INSTITUTO SUPERIOR TÉCNICO
Universidade Técnica de Lisboa

Formalization of the IT Audit Management Process

Tiago Miguel Lopes do Rosário

Dissertação para obtenção do Grau de Mestre em

Engenharia Informática e Computadores

Comité de Avaliação

Presidente:	Professor Mário Rui Gomes
Orientador:	Professor Miguel Mira da Silva
Vogal:	Professor José Borbinha

Julho de 2012

Abstract

Over the last few decades, due to the numerous problems occurred in organizations, various regulations emerged. Compliance needs to ensure the adherence with these obligations, developing internal policies and procedures. However, there is no guarantee that all entities meet the organization requirements, and an auditor is the last line of defence to detect problems that may arise. Despite the importance of audit, it costs are high due to the existence of the many requirements, control implementation high costs, and the introduction of IT in organizations. So, organizations need to use IT related frameworks best practices to improve the way they conduct audits. However, those frameworks don't provide a complete and adaptable IT audit management process. In this thesis we propose the formalization of IT audit management process, taking into consideration the practices provided by the most important frameworks and literature of the area. We also provide the organizational information and applications needed to perform efficient audits. To evaluate our proposal we use YAWL-nets conversion to realize the process good construction and we collect requirements with IT and audit area experts to understand the quality of our proposal. To communicate this research we publish our work in an international conference so that scientific community can know, evaluate, and accept it. We finish our research by provide the main contributions, limitations, and future work.

Keywords: Audit, IT Audit Management Process, Compliance, Formal Process, YAWL-Nets

Resumo

Ao longo dos anos, devido aos problemas que diversas organizações sofreram, emergiram um inúmero de regulamentos. O departamento de compliance precisa de assegurar a adesão a estas obrigações, desenvolvendo políticas e procedimentos internos. No entanto, não existe a garantia de que todas as entidades sigam os requisitos da organização e, desta forma, os auditores são a última barreira para a detecção de problemas. Apesar da sua importância, a auditoria envolve custos elevados devido à existência dos diversos requisitos, aos custos de assegurar a implementação de controlos, e ao grande uso de tecnologias de informação (TI). Portanto, as organizações necessitam de usar as melhores práticas dadas pelas frameworks relacionadas com TI para melhorarem a forma de conduzirem auditorias. Contudo, estas frameworks não fornecem um processo de gestão de auditorias completas e adaptáveis. Nesta tese nós propomos a formalização do processo de gestão de auditoria de TI baseando-nos nas boas práticas que as diversas frameworks e literatura de IT fornecem. Também propomos a informação e as aplicações essenciais para realizar auditorias eficientes. Para modelar a nossa proposta utilizamos YAWL-nets para perceber se o processo está bem construído e levantamos requisitos com especialistas da área de TI e auditoria para perceber a qualidade da nossa proposta. Para comunicar esta investigação, publicámos o nosso trabalho numa conferência internacional para que a comunidade científica possa conhecê-lo, avaliá-lo e dar a sua aceitação do mesmo. Acabamos a nossa investigação com as principais contribuições, limitações, e trabalho futuro.

Keywords: Auditoria, Processo de Auditoria de IT, Compliance, Processo Formal, YAWL-Nets

Acknowledgements

I would like to express my gratitude to Professor Miguel Mira da Silva whose expertise, motivation, encouragement, understanding and patience, positively contributed considerably to my research experience.

I want to thank Rúben Pereira by all the help and guidance provided during this thesis as well as the availability to clarify any questions at any time.

I also like to thanks all the support given by my family, friends and my colleagues, during this thesis.

Finally, I would like to thank all the people that helped me in the collection of information that I used in the evaluation of my proposal and also all the opinions and help given by all Professor Miguel Mira da Silva students, especially all the support given by Carlos Mendes.

Contents

List of Tables

List of Figures

Acronyms

AICPA	American Institute of Certified Public Accountants
BPMN	Business Process Model Notation
COBIT	Control Objectives for Information and Related Technologies
CRUD	Create Read Update Delete
DSR	Design Science Research
EA	Enterprise Architecture
GRC	Governance, Risk and Compliance
GAO	Government Accountability Office
IA	Information Architecture
IIA	Institute of Internal Auditors
IS	Information System
ISACA	Information Systems Audit and Control Association
ISO	International Organization for Standardization
IT	Information Technology
IT AM	Information Technology Audit Management
ITG	Information technology governance
ITIL	Information Technology Infrastructure Library
NIST	National Institute of Standards and Technology
RM	Risk management
PN	Petri-Nets
SOX	Sarbanes-Oxley Act

Chapter 1

Introduction

Over the last few decades, numerous organizations suffered financial losses, jail terms for executives, law suits, degradation of credit rankings and stock price drops (Tarantino, 2009). The occurrence of these scandals which affected organizations such as Enron, WorkdCom, Societe General, LTCM and Sub-prime, adversely impacted business and rudely awakened organizations to act (Senft & Gallegos, 2009).

