of their intentions?		B58		2	O

<ul style="list-style-type: none"> Give the user the reference number? 		B59		2	O
Are identified and describe relevant symptoms of incident?		B66	C16	2	O
If a related problem or know error does not already exist and if the incident satisfies agreed-on criteria for problem registration, is log a new problem?			C18	2	O
All activities of investigate and diagnose are documented in the incident record?		B65		3	O
During the investigation is caring out:					
<ul style="list-style-type: none"> Understanding the chronological order of events? 		B67		2	O
<ul style="list-style-type: none"> Confirming the full impact of the incident (number and range of users affected)? 		B68		2	O
<ul style="list-style-type: none"> Identifying any events that could have triggered the incident? 		B69		2	O
<ul style="list-style-type: none"> Knowledge searches looking for previous occurrences by searching: 					
-Incident/Problem Record?		B70	C17	3	O
-Know Error Database?		B71	C17	3	O
-Knowledge Databases?		B72	C17	3	O
-Manufactures/suppliers			C17	3	O
Error Logs?		B73			
How many categorization levels are user: <ul style="list-style-type: none"> One? Two? Three? Four? Five or more? 		B43		2	O
Is there a criterion that defines the priority of the incidents and the actions that must be taken according to the priority in question?		B44		3	M
Which of these aspects incident prioritization is based on:					
<ul style="list-style-type: none"> Risk to life? 	A9	B45		2	O
<ul style="list-style-type: none"> The number of services affected? 	A9	B46		2	O
<ul style="list-style-type: none"> The level of financial losses? 	A9	B47		2	O
<ul style="list-style-type: none"> Effect on business reputation? 	A9	B48		2	O
<ul style="list-style-type: none"> Regulatory or legislative breaches? 	A9	B49		2	O
Clear guidance is provided for all support staff to enable them to determine the correct urgency and impact levels?		B50		3	O

At no time, the normal priority levels are overridden?		B51		2	O
Is define a priority level for VIPs?		B52		2	O
Incident's priority can change if:					
<ul style="list-style-type: none"> • Circumstances change? 		B53		2	O
<ul style="list-style-type: none"> • Is not resolved within SLA target times? 		B54		2	O
Attempt to resolve the maximum number of incidents in the first line of support?		B60		2	O
Is there a second line support?		B61		2	O
Is there a third line support?		B62		2	O
If multiple incidents have the same type of priority, is define which incident should be pick up and actively worked on?		B64		2	O
Are incidents prioritized based on SLA service definition of business impact and urgency?			C15	2	M
The incident is addressed using the workaround?	A25			2	
Are managed the actions until the impact of the incident is at an acceptable level?	A26			2	M
Are recorded the actions and results for apply workarounds to selected incidents?	A27		C21	3	M
Are addressed the underlying causes using the action proposal that resulted from the analysis of the incidents underlying causes?	A28			2	O
Are manager the actions until the underlying causes is addressed?	A29			2	O
Are recorded the actions and results for address underlying causes of selected incidents?	A30			3	M
Are identified underlying causes of incidents?	A37			2	O
Are recorded information about the underlying causes of an incident or group of incidents?	A38			3	M
Are conduct causal analysis with the people who are responsible for performing related tasks?	A39			3	M
Is determined which group is best suited to address the underlying cause?	A40			2	O
Is determined the actions to be taken to address the underlying cause?	A41			2	O
Is documented the actions to be taken in an action proposal?	A42			3	O

Is verified and validated the action proposal to ensure that it effectively addresses the incident?	A43			2	M
Is communicated the action proposal to relevant stakeholders?	A44			2	M
Is determine which group is best suited to establish and maintain a workaround?	A45			2	M
The workaround is:					
• Planed?	A46			3	O
• Documented?	A47			3	O
Is verify and validate the workaround to ensure that it effectively addresses the incident?	A48			3	O
Is communicated the workaround to relevant stakeholders?	A49			2	O
Are selected and applied the most appropriate incident resolutions?			C20	2	O
If required are performed recovery actions?			C22	2	O
If the resolution can be used as future knowledge sources, are incident resolution documented and assess?			C23	3	M
When a potential resolution has been identified the actions undertaken involve:					
• Asking the user to undertake directed activities?		B74		2	O
• The Service Desk implementing the resolution remotely or centrally?		B75		2	O
• Specialist support groups being asked to implement a resolution?		B76		2	O
• A third-party supplier or maintainer being asked to resolve the fault?		B77		2	O
When a resolution has been found, is done a testing to ensure that recovery action is complete?		B78		2	O
If is necessary two or more groups take recovery actions in the same incident, Incident Management coordinate the activities and liaise with all parties involved?		B79		2	O
When incident is resolved, the resolving group pass the incident back to Service Desk for closure action?		B80		2	O
Until they meet the terms of the service agreement and satisfy the incident submitter as appropriate, incidents are:					
• Documented actions?	A31			3	O
• Monitored and tracked?	A32			3	O
Is reviewed the resolution of the incident?	A33			2	O

Is confirmed the results with relevant stakeholders?	A34	B81	C24	2	O
Are closed incidents that meet the criteria for closure?	A35	B86	C25	2	O
The communication with customers and end users are recorded?	A36			3	O
When the Service Desk check that incident is fully resolved, it verify:					
<ul style="list-style-type: none"> That user agrees the incident can be closed? 	A11	B82		2	O
<ul style="list-style-type: none"> That closure categorization is correct or if it changes from the initial incident categorization? 	A11	B83		2	O
<ul style="list-style-type: none"> A user satisfaction call-back or e-mail survey for the agreed percentage of incidents is done? 	A11	B84		2	O
<ul style="list-style-type: none"> If is a recurring problem and decide to take any preventive action? 	A11	B85		2	O
Automatic closure period its applied to:					
<ul style="list-style-type: none"> All incidents? 		B87		2	O
<ul style="list-style-type: none"> Specific Incidents? 		B88		2	O
<ul style="list-style-type: none"> None? 		B89		2	O
An incident can be re-open after closure?		B90		2	O
If a problem recurs from a close incident, how many work days, can be possible re-open:				2	O
<ul style="list-style-type: none"> One? Two? Three? More? 		B91			
If a problem recurs from a closure incident and it can't be re-open, a new incident is open and linked to the previous incident?		B92		2	O
Are escalated incident:					
<ul style="list-style-type: none"> Monitored? 			C26	2	O
<ul style="list-style-type: none"> Request handling procedures? 			C27	2	O
Stakeholders needs for data or reports are identify?			C29	3	M
Reporting frequency and medium to stakeholders are identify?			C30	3	M
Incidents are analyses by category and type?		B94	C31	3	M
Are identified and involved the relevant stakeholders of the process as planned?	A77		C28	2	M
The incident management tools contain information about:					
<ul style="list-style-type: none"> Incident and problem history? 		B93		3	O
<ul style="list-style-type: none"> Action taken to resolve incidents? 		B95		3	O
<ul style="list-style-type: none"> Diagnostic scripts? 		B96		3	O

Is ensured that the incident management system allows the escalation and transfer of incidents among groups?	A12			3	O
Is ensured, in incident management system, that incident information that is useful to the resolution and prevention of incidents is:					
• Storage?	A13			3	O
• Update?	A14			3	O
• Retrieval?	A15			3	O
• Reporting?	A16			3	O

Is maintained the integrity of the incident management system and its contents?	A17			3	M
The information of incidents is used to continual improvement planning?	A101		C35	5	M
Is produced and distributed timely reports?			C36	4	M
Is provided controlled access to online data?			C37	4	M
Is the performance of Incident Management measured according to what is described in the execution plan?		B119		4	M
Are monitored and controlled the process against the plan for performing the process and take appropriate corrective action?	A82			2	M
The measures and work products used in monitoring and controlling are:					
• Total number of incidents?	A84	B120		4	M
• Breakdown of incidents at each stage?		B121		4	M
• Number and percentage of major incidents?		B122		4	M
• Percentage of incidents handled within agreed response time?		B123		4	M
• Size of the current incident backlog?		B124		4	M
• Average cost per incident?		B125		4	M
• Number of incidents re-open and as a percentage of the total?		B126		4	M
• Number and percentage of incidents incorrectly assigned?		B127		4	M
• Number and percentage of incidents incorrectly categorized?		B128		4	M
• Percentage of incidents close by the Service Desk?		B129		4	M
• Number and percentage of the incidents processed per Service Desk agent?		B130		4	M

<ul style="list-style-type: none"> Number and percentage of incidents resolved remotely, without the need for a visit? 		B131		4	M
<ul style="list-style-type: none"> Number of incidents handled by each Incident Model? 		B132		4	M
<ul style="list-style-type: none"> Trends? 	A102		C32	4	M
<ul style="list-style-type: none"> Patterns of recurring issues? 			C33	4	M
<ul style="list-style-type: none"> SLA breaches? 	A85	B123	C34	4	M
<ul style="list-style-type: none"> Breakdown of incidents by time of the day, to help pinpoint peaks and ensure matching of resources? 		B133		4	M
<ul style="list-style-type: none"> Capacity, performance, and availability data that signal potential service incidents? 	A83			4	M
<ul style="list-style-type: none"> Number of transfers between support groups before a service incident is resolved? 	A86			4	M
Is done a statistical management of the performance of one or more sub-processes that are critical to the performance of Incident Management?		B134		4	M
Is scheduled for implementing an action proposal to prevent a class of service incidents from reoccurring?	A87			5	M
Support groups are fully aware of timescales?		B1		2	O
Service Management tools are used to automate timescales?		B2		2	O
Service Management tools are used to automate escalates the incident?		B3		2	O
Is used a pre-defined 'standard' Incident Models?		B4		2	O
The incident Model includes:					
<ul style="list-style-type: none"> The steps that should be taken to handle the incident? 		B5		2	O
<ul style="list-style-type: none"> The chronological order of these steps should be taken in? 		B6		2	O
<ul style="list-style-type: none"> Timescales and thresholds for completion of the actions is define? 		B7		2	O
The incident model is input to the incident-handling support tools?		B9		2	O
The support tools automate:					
<ul style="list-style-type: none"> Handling the process? 		B10		2	O
<ul style="list-style-type: none"> Management the process? 		B11		2	O
<ul style="list-style-type: none"> Escalation the process? 		B12		2	O
Is a separated procedure used for major incidents?		B13		2	O