The damage made by the successive disasters eroded the trust government and people had in corporations, and leads to the rise of new laws and other regulations such as Basel II and Sarbanes-Oxley Act (SOX) (Tarantino, 2009; Carlin & Gallegos, 2007), since weaknesses in regulations were a major contributing factor to the crisis occurrence (Godellawatta, 2009). Plus, the phenomena of globalization which transported organizations to a global marketplace also contributed to increase the regulations (Tarantino, 2009).

The appearance of all these regulations over the years force organizations to improve their compliance management so that they can be on the right side of the law (Thomson Reuters, 2011), forcing them to more vigorously examine effectiveness of their internal controls and processes (Davis, Schiller, & Wheler, 2011).

Nowadays, with the financial crisis, especially in some Europeans countries, we can observe the necessity and importance of rigorous controls which impose some important sectors such as the banking area to comply with regulations that allows problems reduction (Allen & Faff, 2012). For each new law or regulation, compliance department needs to design new internal policies and procedures to deal with the rule specifications (Mcdonough & Sackmann, 2009).

Although the development of policies is a role that belongs to compliance management, there is no guarantee that all entities meet the organization requirements (Radovanovic, Radojevic, Lucix, & Sarac, 2010), and an auditor is the last line of defence to detect problems that may arise (Pai, Hsu, & Wang, 2007).

Audit is an important way for organizations to guarantee a good internal control system and compliance with all requirements (Senft & Gallegos, 2009) since it is an independent and objective assurance activity that employs systemized and standardized methods to obtain evidences (ISO

19011, 2002), evaluate and improve the effect in governance, risk management, control and compliance (Tao, 2011).

With the arrival of the information age, the impact of Information Technology (IT) on organizations keeps growing (Pai, Hsu, & Wang, 2007). Currently, IT has become increasingly more important and began to be comprised in the organization's business core processes (Webster & Watson, 2002). So, it is crucial to achieve a good alignment of IT with business needs (Grembergen & Haes, 2009) which increase the necessity of more requirements in this area (Steinberg, 2011).

On the path to improve the alignment of IT with business needs, organizations use several best practices frameworks[1] to reach their goals - not only in terms of performance but also in terms of being legislation compliant (Steinberg, 2011; Grembergen & Haes, 2009). However, these frameworks and literature isn't complete in the area of IT audit (Rosário, Pereira, & Mira da Silva, 2012).

Despite the importance of auditing, its costs are high due to the existence of the many requirements with it is necessary to comply (Senft & Gallegos, 2009; Tarantino, 2009; Griffin & Lont, 2007), the costs of ensuring control implementation (Pai, Hsu, & Wang, 2007) and the growing complexity derived from the introduction of information technology (IT) in organizations (Pai, Hsu, & Wang, 2007; Carlin & Gallegos, 2007). This makes the effectiveness of the audit low since there is an excessive consumption of assets and resources (Tarantino, 2009) as well as more misunderstandings and frameworks to consider (Senft & Gallegos, 2009).

Since the definition of formal procedures to perform audits can bring benefits to organizations (Tarantino, 2009), and knowing that IT has become crucial to the support, sustainability and growth of the business (De Haes & Grembergen, 2008), in this research we propose the formalization of the IT AM process, taking into consideration the most important frameworks and literature of the area which, as we said, separately don't describe a complete IT AM process (Rosário, Pereira, & Mira da Silva, 2012).

To model the IT AM process we use the Business Process Model Notation (BPMN), considered a de-facto standard for business process modelling (Decker & Barros, 2007). Besides that, to support the formalization we design the information and Information Systems (IS) architectures associated to the proposed process to understand what kind of data must be logical manipulated and what are the applications needed to do it.

By formalization we mean the selection of the main IT AM information sources, using them to elicit the relevant audit practices, mitigate the overlaps, and design the complete process.

[1] When we say frameworks we also include ISO's, laws, acts, regulations and others best practices aggregators.

The research methodology used is Design Science Research (DSR). We will only use constructs and models. Our constructs will be leveraged based on literature review and practitioners' expertise. Afterwards we will integrate our constructs in order to achieve our models in a complete and coherent context. The models are the IT AM process, and IT AM information and IS architectures.