A definition of what constitutes a major incident is agreed and mapped on the incident prioritization system?		B14		3	O
If necessary, separated major incident team, under the direct leadership of Incident Manager, is create to concentrate on this incident alone to ensure that adequate resources and focus?		B15		2	O
Is established and maintain an organizational policy for planning and performing the process?	A51			2	O
Incidents are:					
• Identified?	A52			2	O
• Controlled?	A53			2	O
• Addressed?	A54			2	O
For selected incidents is determined:					
• Workarounds?	A55			2	O
• Underlying causes?	A56			2	O
Is established and maintain the plan for performing the process based on volume and type of service incidents?	A57			2	O
Are provided adequate resources for performing the process, developing the work products, and providing the services of the process?	A58			2	M
The resources provided are:					
• Help desk tools?	A59			2	O
• Remote analysis tools?	A60			2	O
• Automated monitoring tools?	A61			2	O
• Incident management systems?	A62			2	O
Responsibility and authority is assigned for:					
• Performing the process?	A63			2	
• Developing the work products?	A64			2	
• Providing the services of the process?	A65			2	
Are people trained for performing or supporting the process?	A66			2	
The topics included in training people are:					
• Service incident criteria?	A67			2	
• Interacting with those who report service incidents and those who are affected by them?	A68			2	
• Incident management system?	A69			2	
• Analysis techniques?	A70			2	
Are place designated work products of the process under appropriate levels of control?	A71			2	O
The work products under control are:					
• Incident management records?	A72			2	O

• Incident resolution and prevention reports?	A73			2	O
• Action proposals?	A74			2	O
• Workaround description and instructions?	A75			2	O
• Incident database copies?	A76			2	O
Stakeholders are involved in the activities:					
• Establishing an approach to incident resolution and prevention?	A78			2	M
• Identifying service incidents and recording information about them?	A79			2	M
• Analyzing service incidents to determine the best course of action?	A80			2	M
• Reviewing the result of actions for resolving service incidents?	A81			2	M
Are monitored and controlled the process against the plan for performing the process and take appropriate corrective action?	A82			2	O
Is objectively evaluated the adherence of the process against its process description, standards, and procedures, and address noncompliance?	A88			2	M
The activities reviewed are:					
• Establishing an approach to incident resolution and prevention?	A89			2	O
• Identifying service incidents and recording information about them?	A90			2	O
• Communicating the status of service incidents?	A91			2	O
The work products reviewed are:					
• Service incident database?	A92			2	O
• Workarounds?	A93			2	O
• Action proposals?	A94			2	O
• Service incident records?	A95			2	O
Are reviewed with higher level management:					
• Activities?	A96			2	M
• Status?	A97			2	M
• Results?	A98			2	M
Are resolved issues with higher level management?	A99			2	M
Is established and maintained the description of a defined process?	A100			3	M
Witch measures are collected:					
• Number of times the incident management system is accessed and for what purpose?	A103			3	M

• Results of applying workarounds and implementing action proposals?	A104			3	M
Is established and maintained quantitative objectives for the process, which address quality and process performance, based on customer needs and business objectives?	A105			4	M
Is stabilized the performance of one or more sub processes to determine the ability of the process to achieve the established quantitative quality and process-performance objectives?	A106			4	M
Is ensured continuous improvement of the process in fulfilling the relevant business objectives of the organization?	A107			5	M
Are identified and corrected the root causes of defects and other problems in the process?	A108			5	M

Label:

M- Management

O- Operational

Appendix C

Activities - Level 2
Is define criteria for determining what an incident is?
For determining which categories an incident belong to is defined:
<ul style="list-style-type: none"> • Categories?
<ul style="list-style-type: none"> • Criteria?
Is describe how responsibility for processing incidents is assigned and transferred?
Costumer and end users have mechanisms to report incidents?
Is defined methods and secure tools to use for incident management?
All relevant customers and end users who may be affected by a report incident are notified? How? _____
Are defined criteria for determining categories of actions and responses to be taken based on severity and priority levels?
Is identify requirements on the amount of time defined for the resolution of incidents in the service agreement?
Are identified and monitored incidents that are in scope?
Does your organization have channels in place to receive incidents notifications?
How can received incidents notifications:
<ul style="list-style-type: none"> • By phone?
<ul style="list-style-type: none"> • Other?
Detail: _____
Does your organization have mechanisms in place to automatically detect incidents?
Are incidents reported and/or detected logged?
<ul style="list-style-type: none"> • If support staff visit the customers:
<ul style="list-style-type: none"> • They ask for further incidents?
A separate incident record is logged for each additional incident?
To ensure consistent approaches for handling incidents is define criteria for problem registration?
The users are informed about and conducting trend analysis?
Are define incident models for known errors?
Are define incident escalation rules and procedures:
<ul style="list-style-type: none"> • For major incidents?
<ul style="list-style-type: none"> • For security incidents?
<ul style="list-style-type: none"> • For all?
Incident knowledge sources are defined?
Incident knowledge use are defined?
Each incident includes the information:
<ul style="list-style-type: none"> • Unique reference number?
<ul style="list-style-type: none"> • Categorization?
<ul style="list-style-type: none"> • Urgency?
<ul style="list-style-type: none"> • Impact?
<ul style="list-style-type: none"> • Priorization?

<ul style="list-style-type: none"> • Date/Time record?
<ul style="list-style-type: none"> • Name/ID of the person and/or group recording the incident?
<ul style="list-style-type: none"> • Method of notification?
<ul style="list-style-type: none"> • Name/department/phone/location of user?
<ul style="list-style-type: none"> • Call-back method?
<ul style="list-style-type: none"> • Description of symptoms?
<ul style="list-style-type: none"> • Incident Status?
<ul style="list-style-type: none"> • Related Configuration item?
<ul style="list-style-type: none"> • Support group/person to which the incident is allocated?
<ul style="list-style-type: none"> • Related Know Error?
<ul style="list-style-type: none"> • Activities undertaken to resolve the incident?
<ul style="list-style-type: none"> • Resolution Date and time?
<ul style="list-style-type: none"> • Closure category?
<ul style="list-style-type: none"> • Type?
<p>If Service Desk does not work 24/7 and the responsibility for the first-line passes to another group, they have equally rigorous about logging and incident details?</p>
<p>Is determined which group is best suited to take action to address the incident?</p>
<p>Is a determined action that must be taken to address the incident?</p>
<p>In the initial diagnosis are use:</p>
<ul style="list-style-type: none"> • Diagnostic scripts?
<ul style="list-style-type: none"> • Know error information?
<p>If is possible and the incident was reported by telephone, Service Desk Analyst will resolve the incident while the user still on the telephone?</p>
<p>If is not possible to the Service Desk Analyst resolve a reported telephone incident, it:</p>
<ul style="list-style-type: none"> • Inform the user of their intentions?
<ul style="list-style-type: none"> • Give the user the reference number?
<p>Are identify and describe relevant symptoms of incident?</p>
<p>If a related problem or know error does not already exist and if the incident satisfies agreed-on criteria for problem registration, is log a new problem?</p>
<p>During the investigation is caring out:</p>
<ul style="list-style-type: none"> • Understanding the chronological order of events?
<ul style="list-style-type: none"> • Confirming the full impact of the incident (number and range of users affected)?
<ul style="list-style-type: none"> • Identifying any events that could have triggered the incident?
<p>How many categorization levels are user:</p>
<ul style="list-style-type: none"> • One?
<ul style="list-style-type: none"> • Two?
<ul style="list-style-type: none"> • Three?
<ul style="list-style-type: none"> • Four?
<ul style="list-style-type: none"> • Five or more?
<p>Which of these aspects incident prioritization is based on:</p>
<ul style="list-style-type: none"> • Risk to life?
<ul style="list-style-type: none"> • The number of services affected?

<ul style="list-style-type: none"> • The level of financial losses?
<ul style="list-style-type: none"> • Effect on business reputation?
<ul style="list-style-type: none"> • Regulatory or legislative breaches?
At no time, the normal priority levels are overridden?
Is define a priority level for VIPs?
Incident's priority can change if:
<ul style="list-style-type: none"> • Circumstances change?
<ul style="list-style-type: none"> • Is not resolved within SLA target times?
Attempt to resolve the maximum number of incidents in the first line of support?
Is there a second line support?
Is there a third line support?
If multiple incidents have the same type of priority, is define which incident should be pick up and actively worked on?
Are incidents prioritized based on SLA service definition of business impact and urgency?
The incident is addressed using the workaround?
Are managed the actions until the impact of the incident is at an acceptable level?
Are addressed the underlying causes using the action proposal that resulted from the analysis of the incidents underlying causes?
Are manager the actions until the underlying causes is addressed?
Are identified underlying causes of incidents?
Is determined which group is best suited to address the underlying cause?
Is determined the actions to be taken to address the underlying cause?
Is verified and validated the action proposal to ensure that it effectively addresses the incident?
Is communicated the action proposal to relevant stakeholders?
Is determine which group is best suited to establish and maintain a workaround?
Is communicated the workaround to relevant stakeholders?
Are selected and applied the most appropriate incident resolutions?
If required are performed recovery actions?
When a potential resolution has been identified the actions undertaken involve:
<ul style="list-style-type: none"> • Asking the user to undertake directed activities?
<ul style="list-style-type: none"> • The Service Desk implementing the resolution remotely or centrally?
<ul style="list-style-type: none"> • Specialist support groups being asked to implement a resolution?
<ul style="list-style-type: none"> • A third-party supplier or maintainer being asked to resolve the fault?
When a resolution has been found, is done a testing to ensure that recovery action is complete?
If is necessary two or more groups take recovery actions in the same incident, Incident Management coordinate the activities and liaise with all parties involved?
When incident is resolved, the resolving group pass the incident back to Service Desk for closure action?
Is reviewed the resolution of the incident?
Is confirmed the results with relevant stakeholders?
Are closed incidents that meet the criteria for closure?
When the Service Desk check that incident is fully resolved, it verify:
<ul style="list-style-type: none"> • That user agrees the incident can be closed?

<ul style="list-style-type: none"> • That closure categorization is correct or if it changes from the initial incident categorization?
<ul style="list-style-type: none"> • A user satisfaction call-back or e-mail survey for the agreed percentage of incidents is done?
<ul style="list-style-type: none"> • If is a recurring problem and decide to take any preventive action?
Automatic closure period its applied to:
<ul style="list-style-type: none"> • All incidents?
<ul style="list-style-type: none"> • Specific Incidents?
<ul style="list-style-type: none"> • None?
An incident can be re-open after closure?
If a problem recurs from a close incident, how many work days, can be possible re-open:
<ul style="list-style-type: none"> • One?
<ul style="list-style-type: none"> • Two?
<ul style="list-style-type: none"> • Three?
<ul style="list-style-type: none"> • More?
If a problem recurs from a closure incident and it can't be re-open, a new incident is open and linked to the previous incident?
Are escalated incident:
<ul style="list-style-type: none"> • Monitored?
<ul style="list-style-type: none"> • Request handling procedures?
Are identified and involved the relevant stakeholders of the process as planned?
Are monitored and controlled the process against the plan for performing the process and take appropriate corrective action?
Support groups are fully aware of timescales?
Service Management tools are used to automate timescales?
Service Management tools are used to automate escalate the incident?
Is used a pre-defined 'standard' Incident Models?
The incident Model includes:
<ul style="list-style-type: none"> • The steps that should be taken to handle the incident?
<ul style="list-style-type: none"> • The chronological order of these steps should be taken in?
<ul style="list-style-type: none"> • Timescales and thresholds for completion of the actions is define?
The incident model is input to the incident-handling support tools?
The support tools automate:
<ul style="list-style-type: none"> • Handling the process?
<ul style="list-style-type: none"> • Management the process?
<ul style="list-style-type: none"> • Escalation the process?
Is a separated procedure used for major incidents?
If necessary, separated major incident team, under the direct leadership of Incident Manager, is create to concentrate on this incident alone to ensure that adequate resources and focus?
Is establish and maintain an organizational policy for planning and performing the process?
Incidents are:
<ul style="list-style-type: none"> • Identified?
<ul style="list-style-type: none"> • Controlled?
<ul style="list-style-type: none"> • Addressed?

For selected incidents is determined:
<ul style="list-style-type: none"> • Workarounds?
<ul style="list-style-type: none"> • Underlying causes?
Is established and maintain the plan for performing the process based on volume and type of service incidents?
Are provided adequate resources for performing the process, developing the work products, and providing the services of the process?
The resources provided are:
<ul style="list-style-type: none"> • Help desk tools?
<ul style="list-style-type: none"> • Remote analysis tools?
<ul style="list-style-type: none"> • Automated monitoring tools?
<ul style="list-style-type: none"> • Incident management systems?
Responsibility and authority is assigned for:
<ul style="list-style-type: none"> • Performing the process?
<ul style="list-style-type: none"> • Developing the work products?
<ul style="list-style-type: none"> • Providing the services of the process?
Are people trained for performing or supporting the process?
The topics included in training people are:
<ul style="list-style-type: none"> • Service incident criteria?
<ul style="list-style-type: none"> • Interacting with those who report service incidents and those who are affected by them?
<ul style="list-style-type: none"> • Incident management system?
<ul style="list-style-type: none"> • Analysis techniques?
Are place designated work products of the process under appropriate levels of control?
The work products under control are:
<ul style="list-style-type: none"> • Incident management records?
<ul style="list-style-type: none"> • Incident resolution and prevention reports?
<ul style="list-style-type: none"> • Action proposals?
<ul style="list-style-type: none"> • Workaround description and instructions?
<ul style="list-style-type: none"> • Incident database copies?
Stakeholders are involved in the activities:
<ul style="list-style-type: none"> • Establishing an approach to incident resolution and prevention?
<ul style="list-style-type: none"> • Identifying service incidents and recording information about them?
<ul style="list-style-type: none"> • Analyzing service incidents to determine the best course of action?
<ul style="list-style-type: none"> • Reviewing the result of actions for resolving service incidents?
Are monitored and controlled the process against the plan for performing the process and take appropriate corrective action?
Is objectively evaluated the adherence of the process against its process description, standards, and procedures, and address noncompliance?
The activities reviewed are:
<ul style="list-style-type: none"> • Establishing an approach to incident resolution and prevention?
<ul style="list-style-type: none"> • Identifying service incidents and recording information about them?
<ul style="list-style-type: none"> • Communicating the status of service incidents?

The work products reviewed are:
<ul style="list-style-type: none"> • Service incident database?
<ul style="list-style-type: none"> • Workarounds?
<ul style="list-style-type: none"> • Action proposals?
<ul style="list-style-type: none"> • Service incident records?
Are reviewed with higher level management:
<ul style="list-style-type: none"> • Activities?
<ul style="list-style-type: none"> • Status?
<ul style="list-style-type: none"> • Results?
Are resolved issues with higher level management?

Activities - Level 3
Incident Records include the following data:
<ul style="list-style-type: none"> • Unique reference number?
<ul style="list-style-type: none"> • Incident classification?
<ul style="list-style-type: none"> • Data and time of recording?
<ul style="list-style-type: none"> • Name and identity of the person recording the incident record?
<ul style="list-style-type: none"> • Name and identity of the person updating the incident record?
<ul style="list-style-type: none"> • Name/organization/contact details of affected users?
<ul style="list-style-type: none"> • Description of incident symptoms?
<ul style="list-style-type: none"> • Incident category?
<ul style="list-style-type: none"> • Incident Impact?
<ul style="list-style-type: none"> • Incident urgency?
<ul style="list-style-type: none"> • Incident priority?
<ul style="list-style-type: none"> • Closure details including:
<ul style="list-style-type: none"> -Time?
<ul style="list-style-type: none"> -Category?
<ul style="list-style-type: none"> -Action taken?
<ul style="list-style-type: none"> -Person of closing the record?
<ul style="list-style-type: none"> • Relationship with other:
<ul style="list-style-type: none"> -Incidents?
<ul style="list-style-type: none"> -Problems?
<ul style="list-style-type: none"> -Changes?
<ul style="list-style-type: none"> -Know error?
<ul style="list-style-type: none"> • Details of any actions taken to try to:
<ul style="list-style-type: none"> -Diagnose incident?
<ul style="list-style-type: none"> -Resolve incident?
<ul style="list-style-type: none"> -Re-create incident?
A full historical record is maintained?
Is analyzed incident data?
Actions to be taken are planed?

All activities of investigate and diagnose are documented in the incident record?
During the investigation is caring out:
<ul style="list-style-type: none"> • Knowledge searches looking for previous occurrences by searching:
<ul style="list-style-type: none"> • Incident/Problem Record?
<ul style="list-style-type: none"> • Know Error Database?
<ul style="list-style-type: none"> • Knowledge Databases?
<ul style="list-style-type: none"> • Manufactures/suppliers Error Logs?
Is there a criterion that defines the priority of the incidents and the actions that must be taken according to the priority in question?
Clear guidance is provided for all support staff to enable them to determine the correct urgency and impact levels?
Incident's priority can change if:
Are recorded the actions and results for apply workarounds to selected incidents?
Are recorded the actions and results for address underlying causes of selected incidents?
Are recorded information about the underlying causes of an incident or group of incidents?
Are conduct causal analysis with the people who are responsible for performing related tasks?
Is documented the actions to be taken in an action proposal?
The workaround is:
<ul style="list-style-type: none"> • Planed?
<ul style="list-style-type: none"> • Documented?
Is verify and validate the workaround to ensure that it effectively addresses the incident?
If the resolution can be used as future knowledge sources, are incident resolution documented and assess?
Until they meet the terms of the service agreement and satisfy the incident submitter as appropriate, incidents are:
<ul style="list-style-type: none"> • Documented actions?
<ul style="list-style-type: none"> • Monitored and tracked?
The communication with customers and end users are recorded?
Stakeholders needs for data or reports are identify?
Reporting frequency and medium to stakeholders are identify?
Incidents are analyses by category and type?
The incident management tools contain information about:
<ul style="list-style-type: none"> • Incident and problem history?
<ul style="list-style-type: none"> • Action taken to resolve incidents?
<ul style="list-style-type: none"> • Diagnostic scripts?
Is ensured that the incident management system allows the escalation and transfer of incidents among groups?
Is ensured, in incident management system, that incident information that is useful to the resolution and prevention of incidents is:
<ul style="list-style-type: none"> • Storage?
<ul style="list-style-type: none"> • Update?

<ul style="list-style-type: none"> • Retrieval?
<ul style="list-style-type: none"> • Reporting?
Is maintained the integrity of the incident management system and its contents?
A definition of what constitutes a major incident is agreed and mapped on the incident prioritization system?
Is established and maintained the description of a defined process?
Which measures are collected:
<ul style="list-style-type: none"> • Number of times the incident management system is accessed and for what purpose?
<ul style="list-style-type: none"> • Results of applying workarounds and implementing action proposals?