To evaluate our proposal, we use four types of evaluation:

- Conversion of BPMN IT AM process into Yawl-Nets, used to evaluate the good construction of a BPMN design (Gudivada & Nandigam, 2009). This part of evaluation is focus on the process.

- Interviews with long time specialists in the area of IT. With this part of evaluation we intend to obtain a set of essentials requirements in audit responsibility.

- Questionnaires with IT auditors. These questionnaires have the purpose of understand if practitioners agree and accept the created models using the Moody & Shanks framework (Moody & Shanks, 2003) described in Section 5.3.

- Paper publication in a respectful international conference which brings valuable input for further research, feedback and approval by scientific community.

1.1 Problem

Nowadays organizations are facing an increasing number of regulations (requirements) with which it is necessary to be compliant (Tarantino, 2009; Radovanovic, Radojevic, Lucix, & Sarac, 2010) as well as an increasing number of required internal controls (Searcy, Woodproof, & Behn, 2003). Besides this, IT audit procedures also become more complex (Pai, Hsu, & Wang, 2007) since the way requirements are analyzed has also become more complex over the time (Griffin & Lont, 2007). So the way how audits are performed is affected (Senft & Gallegos, 2009). Due to this fact, IT auditors' effort is growing (Griffin & Lont, 2007) but the degree of compliance achieved is decreasing (Tarantino, 2009).

Organizations are finding soaring legal and regulatory compliance costs while effectiveness declines, giving rise to huge fines, penalties, awards, and settlements (Steinberg, 2011) and in many times they fail to comprise an effective compliance system (Mcdonough & Sackmann, 2009).

To implement an efficient IT AM process that solves these problems, organizations audit departments can use frameworks to elicit best practices in the way of perform audits.

However, frameworks are seen as complex (Pereira & Mira da Silva, 2010), too general (Morimoto, 2009), overlapping each other (Pereira & Mira da Silva, 2011; Sahibudin, Sharifi, & Ayat, 2008), hard to implement (Nicewicz-Modrzewska & Stolarski, 2008) and separately they don't propose a complete IT AM process (Rosário, Pereira, & Mira da Silva, 2012). As a result, organizations can't implement a complete process based on best practices (Rosário, Pereira, & Mira da Silva, 2012).

Since audit is a crucial way for organizations to achieve their goals and knowing that IT has become crucial to the support, sustainability and growth of the business (De Haes & Grembergen, 2008), IT AM process activities need to be well defined so that they have a high level of maturity and not be carried out in an *ad-hoc* way (Tarantino, 2009). To achieve these intents, activities need to be standardized and the IT AM process needs to be well defined (Senft & Gallegos, 2009; Tarantino, 2009).

In summary we can state that the problem of this thesis can be described as:

Most organizations IT audit management process is not efficient since it cannot be based on best practices given that frameworks are seen as complex, too general, overlapping each other, hard to implement and separately they don't propose a complete IT audit management process.

We intend to formalize the IT AM process by taking into consideration the most important frameworks and literature of the area contributing to solve this problem. Without the formalization of the process, audit will, in most cases, keep being performed in an *ad-hoc* way (Rosário, Pereira, & Mira da Silva, 2012).

1.2 Thesis Structure

This document is divided in six main chapters:

1. **Introduction:** This chapter focuses on the general context in which the theory fits and in the problems this thesis addresses.

2. **Research Methodology:** Second chapter focuses on the methodology used in the research.

3. **Related Work:** In chapter three we perform a literature review that will be crucial for our proposal's coherence.

4. **Proposal:** In chapter four we detail the constructs and models of IT AM proposal.

5. **Evaluation:** Chapter five provides an analysis and discussion of the artifacts' developed, including the evaluation phase of design science research.

6. **Conclusion:** In chapter six we provide our conclusion, contributions, limitations, lessons learned and future work.

Chapter 2

Research Methodology

The research methodology that will be used in this thesis is Design Science Research (DSR). Toward the end of the 1990s began growing in popularity for use in scholarly investigations in IS. DSR methodology is conducted in two complementary phases, build and evaluate. In contrast with behaviour research, design-oriented research builds a “to-be” conception and posteriorly seeks to build the system according to the defined model taking into account restrictions and limitations (Osterle, et al., 2011). Design science addresses research through the building and evaluation of artefacts designed to meet the identified business needs (Hevner & March, 2004) instead of analysing existing IS in order to identify causal relations (Osterle, et al., 2011).

Since we build and evaluate new and innovative artefacts following the design research paradigm (Hevner et al., 2004), we argue that a better understanding of IT AM process can be accomplish.