Activities - Level 4
Is produced and distributed timely reports?
Is provided controlled access to online data?
Is the performance of Incident Management measured according to what is described in the execution plan?
The measures and work products used in monitoring and controlling are:
<ul style="list-style-type: none"> • Total number of incidents?
<ul style="list-style-type: none"> • Breakdown of incidents at each stage?
<ul style="list-style-type: none"> • Number and percentage of major incidents?
<ul style="list-style-type: none"> • Percentage of incidents handled within agreed response time?
<ul style="list-style-type: none"> • Size of the current incident backlog?
<ul style="list-style-type: none"> • Average cost per incident?
<ul style="list-style-type: none"> • Number of incidents re-open and as a percentage of the total?
<ul style="list-style-type: none"> • Number and percentage of incidents incorrectly assigned?
<ul style="list-style-type: none"> • Number and percentage of incidents incorrectly categorized?
<ul style="list-style-type: none"> • Percentage of incidents close by the Service Desk?
<ul style="list-style-type: none"> • Number and percentage of the incidents processed per Service Desk agent?
<ul style="list-style-type: none"> • Number and percentage of incidents resolved remotely, without the need for a visit?
<ul style="list-style-type: none"> • Number of incidents handled by each Incident Model?
<ul style="list-style-type: none"> • Trends?
<ul style="list-style-type: none"> • Patterns of recurring issues?
<ul style="list-style-type: none"> • SLA breaches?
<ul style="list-style-type: none"> • Breakdown of incidents by time of the day, to help pinpoint peaks and ensure matching of resources?
<ul style="list-style-type: none"> • Capacity, performance, and availability data that signal potential service incidents?
<ul style="list-style-type: none"> • Number of transfers between support groups before a service incident is resolved?
Is done a statistical management of the performance of one or more sub-processes that are critical to the performance of Incident Management?

Is established and maintained quantitative objectives for the process, which address quality and process performance, based on customer needs and business objectives?
--

Is stabilized the performance of one or more sub processes to determine the ability of the process to achieve the established quantitative quality and process-performance objectives?
--

<i>Activities - Level 5</i>

The information of incidents is used to continual improvement planning?

Is scheduled for implementing an action proposal to prevent a class of service incidents from reoccurring?
--

Is ensured continuous improvement of the process in fulfilling the relevant business objectives of the organization?
--

Are identified and corrected the root causes of defects and other problems in the process?
--

Appendix D

Questionnaire**Incident Management Process**

This questionnaire about Incident Management is carried out within the scope of a Master's thesis of ISCTE.

The results will be sent to the interviewee by email few days after the interview.

It is guaranteed that both company and interviewee name and identification will be treated confidentially and shall never be revealed.

Thank you in advance for the availability and most sincere response.

<u>Interviewee</u>	
Name	
Post	
Years of experience	

<u>Company</u>	
Name	
Industry	
Number of employees	
Number of IT employees	
Multinational	
Regarding the IT Strategy, what kind(s) of IT strategy is(are) used? (Note: More than 1 (one) option can be chosen)	
• IT for comprehensiveness	
• IT for flexibility	
• IT for efficiency	
Regarding the IT structure what is the structure used in the organization? (Note: Only 1 (one) answer is available)	
• Centralized	
• Decentralized	
• Federal	
What maturity level do you think your organization is regarding incident management process?	
• 1?	
• 2?	
• 3?	
• 4?	
• 5?	
Did you perform an official implementation of incident management process adopting some of the following IT frameworks?	
• CMMI?	
• COBIT?	
• ITIL?	
• None?	

Activities	Yes	No	In Implementation
Is defined a criterion for determining what an incident is?			
Are defined methods and secure tools to execute incident management process? Which ones:			
For determining which incidents belong to is defined categories?			
How many categorization levels are use:			
• One?			
• Two?			
• Three?			
• Four?			
• Other?			
Detail:			
Is described how responsibility for processing incidents is assigned and transferred?			
Customer and end users have mechanisms to report incidents? Which ones:			
All relevant customers and end users who may be affected by a reported incident are notified? How?			
Is a criterion defined for determining categories of actions and responses to be taken based on severity and priority levels?			
Are defined the minimum and maximum amounts of time needed to resolve an incident?			
Does your organization have mechanisms in place to automatically detect incidents?			
If support staff visit the customers during the resolution of an incident:			
• They ask for further incidents?			
• A separate incident record is logged for each additional incident?			
To ensure consistent approaches for handling incidents is defined criteria for problem registration?			
Are defined incident models for known errors?			
Do the incident management tools allow the escalation and transfer of incidents among groups?			
Are defined incident escalation rules and procedures:			
• For major incidents?			
• For security incidents?			
• For all?			
• Other:			
Detail:			
Incident knowledge sources are defined?			
Is there a definition of how can incident knowledge sources be used?			

If for any reason the first line passes the responsibility to another group, do they have access to all information about logging and incident details?			
Is determined which group is best suited to take action and address the incident?			
Are determined actions that must be taken to address the incident?			
Is an initial diagnosis made?			
In the initial diagnosis are use:			
<ul style="list-style-type: none"> • Diagnostic scripts? 			
<ul style="list-style-type: none"> • Know error information? 			
<ul style="list-style-type: none"> • Other? 			
Detail:			
When reported by telephone, will the staff try to solve the incident while the user still on the telephone?			
When the staff cannot solve a reported telephone incident during the call, do they:			
<ul style="list-style-type: none"> • Inform the user of their intentions? 			
<ul style="list-style-type: none"> • Give the user the reference number? 			
<ul style="list-style-type: none"> • Other? 			
Detail:			
If a related problem or know error does not already exist and if the incident satisfies agreed-on criteria for problem registration, is a new problem logged?			
Which of the following activities are performed during the investigation?			
<ul style="list-style-type: none"> • Understand the chronological order of events? 			
<ul style="list-style-type: none"> • Confirm the full impact of the incident: 			
-Number of users affected?			
-Range of users affected?			
-Others: _____			
<ul style="list-style-type: none"> • Identify any events that could have triggered the incident? 			
<ul style="list-style-type: none"> • Other? 			
Detail:			
Which of the following aspects contribute to define the incident priority:			
<ul style="list-style-type: none"> • Risk to life? 			
<ul style="list-style-type: none"> • The number of services affected? 			
<ul style="list-style-type: none"> • The level of financial losses? 			
<ul style="list-style-type: none"> • Effect on business reputation? 			
<ul style="list-style-type: none"> • Regulatory or legislative breaches? 			
<ul style="list-style-type: none"> • Other? 			
Detail:			
Is it possible to override normal priority levels?			
Is defined a priority level for VIPs?			

Incident's priority can change if:			
<ul style="list-style-type: none"> • Circumstances change? 			
<ul style="list-style-type: none"> • Is not resolved within SLA target times? 			
<ul style="list-style-type: none"> • Other? 			
Detail:			
Does the first line of support as the goal to resolve the maximum number of incidents?			
Is there a second line support?			
Is there a third line support?			
If multiple incidents have the same type of priority, is defined which incident should be picked up and actively worked on?			
Are incidents prioritized based on SLA definition?			
Is the incident addressed using a workaround?			
Are the actions managed until the impact of the incident to be at an acceptable level?			
Are identified underlying causes of incidents?			
Are addressed the underlying causes of incident using the action proposal?			
Are incidents escalated until the underlying causes be discovered?			
Is the action proposal communicated to relevant stakeholders?			
Is the suitable group to establish and maintain a workaround determined?			
Is the workaround communicated to relevant stakeholders?			
If required are performed recovery actions?			
When a possible resolution is identified, the actions undertaken involve:			
<ul style="list-style-type: none"> • Asking the user to undertake directed activities 			
<ul style="list-style-type: none"> • The Service Desk implementing the resolution remotely or centrally 			
<ul style="list-style-type: none"> • Specialist support groups being asked to implement a resolution 			
<ul style="list-style-type: none"> • A third-party supplier or maintainer being asked to resolve the fault 			
<ul style="list-style-type: none"> • Other? 			
Detail:			
When a resolution is found, is done a testing to ensure that recovery action is complete?			
When two or more groups are required to take recovery actions in the same incident, Incident Manager coordinate the activities and liaise with all parties involved?			
When incident is resolved, the resolving group pass the incident back to Service Desk for closure action?			
Is the resolution of the incident reviewed?			
Are the results confirmed with relevant stakeholders?			
Are the incidents that meet the criteria for closure closed?			

When the Service Desk check that incident is fully resolved, it verify:			
<ul style="list-style-type: none"> if the user agrees that the incident can be closed? 			
<ul style="list-style-type: none"> if closure categorization is correct or if it's different from the initial incident categorization? 			
<ul style="list-style-type: none"> If a user satisfaction call-back or e-mail survey for the agreed percentage of incidents is done/sent? 			
<ul style="list-style-type: none"> If is a recurring problem and a preventive action should be made? 			
<ul style="list-style-type: none"> Other? 			
Detail:			
Automatic closure period its applied to:			
<ul style="list-style-type: none"> All incidents? 			
<ul style="list-style-type: none"> Specific Incidents? 			
Detail:			
<ul style="list-style-type: none"> None? 			
An incident can be re-open after closure?			
When:			
If a problem recurs from a closure incident and it can't be re-open, a new incident is opened and linked to the previous incident?			
Escalated incidents:			
<ul style="list-style-type: none"> Are monitored? 			
<ul style="list-style-type: none"> Require specific procedures to be handled? 			
Are identified and involved the relevant stakeholders of the process as planned?			
Support groups are fully aware of timescales?			
Exist a pre-defined 'standard' Incident Models?			
The Incident Model includes:			
<ul style="list-style-type: none"> The steps that should be taken to handle the incident? 			
<ul style="list-style-type: none"> The chronological order that such steps should be taken in? 			
<ul style="list-style-type: none"> The definition of timescales and thresholds for completion of the actions 			
<ul style="list-style-type: none"> Other? 			
Detail:			
The incident model is an input to the incident-handling support tools?			
Do the support tools automate:			
<ul style="list-style-type: none"> The process handling? 			
<ul style="list-style-type: none"> The process management? 			
<ul style="list-style-type: none"> The incident escalation? 			
<ul style="list-style-type: none"> Timescales? 			
Is a different procedure used for major incidents?			

If necessary, a separated major incident team, under the direct leadership of Incident Manager, is created to concentrate on this incident alone and ensure adequate resources and focus?			
Is established and maintained an organizational policy for planning and performing the incident management process?			
Is established and maintained a plan for performing the incident management process based on volume and type of service incidents?			
Are provided adequate resources for:			
• Performing the process			
• Developing work products			
The resources provided are:			
• Help desk tools?			
• Remote analysis tools?			
• Automated monitoring tools?			
• Incident management systems?			
Responsibility and authority is assigned for:			
• Performing the process?			
• Developing the work products?			
Are people trained for performing or supporting the process?			
The topics included in training are:			
• Service incident criteria?			
• Interacting with those who report service incidents and those who are affected by them?			
• Incident management system?			
• Analysis techniques?			
• Other?			
Detail:			
Stakeholders are involved in the following activities:			
• Establishing an approach to incident resolution and prevention?			
• Identifying service incidents and recording information about them?			
• Analyzing service incidents to determine the best course of action?			
• Reviewing the result of actions for resolving service incidents?			
• Other?			
Detail:			
Are monitored and controlled the IM process against the execution plan?			
Is objectively evaluated the adherence of the IM process against:			
• Process description?			
• Standards?			
• Procedures?			

The activities are reviewed?			
The activities reviewed are:			
<ul style="list-style-type: none"> Establishing an approach to incident resolution and prevention? 			
<ul style="list-style-type: none"> Identifying service incidents and recording information about them? 			
<ul style="list-style-type: none"> Communicating the status of service incidents? 			
<ul style="list-style-type: none"> Other? 			
Detail:			
Are reviewed with higher level management:			
<ul style="list-style-type: none"> Prevention activities? 			
<ul style="list-style-type: none"> Status of significant service incidents? 			
<ul style="list-style-type: none"> Results of workarounds? 			
<ul style="list-style-type: none"> Other? 			
Detail:			
If necessary are resolved issues reviewed with higher level management?			
Incident Records include the following data:			
<ul style="list-style-type: none"> Unique reference number? 			
<ul style="list-style-type: none"> Incident classification? 			
<ul style="list-style-type: none"> Data and time of recording? 			
<ul style="list-style-type: none"> Name and identity of the person recording the incident record? 			
<ul style="list-style-type: none"> Name and identity of the person updating the incident record? 			
<ul style="list-style-type: none"> Name/organization/contact details of affected users? 			
<ul style="list-style-type: none"> Method of notifications? 			
<ul style="list-style-type: none"> Call-back method? 			
<ul style="list-style-type: none"> Description of incident symptoms? 			
<ul style="list-style-type: none"> Support group/person to which incident is allocated? 			
<ul style="list-style-type: none"> Incident Status? 			
<ul style="list-style-type: none"> Incident category? 			
<ul style="list-style-type: none"> Incident Impact? 			
<ul style="list-style-type: none"> Incident urgency? 			
<ul style="list-style-type: none"> Incident priority? 			
<ul style="list-style-type: none"> Closure details including: 			
<ul style="list-style-type: none"> -Time? 			
<ul style="list-style-type: none"> -Category? 			
<ul style="list-style-type: none"> -Action taken? 			
<ul style="list-style-type: none"> -Person of closing the record? 			

<ul style="list-style-type: none"> Relationship with other: 			
-Incidents?			
-Problems?			
-Changes?			
-Know error?			
<ul style="list-style-type: none"> Details of any actions taken to try to: 			
-Diagnose incident?			
-Resolve incident?			
<ul style="list-style-type: none"> All activities of investigation and diagnosis? 			
<ul style="list-style-type: none"> Other? 			
Detail:			
A full historical record is maintained?			
During the investigation is carried out:			
<ul style="list-style-type: none"> Knowledge searches looking for previous occurrences by searching: 			
-Incident/Problem Record?			
-Know Error Database?			
-Knowledge Databases?			
-Manufactures/suppliers Error Logs?			
Are recorded the actions and results to apply workarounds to selected incidents in the future?			
Are recorded the actions and results to address underlying causes of selected incidents in the future?			
Are conducted causal analysis with the people who are responsible for performing related tasks?			
Are the actions to be taken in an action proposal documented?			
The workaround is:			
<ul style="list-style-type: none"> Planned? 			
<ul style="list-style-type: none"> Documented? 			
If the resolution can be used as future knowledge sources, are incident resolution:			
<ul style="list-style-type: none"> Documented? 			
<ul style="list-style-type: none"> Assessed? 			
The communication with customers and end users are recorded?			
Stakeholders needs for data or reports are identify?			
Reporting frequency and medium to stakeholders are identifying?			
Incidents are analyzed by category?			
The incident management tool contains information about:			
<ul style="list-style-type: none"> Incident history? 			
<ul style="list-style-type: none"> Problem history? 			
<ul style="list-style-type: none"> Action taken to resolve incidents? 			
<ul style="list-style-type: none"> Diagnostic scripts? 			

<ul style="list-style-type: none"> • Other? 			
Detail:			
Is ensured, in incident management tools, that incident information useful to incident resolution and prevention is:			
<ul style="list-style-type: none"> • Storage? 			
<ul style="list-style-type: none"> • Update? 			
<ul style="list-style-type: none"> • Retrieval? 			
<ul style="list-style-type: none"> • Reporting? 			
Is the integrity of the incident management tools and its contents maintained?			
Is established and maintained the description of IM process?			
Are timely reports:			
<ul style="list-style-type: none"> • Produced? 			
<ul style="list-style-type: none"> • Distributed? 			
Is provided controlled access to online data?			
Is the performance of IM measured based on what is described in the execution plan?			
Which of the following measures and work products are used in monitoring and controlling:			
<ul style="list-style-type: none"> • Total number of incidents 			
<ul style="list-style-type: none"> • Breakdown of incidents at each stage 			
<ul style="list-style-type: none"> • Number and percentage of major incidents 			
<ul style="list-style-type: none"> • Percentage of incidents handled within agreed response time 			
<ul style="list-style-type: none"> • Size of the current incident backlog 			
<ul style="list-style-type: none"> • Average cost per incident 			
<ul style="list-style-type: none"> • Number of incidents re-open and as a percentage of the total 			
<ul style="list-style-type: none"> • Number and percentage of incidents incorrectly assigned 			
<ul style="list-style-type: none"> • Number and percentage of incidents incorrectly categorized 			
<ul style="list-style-type: none"> • Percentage of incidents close by the Service Desk 			
<ul style="list-style-type: none"> • Number and percentage of the incidents processed per Service Desk agent 			
<ul style="list-style-type: none"> • Number and percentage of incidents resolved remotely, without the need for a visit 			
<ul style="list-style-type: none"> • Number of incidents handled by each Incident Model 			
<ul style="list-style-type: none"> • Trends 			
<ul style="list-style-type: none"> • Patterns of recurring issues 			
<ul style="list-style-type: none"> • SLA breaches 			
<ul style="list-style-type: none"> • Breakdown of incidents by time of the day, to help pinpoint peaks and ensure matching of resources 			
<ul style="list-style-type: none"> • Capacity, performance, and availability data that signal potential service incidents 			

<ul style="list-style-type: none"> Number of transfers between support groups before a service incident is resolved 			
<ul style="list-style-type: none"> Number of times the incident management system is accessed and for what purpose 			
<ul style="list-style-type: none"> Results of applying workarounds and implementing action proposals 			
<ul style="list-style-type: none"> Other? 			
Detail:			
Is done a statistical management of the performance of one or more sub-processes that are critical to the performance of IM?			
Is established and maintained quantitative objectives for the process, which address quality and process performance, based on customer needs and business objectives?			
Is stabilized the performance of one or more sub processes to determine the ability of the process to achieve the established quantitative quality and process-performance objectives?			
The information of incidents is used to continual improvement planning?			
Is scheduled for implementing an action proposal to prevent a class of service incidents from reoccurring?			
Is ensured continuous improvement of the process in fulfilling the relevant business objectives of the organization?			
Are identified and corrected the root causes of defects and other problems in the process?			

Do you think that this questionnaire is complete?	
If not, what do you think its missing?	
Do you think that this questionnaire is useful?	

Appendix E



IT Incident Management

RELATÓRIO INDIVIDUAL



Professor Rúben Pereira - Ruben.Filipe.Pereira@iscte-iul.pt
João Aguiar - jffar@iscte-iul.pt

Análise Global

Depois de analisar as respostas dadas, às 207 atividades sobre o processo de gestão de incidências foi possível obter a um nível mais objetivo e qualitativo a informação sobre a maturidade do processo.

Sendo que o nível de maturidade número 2 é o que concentra o maior numero de atividades, conseqüentemente também é o nível onde se verifica o maior numero de realizadas pela organização. No nível 3 são realizadas 32 das atividades enquanto que 13 não se verificam, existem 5 que não são aplicáveis devido a diversos fatores. No nível 4 é onde a maturidade é mais baixa com 20 atividades não efetuadas e apenas 11 a serem realizadas. No nível 5 onde existe 4 atividades na totalidade, todas são realizadas.