Based on the four design artefacts produced by design science research in IS (constructs, models, methods and instantiations) we will focus on constructs and models. Constructs are necessary to describe certain aspects of a problem domain and allow the development of the research project’s terminology (Schermann, Ohmann, & Krcmar). In other words, they provide the language in which problems and solutions are defined and communicated (Schon, 1983). Models use constructs to represent a real world situation, the design problem and the solution space (Simon, 1996).

We propose three models, IT AM process, IT AM information architecture and IT AM IS architecture which have associated, respectively, three groups of constructs: IT audit phases and sub-phases, IT audit roles, IT audit activities and IT audit data; IT AM process information entities; and the two first developed models which are the input of the third model.

As advisable by March & Smith (March & Smith, 1995) the research methodology applied is divided according to the two processes of design science research in IS: build and evaluate. The build process is composed by two stages and the evaluation process is comprised by only one (Table 1). This kind of research approach was already used in other research papers as (De Haes & Grembergen, 2008; Vicent & Mira Da Silva, 2011; Pereira & Mira da Silva, 2012).

In the first stage we have started with literature review. Because research in some of the proposed constructs is poorly explored/synthesized or even in the early stages, part of this research is exploratory rather than hypothesis testing.

Table 1. Research Methodology

Build				**Evaluate**
Constructs Definition:	**IT AM Process Construction:**	**IT AM Information Architecture Construction:**	**IT AM IS Architecture Construction:**	**Evaluation:**
- IT Audit Sub-Phases[2] - IT Audit Roles - IT Audit Activities - IT Audit Data	- Analyze the relationship between constructs - Integrate constructs			- Interviews - Yawl-Nets - Questionnaire
- IT AM Process Information Entities		- Analyze the relationship between constructs - Integrate constructs		- Interviews - Questionnaire
- IT AM Process - IT AM Information Architecture			- Analyze the relationship between constructs - Integrate constructs	- Interviews - Questionnaire

Exploratory research often builds on secondary research, “such as reviewing available literature and/or data or qualitative approaches such as informal discussions with customers, employees, management or depth interviews, focus group projective methods, case studies or pilot studies” (De Haes & Grembergen, 2008).

In order to leverage the IT audit sub-phases, IT audit roles, IT audit activities, IT audit data and IT AM process information entities we will use extensive literature review. The approach used in this thesis follows the concept-centric methodology of IS literature reviews as outlined in (Webster & Watson, 2002).

Österle et al. (Osterle, et al., 2011) also point four principles that design-oriented IS research must comply with, and that we followed:

[2] IT Audit Phases are given in the Related Work section since it is not an our construct

- **Abstraction.** This thesis proposes a complete and adaptable IT AM process. Hence it must be abstract in order to generalize the IT audit processes, and must provide procedures that allow the generalization of future implementations.

- **Originality.** The artefact proposed is not present in the body of knowledge of the domain.

- **Justification.** The various methods proposed to evaluate the artefact should justify the artefact.

- **Benefit.** A complete, general and adaptable IT AM process based on literature and frameworks best practices helps organizations in the conduction of more efficient audits.

Additionally, we followed the guidelines for design science research proposed by Hevner (Hevner & March, 2004). These guidelines are: design as an artefact, problem relevance, design evaluation, research contributions, research rigour, design as a search process, and communication of research. A design artefact is complete and effective when satisfies the requirements and constraints of the problem that was meant to solve. In this thesis we evaluated our artefacts through interviews and questionnaires, and using conversion to Yawl-Nets in the IT AM Process Model. Submitting these research results to respected international conferences, we also used the appraisal of the scientific community as evaluation criteria.

Chapter 3

Related Work

In this chapter we essentially describe the main ideas around audit function, in a way that allows a complete understanding about this domain and it relationships with others. To this purpose, we describe the following sections:

3.1 **Governance, Risk and Compliance (GRC)**. We provide and superficial definition of GRC domain in order to understand the domains with which audit is related.

3.2 **Governance**. We provide the definition of governance.

3.3 **Risk**. We provide the definition of risk management.

3.4 **Compliance**. We provide a more complete description of compliance field since it is the domain where audit remains.

3.5 **Audit**. We provide the main concepts and objectives behind audit function.

3.6 **IT Audit Management Process**. We describe the phases of an IT AM process in a non-detailed level. As we said before, IT AM process is not provided in detail by a framework or main literature since they are always incomplete (Rosário, Pereira, & Mira da Silva, 2012). However, frameworks and literature provide an idea about the four main phases of audit that we provide here and which are the foundation to IT AM process BPMN detailed decomposition of our proposal.