Pelos gráficos 1, 2, 3 e 4 é possível visualizar com maior facilidade a distribuição das atividades efetuadas e não efetuadas relativamente aos níveis de maturidade 2, 3, 4 e 5 respectivamente.

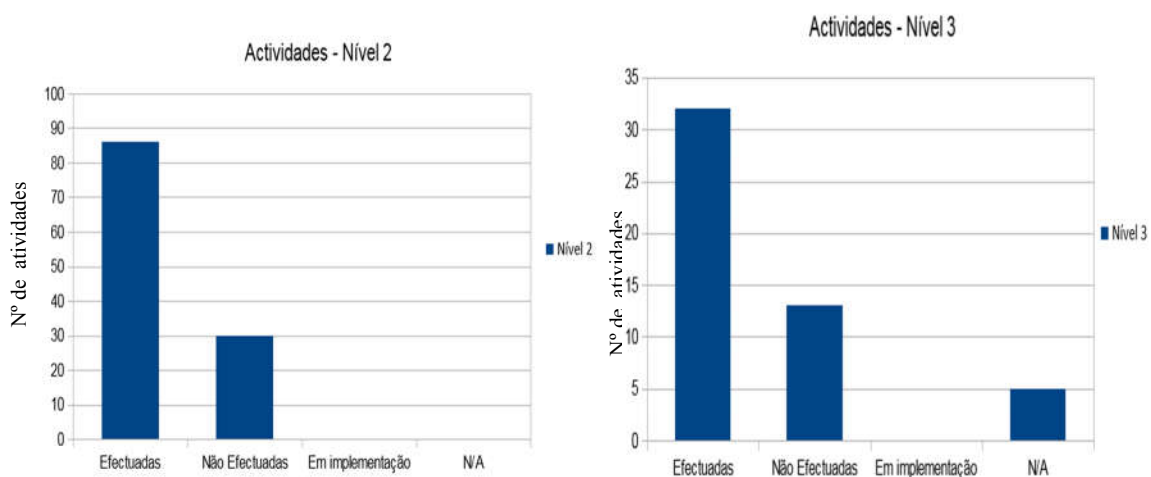


Gráfico 1 - Distribuição das Atividades Nível 2

Gráfico 2 - Distribuição das Atividades Nível 3

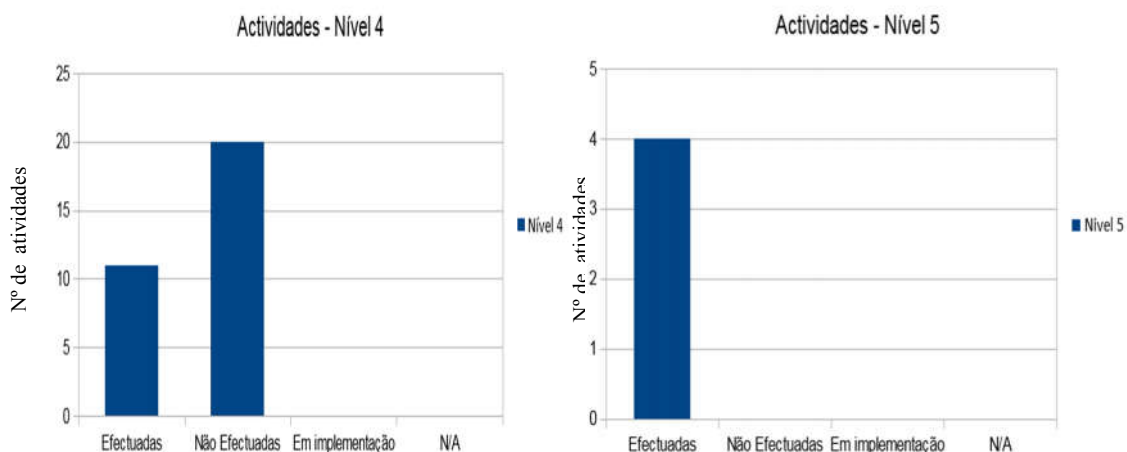


Gráfico 3 - Distribuição das Atividades Nível 4

Gráfico 4 - Distribuição das Atividades Nível 5

Em termos globais a distribuição de todos os níveis de maturidade pelas respostas possíveis está ilustrado no gráfico 5.

Distribuição de Actividades

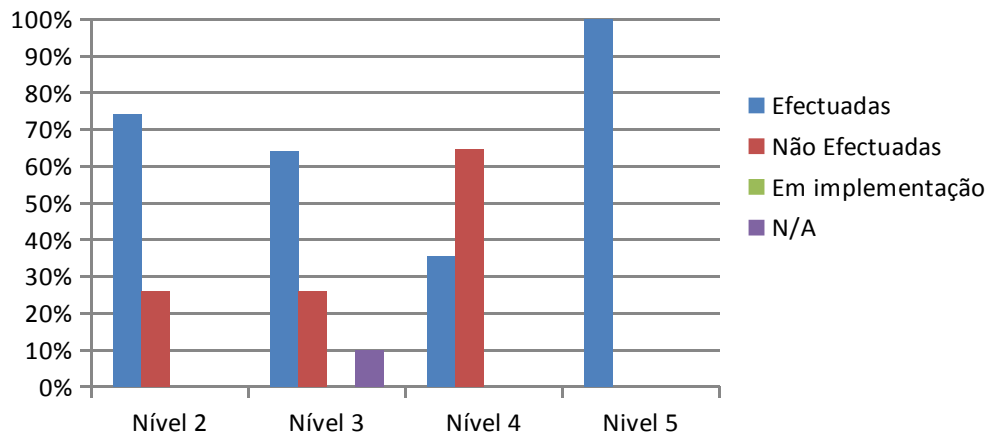


Gráfico 5 - Distribuição dos 5 Níveis de Maturidade

Como podemos verificar a maturidade do nível 4 é mais baixa quando comparada com os restantes níveis de maturidade. Já os níveis 2 e 5 atingem 75% das principais actividades. No nível 3 de maturidade fica-se pelos 64%. Estando apenas a 11% de atingir o nível seguinte.

Análise de Framework's

Outro tipo de análise com relevo ao nível de investigação é a distribuição das atividades consoante as diferentes *Framework's* de IT. No gráfico 6 podemos verificar essa mesma distribuição e salienta-se com especial relevo que as sobreposições de atividades das 3 *Framework's* perfaz 22% do total das atividades.

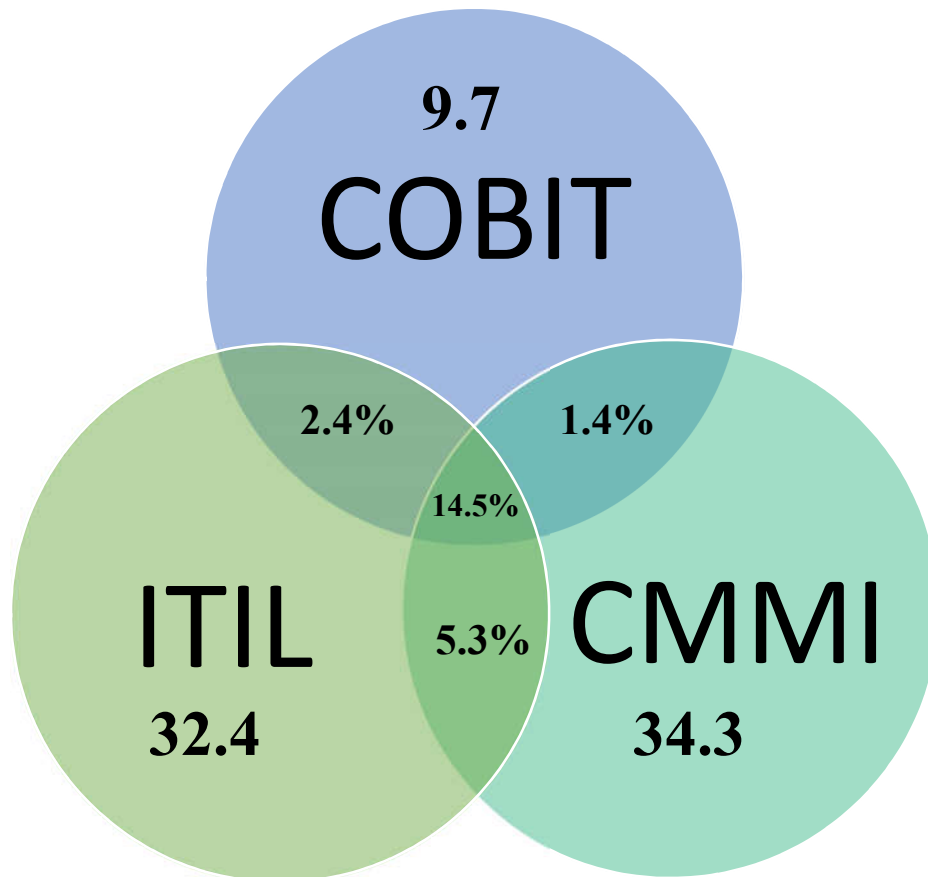


Gráfico 6 - Distribuição das atividades por Framework

Relativamente às atividades que a organização efetua no processo de Gestão de Incidências a distribuição pode ser observada no Gráfico 7.