3.7 **IT Audit Bodies and Standards**. Since IT audit is a specific function and it's not oriented by the same organisms and standards of general audit, we describe the main organisms in the area in order to be able to understand what kind of standards and practices they provide.

3.8 **Theoretical Background**. We provide the theoretical background necessary for the construction of our proposal.

3.9 **Conclusion.** We give the main conclusions of this chapter and provide an analysis about the limitations of actual work made in IT audit management function.

3.1 Governance, Risk, and Compliance (GRC)

IT audit is inserted in IT compliance domain which in turn belongs to Governance, Risk and Compliance (GRC) (Vicent & Mira Da Silva, 2011).

Racz provides the definition of GRC which can be the basis for our description:

“GRC is an integrated, holistic approach to organization-wide governance, risk and compliance ensuring that an organization acts ethically correct and in accordance with its risk appetite, internal policies and external regulations, through the alignment of strategy, processes, technology and people, thereby improving efficiency and effectiveness” (Racz, 2010).

The definition of GRC shows that Governance, Risk and Compliance are domains with too many relations between them. Despite of our research is focus in audit which belongs to compliance, it is important to realize that audit also is part of a major domain, affecting directly compliance, but also more indirectly governance and risk management (Vicent & Mira Da Silva, 2011). So it is important to understand the meaning and main objectives of governance, risk and compliance.

3.2 Governance

Corporate governance has the goal of defend the interests of organization stakeholders (Weill & Ross, 2004) who can include board members, organization executives, employees, stockholders, suppliers, customers, and the community in which the organization operates (Tarantino, 2009).

The goals describe above are stated in the definition of corporate governance:

“Corporate governance needs to define and realize missions and goals, establish strategic direction, policies and objectives to that end, and monitor implementation” (Mcginnis, Pumphrey, Trimmer, & Wiggins, 2004).

Information technology governance (ITG) is part of corporate governance (Grembergen & Haes, 2009; Racz, 2010). It applies corporate governance concepts to drive and control IT in a strategic way, concerning about the value IT delivers to an organization (Grembergen & Haes, 2009).

ITG is defined as:

“The system by which the current and future use of IT is directed and controlled. It involves evaluating and directing the plans for the use of IT to support the organization and monitoring this use to achieve plans. It includes the strategy and policies for using IT within an organization” (Lewis & Millar, 2008).

3.3 Risk

Risk management (RM) provides organizations a programmatic way to deal with business uncertainty and the associated risk and opportunity (Tarantino, 2009). It seeks to identify, assess, and measure risk and then develop countermeasures to handle it (COSO, 2004).

RM is defined as:

"A process, affected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives" (COSO, 2004).

3.4 Compliance

In an organizational context, compliance describes the processes that ensure the adherence of an organization to regulatory, legal, contractual and other obligations such as standards, internal policies and contractual obligations (Tarantino, 2009).

So, compliance must guarantee that the organization is following all its obligations, and thus is operating within the defined mandated and voluntary boundaries (Banca D'Italia, 2007).

Compliance is defined as:

"The process of adherence to professional codes of practice, policies and decisions as well as the process that assures conformity within regulations, controlling all the activities of the organization and reporting the right information to the right people" (Bace & Rozwell, 2006).

The myriad of activities, processes and behaviors that lay on compliance can be overwhelming (Griffin & Lont, 2007). But if organizations can manage all these activities and prove it, they will operate more efficiently, compete more effectively, and achieve their objectives (Tarantino, 2009).

Compliance needs to be aligned with governance since there is a set of policies and procedures which deal with aspects of these legal and regulatory requirements (Steinberg, 2011). For each new law or regulation, new internal policies and procedures are designed to deal with the rule specifications (Mcdonough & Sackmann, 2009) and their good implementation is assessed by audit activity (Grembergen & Haes, 2009). In order to achieve compliance with regulations, organizations must ensure that their business practices are in accordance with these requirements (Thomson Reuters, 2011).

Compliance is responsible for design compliant business processes. However, auditors need to complement this task because some deviations from an expected business process might occur (ISO 19011, 2002).

Compliance functions can be decomposed in four major objectives:

- **Identify and assess regulations**. Compliance needs to identify and understand the existing regulations (Thomson Reuters, 2011), and how they apply to the company and its operations (Tarantino, 2009).

- **Develop and implement policies**. A policy is a document that establishes rules for expected behaviour of individuals, processes, and/or relationships (Thomson Reuters, 2011; Tarantino, 2009). Procedures are documents that provide an established or official way of complying with a policy (Thomson Reuters, 2011; Tarantino, 2009). By the definition of ITG, policies are managed by governance too, so, compliance needs to closely collaborate with it.