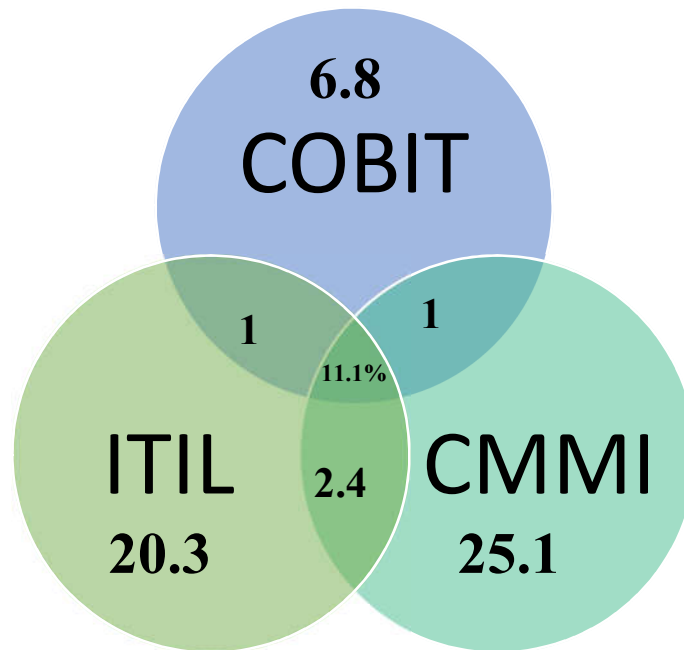


Gráfico 7 - Distribuição de atividades efetuadas por Framework

A soma das percentagens de atividades realizadas, do gráfico 7, perfaz aproximadamente 68% do total das 207 atividades.

A distribuição das atividades efetuadas por *Framework* é semelhante à distribuição global das atividades com um pequeno foco nas atividades do CMMI em que são efetuadas 25,1% das 34,3% das atividades. No ITIL são realizadas 20,3% das 32,4% das atividades. O COBIT tem uma substancial queda percentual das atividades efetuadas, em que das 9,7% de total de atividades apenas 6,8% são realizadas, o que podemos concluir que o processo se acentua mais na operacionalidade e não tanto na gestão. Relativamente às atividades que sobrepõem as 3 *frameworks* do total de 14,5% de atividades, 15,5% são efetuadas.

Considerações Finais e Propostas de Melhoria

O racional definido para a obtenção de um certo nível de maturidade é de 75% de atividades realizadas do nível correspondente.

Depois da análise estatística do questionário obtido, considera-se que a organização tem um nível de maturidade 2 no processo de gestão de incidências. Neste nível são efetuadas 75% das atividades.

Para atingir o nível de maturidade 3 é aconselhável implementar, pelo menos, 6 das atividades em falta na Tabela 1.

O registo de incidências deverá ter os seguintes dados:
· Nome/Organização/Contacto dos utilizadores afetados.
· Categorização nos detalhes do fecho.
Durante a investigação deve ser tido em conta a procura de ocorrências anteriores, em <i>Error Logs</i> de fabricantes/fornecedores.
Efetuar uma análise casual com os responsáveis de executar tarefas relacionadas.
Documentar soluções alternativas.
A ferramenta de gestão de incidências deverá conter informações sobre:
· Histórico de incidências.
· Histórico de problemas.
· Ações a efetuar para resolver incidências.
· Script's de diagnostico.
É necessário garantir, na ferramenta de gestão de incidências, que a informação útil para a resolução e prevenção é:
· Armazenada.
· Atualizada.
· Recuperável.
· Reportada.

Tabela 1 - Lista de atividades em falta do nível 3

No nível 4 de maturidade é onde o processo tem o nível mais baixo de maturidade com o total de atividades não efetuadas ser superior ao nível de atividades efetuadas. É recomendado especial atenção a este nível e que se efetuem:

- Estabelecimento de objetivos qualitativos/quantitativos de um ou mais subprocessos de forma a determinar a capacidade do processo.
- Gestão estatística da performance de um ou mais subprocessos do processo de Gestão de Incidências.
- Estabelecimento de objetivos quantitativos baseados nas necessidades do cliente e objetivo de negócio.

Outros fatores para obter o nível 4 de maturidade são sugeridas a análise de métricas, assim como a produção e distribuição de relatórios. Com estas recomendações é possível fazer uma análise preditiva otimizando o processo e poupando tempo e recursos.

Obrigado pela disponibilidade e ajuda na investigação.

Atentamente,
João Aguiar

Appendix F



IT Incident Management
RELATÓRIO GERAL



Professor Rúben Pereira - Ruben.Filipe.Pereira@iscte-iul.pt
João Aguiar - jffar@iscte-iul.pt

Análise Global

Este processo de investigação da maturidade do processo de Gestão de Incidências, possibilitou entrevistar sete organizações diferentes. Estas organizações diferem num conjunto de fatores como: indústria, tamanho, estratégia, estrutura e processos. Apesar do tamanho das organizações variar significativamente, todas as organizações são de dimensões consideráveis e úteis para a investigação.

Na Tabela 1 é possível verificar a heterogeneidade destas organizações.

Tabela 1 - Organizações entrevistadas

Industry	Size	IT employees	Multinational	IT Strategy	IT Structure
Education	1.287	20	No	Flexibility and Efficiency	Centralized
Retailing	6.000	4	Yes	Efficiency	Federal
Conglomerate	360.000	7500	Yes	Efficiency	Decentralized
Electricity, Telecommunications and Automation	1.300	9	Yes	Flexibility	Decentralized
Health	2.700	9	No	Flexibility and Comprehensiveness	Centralized
Telecommunications	2.000	----	No	Comprehensiveness and Efficiency	Decentralized
Pharmaceuticals	42.000	1320	Yes	Efficiency	Federal

Como é possível verificar a sua estrutura e estratégia de TI também difere nas diversas organizações. Por outro lado, relativamente à *framework* de TI mais utilizada pelas organizações, foi respondido que utilizam o ITIL ou não utilizam nenhuma (Figura 1).

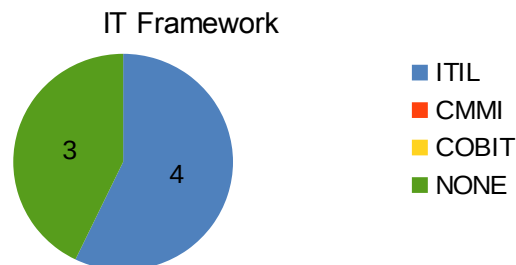


Figura 1 - Framework de TI

Apesar desta indicação verificou-se na análise da entrevista que as sete empresas efetuam mais atividades da *framework* CMMI.

Depois de analisar as respostas dadas, às 207 atividades sobre o processo de gestão de incidências foi possível obter a um nível mais objetivo e qualitativo a informação sobre a maturidade do processo.

Foi solicitada uma indicação de qual o nível de maturidade que consideravam que o seu processo de gestão de incidências se encontrava. Na Figura 2 é feita uma comparação entre essa previsão e o nível de maturidade efetivamente atingido.

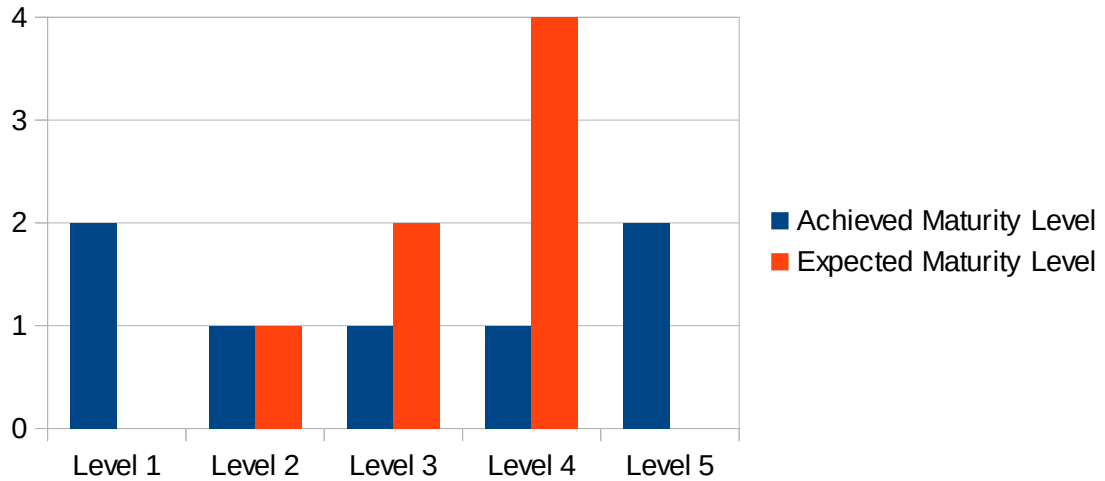


Figura 2- Nível de Maturidade expectável VS atingido

Como se pode verificar pela Figura 2 mais de metade das organizações expectarão que o nível de maturidade do processo seria o Nível 4. No fundo, a expectativa é mais concentrada, enquanto que o resultado final é mais disperso. De realçar que o nível 4 de maturidade que era o mais expectável é onde se verifica menor número de atividades efetuadas (Figura 3).

Nenhuma achou que estaria no nível 1 ou nível 5 de maturidade, mas mais de metade se encontra nesses níveis. No geral, seis empresas não se encontram no nível que esperariam e dessas empresas, três encontram-se num nível mais a baixo e as outras três num nível superior.

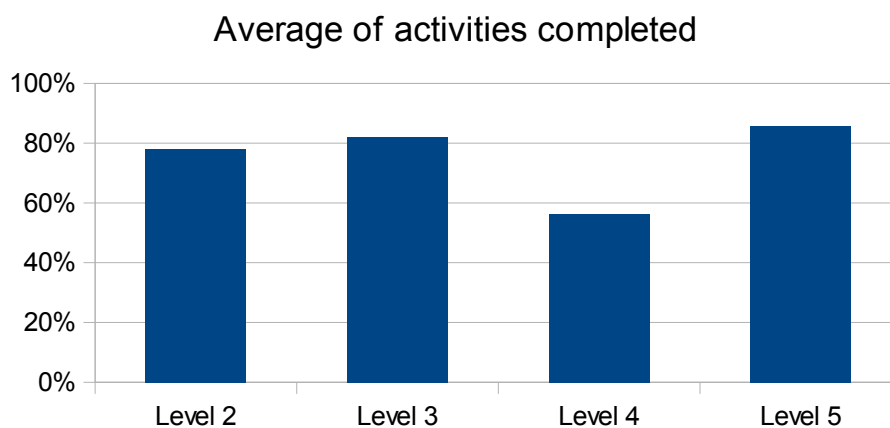


Figura 3 - Atividades Completas por Nível

O facto de o nível 4 de maturidade ser o mais baixo, significa que apesar de se fazerem planeamos, documentar e registar os documentos não se aproveita essa informação para fazer

uma análise preditiva e melhoria continua. Mesmo em organizações que estejam no nível 5 de maturidade irá diminuir o potencial de eficiência de atividades implementadas no nível 5 de maturidade.

De realçar também que no nível 3 de maturidade, em média se completam mais atividades do que no nível 2 de maturidade.

Na figura 4 é possível visualizar a distribuição de atividades completas pelas sete organizações.

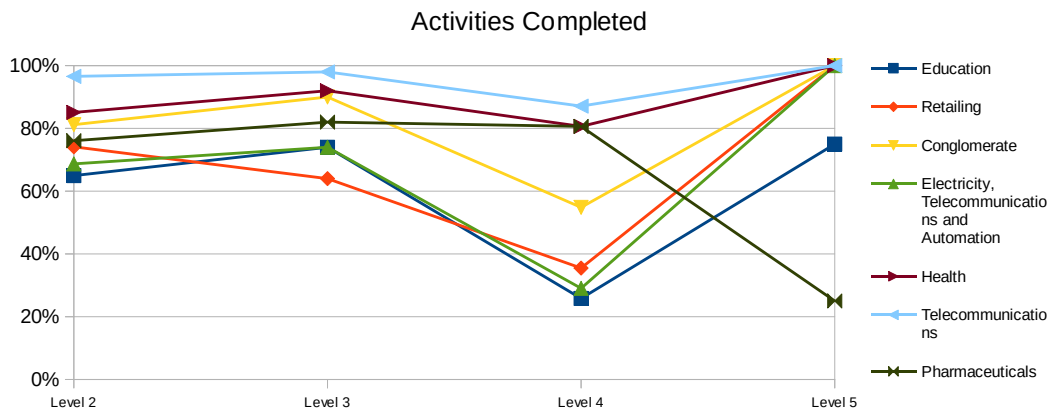


Figura 4 - Atividades Completas por Organização

Mais uma vez é possível verificar a baixa maturidade no nível 4. Por outro lado, é possível visualizar a homogeneidade da distribuição das diferentes organizações. Este resultado é obtido ainda que as organizações sejam diferentes em vários aspetos.

Chamamos a atenção da importância que o nível 4 tem na eficiência do nível 5. Só com uma boa organização de reports, métricas, KPIs, entre outros, é possível retirar o melhor das atividades colocadas em prática do nível 5. Ter a informação certa, na altura certa, no tempo certo, pode ditar uma vantagem competitiva para qualquer organização.

Análise de Framework's

Outro tipo de análise com relevo ao nível de investigação é a distribuição das atividades consoante as diferentes *Framework's* de IT. Na Figura 5 podemos verificar essa mesma distribuição e salienta-se com especial relevo que as sobreposições de atividades das 3 *Framework's* perfaz 22% do total das atividades.

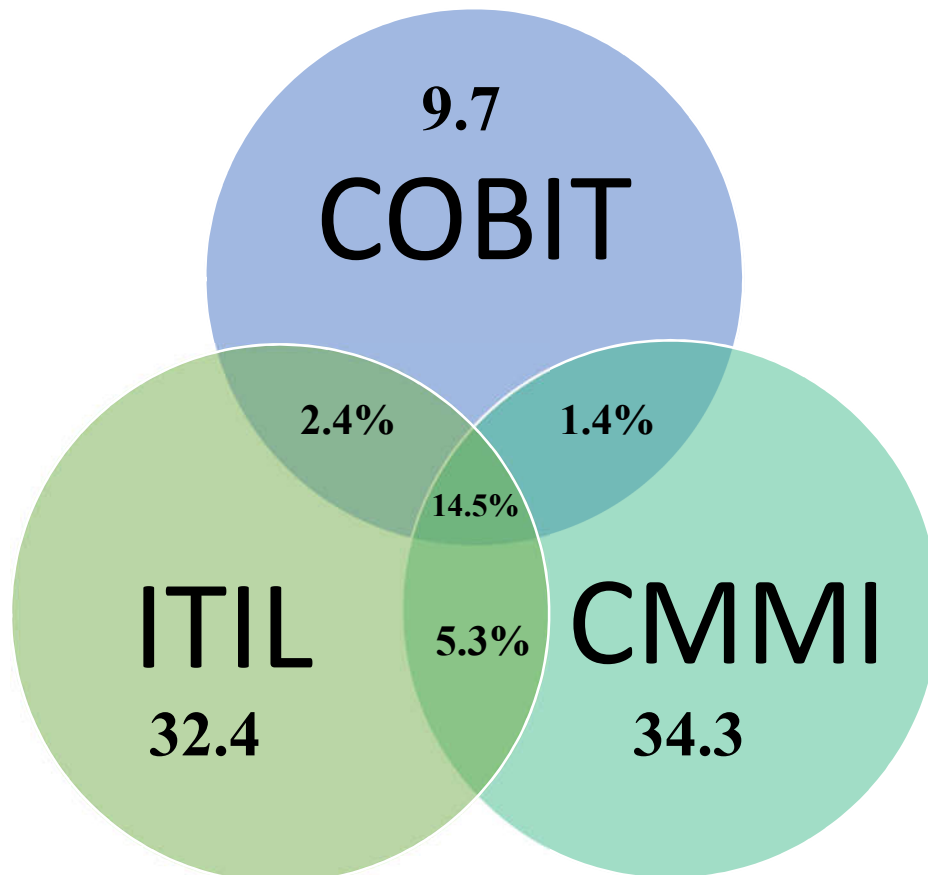


Figura 5 - Distribuição de Atividades

De salientar que o Modelo de Maturidade contempla a maioria de atividades do CMMI-SVC e do ITIL. Modelos que são claramente mais operacionais. Por outro lado, o COBIT tem exclusividade de 9.7% de atividades, mas tem 18.3% das atividades partilhadas com as outras *frameworks*. Esta *framework* é claramente mais focada na gestão dos processos.

No gráfico 6 é possível verificar a distribuição da média das atividades realizadas pelas sete organizações.

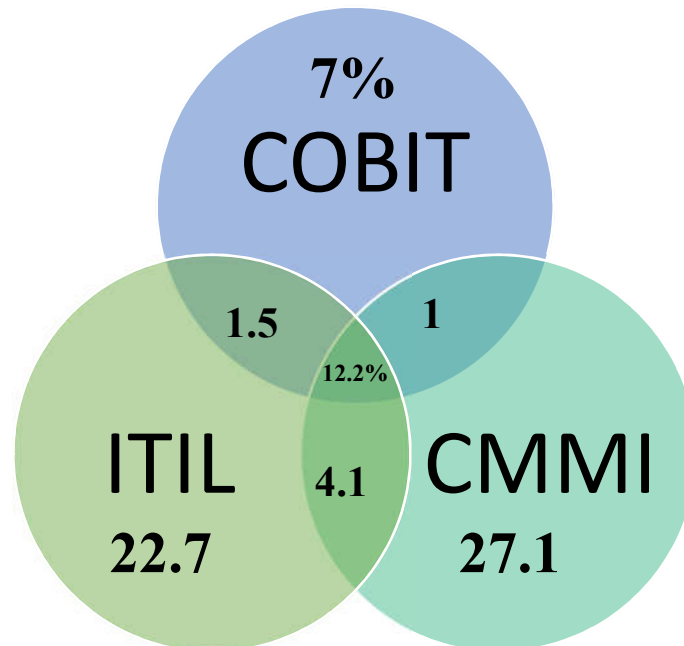


Figura6 - Distribuição de Atividades Efetuadas

A soma das percentagens de atividades realizadas, do gráfico 6, perfaz aproximadamente 75,6% do total das 207 atividades.

A distribuição das atividades efetuadas por *Framework* é semelhante à distribuição global das atividades com um pequeno foco nas atividades do CMMI em que são efetuadas 27,1% das 34,3% das atividades. No ITIL são realizadas 22,7% das 32,4% das atividades. O COBIT tem uma substancial queda percentual das atividades efetuadas, em que das 9,7% de total de atividades 7% são realizadas, o que podemos concluir que o processo se acentua mais na operacionalidade e não tanto na gestão. Relativamente às atividades que sobrepõem as 3 *framework*'s do total de 14,5% de atividades, 12,2% são efetuadas.

Considerações Finais

O racional definido para a obtenção de um certo nível de maturidade é de 75% de actividades realizadas do nível correspondente.

Em conclusão pudemos indicar 3 pontos fulcrais:

- As organizações documentam grande parte dos procedimentos e registam dados no processo de gestão de incidências
- Na sua maioria as organizações não aproveitam os dados recolhidos de incidências para fazer análise preditiva e melhoria continua
- Todas as organizações consideram a entrevista útil e dão grande importância ao processo de gestão de incidências.

Este trabalho de investigação proporcionou aprofundar os modelos de maturidades especificamente no Processo de Gestão de Incidências. Com um foco muito específico na eliminação da sobreposição de *frameworks* de forma a avaliar a maturidade do processo de forma mais célere.

Agradecimentos

Uma vez mais, agradecemos a sua disponibilidade e ajuda para o desenvolvimento deste trabalho de investigação. É graças a isso, que podemos evoluir a comunidade científica e profissional.

Ficamos ao dispor para qualquer esclarecimento adicional.

Atentamente,
João Aguiar