- **Educate and advise**. Compliance should establish written guidance to staff on the appropriate implementation of compliance laws, rules and standards through policies and procedures and other documents such as internal codes of conduct and practice guidelines (Thomson Reuters, 2011).

- **Monitor and document**. Compliance needs to make sure that, policies and procedures are being followed and that compliance efforts are being clearly documented (Senft & Gallegos, 2009).

To achieve these objectives, compliance needs to establish a structure based on four parts (Tarantino, 2009; Vicent & Mira Da Silva, 2011; Banca D'Italia, 2007) which we represent in Figure 1.

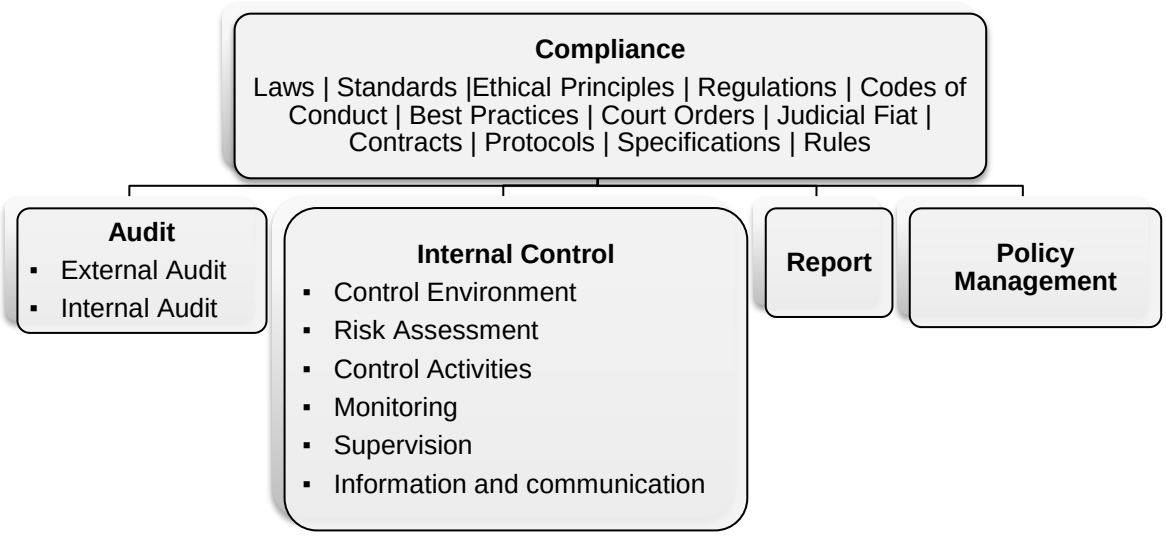

Figure 1. Compliance Structure. *Adapted from (Rosário, Pereira, & Mira da Silva, 2012)*

Since IT is becoming pervasive in any organization of the world (Webster & Watson, 2002), IT decisions cannot be primarily based upon technology updates, storage capacity or cost savings independently of legal and compliance considerations (Little, 2007). So it is imperative for IT departments to ensure that their applications meet all compliance requirements that govern their products, services, and other activities (Gudivada & Nandigam, 2009).

When we talk of IT compliance, we are mainly focusing on metering and auditing software licenses, authorization and authentication for IT resource usage, physical security for computer systems, data centers, policies and procedures for IT operations and help desk support, protecting the privacy of data stored on computer systems, and prevention and detection of illegal activities (Tarantino, 2009).

IT influences the achievement of compliance because automation is a way to perform an efficient validation of compliance requirements and it also improves controls (Thomson Reuters, 2011). Since corporations heavily depend on IT systems for their daily operations, it is natural that they play a greater role in meeting the compliance requirements (Gudivada & Nandigam, 2009).

3.5 Audit

Audits are conducted in diverse legal and cultural environments (Tarantino, 2009), within organizations that vary in purpose, size, complexity, and structure, and by persons within or outside the organization (The Institute of Internal Auditors, 2010). However, the benefits to organizations are always the same since auditors are counsellors in advising on control issues as they relate to business processes (Carlin & Gallegos, 2007), promoting the collaboration and integration of the corporate governance and modern internal controls (Yang, 2011).

Audit is an independent and objective assurance activity (ISO 19011, 2002; Thomson Reuters, 2011) that employs systemized and standardized methods (Tarantino, 2009) to evaluate and improve the process of governance, risk management, control and treatment, so as to help the organization achieve its objectives (Tao, 2011).

Audits can be classified as internal or external (ISO 19011, 2002):

- **Internal audit.** Internal audits, sometimes called first party audit, are conducted by the organization itself for support management review and other internal reasons, and may provide the basis of self compliance.

- **External audit:** External audits include those generally called audits of the second and third parts. The second party audits are performed by the parties with an interest in the organization, such as customers. The third-party audits are conducted by independent external auditors, such as those who make compliance certification with the requirements of

ISO's, acts or other frameworks.

Audit provides management with assurance, design and operation of the governance, risk management and control processes in their organizations, which requires an impartial view (Tarantino, 2009). However, it is important to note that the role of audit management is not just to perform audits. Audit exists to provide:

- **Assurance**. Assurance includes an objective examination of evidence (Tarantino, 2009) intended to provide confidence as well as providing accurate and current information about the efficiency and effectiveness of policies and operations, and the status of compliance with the statutory obligations (Senft & Gallegos, 2009; Chen, Yoon, Frenz, & Compres, 2011).

- **Assessment and Recommendations**. Audit adds value by assessing and making recommendations on the effectiveness of the mechanisms that are in place to ensure that the organization achieves its objectives (Senft & Gallegos, 2009) and by performing this function in a way that demonstrates informed, accountable decision-making with regard to ethics, compliance, risk, economy and efficiency (Thomson Reuters, 2011) The recommendations have associated evidences and are compiled into action plans that organizations should follow to improve their mechanisms (Vicent & Mira Da Silva, 2011).

- **Oversight**. Audit contributes to the basis by which decision-makers achieve oversight and control of their organizations, target their attention to areas in need of improvement and demonstrate accountability (Thomson Reuters, 2011). Accordingly, audit takes a disciplined, evidence-based approach to determining whether or not assurance can be provided and to ensuring key systems and processes are appropriately designed and are functioning as intended (Davis, Schiller, & Wheler, 2011).

- **Advisory Services**. As an adjunct to the assurance role, and with their knowledge, auditors also provide advisory services to their organizations and offer solution-oriented recommendations (Thomson Reuters, 2011).

The impact of IT on organizations keeps growing (Pai, Hsu, & Wang, 2007). Currently, IT has become increasingly more important and it is comprised in the organization's business core processes (Webster & Watson, 2002). So, it is crucial to achieve a good alignment of IT with business needs (Grembergen & Haes, 2009) which increases the necessity of more requirements in this area (Steinberg, 2011). Due to this, audit began to incorporate the IT area, emerging the IT audit domain.

Nowadays, IT auditors' role is becoming crucial to organization success since their work evolved from monitoring and evaluation to the identification, consultation (Yang, 2011) and partnership of senior management (Carlin & Gallegos, 2007). IT Auditors are now, counsellors in advising on IT control issues as they relate to business processes (Carlin & Gallegos, 2007), promoting the collaboration

and integration of the corporate governance and modern internal controls (Yang, 2011). They are also a partner in helping managers develop and implement the policies needed to attain information assurance (Carlin & Gallegos, 2007). The transformation is also conducive to the unity of the external accountability and the internal accountability of all types of enterprises (Yang, 2011).

So, IT audits ensure that organizations monitor how they do business and protect the interests of main stakeholders as managers, employees, customers, and investors (Carlin & Gallegos, 2007).

One of the audit's fundamental purposes is to ensure the correct implementation of certain standards and regulations (Senft & Gallegos, 2009; Adrian, Beres, & Shiu, 2008). Also, to improve the management of IT, organizations are using practice frameworks (COBIT, ITIL, etc) to ease the work (Adrian, Beres, & Shiu, 2008). It is the responsibility of the audit team to test if they are well implemented (Senft & Gallegos, 2009). IT audit represents a procedure used to assess whether the IT acts in the function are successfully accomplishing the business objectives.

IT audit definition is given by the Institute of Internal Auditors (IIA):

"IT audit is the process of gathering and evaluating evidence based on which one can evaluate the performance of IT systems, i.e., to determine whether the operation of IS in the function of preserving the property and maintain data integrity" (The Institute of Internal Auditors, 2010).

IT audit also includes the use of IT to support audits (Senft & Gallegos, 2009) which allows more efficient ways of analyzing the effectiveness of the implemented controls (Tarantino, 2009).

To finalize the audit description we show a graphical representation with the essentials concepts in a conceptual map which can provide a good visualization of the domain. The conceptual map can be seen in Figure 2.

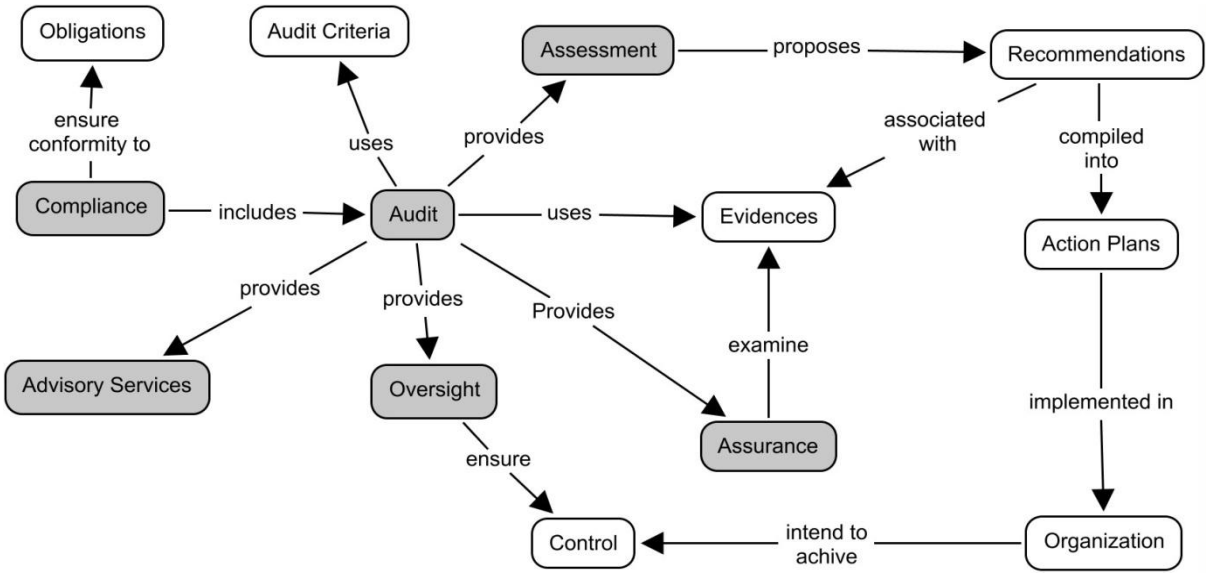

Figure 2. Audit Essentials Conceptual Map. *Adapted from (Rosário, Pereira, & Mira da Silva, 2012)*

3.6 IT Audit Management Process

IT Audit management process is defined as "a systematic, independent and documented process for obtaining audit evidences and its objective assessment in order to determine the extent to which audit criteria are satisfied. Audit evidences are records, statements or other information that is verifiable and relevant to audit criteria. Audit criteria are a set of policies, procedures or requirements" (ISO 19011, 2002).

The process can be described as a set of steps that are separate in phases, each one with a purpose well defined to achieve audit objectives (Senft & Gallegos, 2009).

Although there isn't a complete IT AM process proposed by frameworks or main literature, there is a consensus about the more generic audit phases (Rosário, Pereira, & Mira da Silva, 2012) that constitute an one direction flux (Grembergen & Haes, 2009) as we demonstrate in Figure 3.

Figure 3. IT Audit Phases

So, the descriptions of IT audit phases provided by frameworks and main literature (ISO 19011, 2002; Davis, Schiller, & Wheler, 2011; De Haes & Grembergen, 2008 for example) are:

- **Planning**. This phase provides the audit meaning. It is defined what is pretending with the audit which is critical from a business perspective. Also it is defined what is included in the audit, establishing the audit boundaries.

- **Preparation**. In this phase it is defined the essentials to perform the audit, selecting the requirements to evaluate, determining who will participate in the audit and choosing all the support documents and tool necessary to perform the audit.

- **Execution**. This phase correspond to the conduction of the audit. All the tests, procedures and problems finding are made using evidences elicitation.

- **Reporting**. In this phase it is made an audit report where all the audit findings are listed and explained. This document should provide solutions which guarantee that audit meaning (establish in Planning phase) is reached.

3.6.1 ISO 19011

ISO 19011 (ISO 19011, 2002) needs to be referred since it is the only best practice aggregator[3] that tries to provide a complete IT AM process. The other analyzed documentation doesn't provide detailed information about the process itself focusing on the auditor behavior or singular activities. The exception is some literature such as Senft and Gallegos (Senft & Gallegos, 2009) or Tarantino (Tarantino, 2009) which give their point of view of the process but in a low-detailed perspective.

ISO 19011 intent to provides guidance in the management of audit programmes, the conduct of internal or external audits of quality and/or environmental management systems, as well as on the competence and evaluation of auditors.

The process provided by this ISO, have a good detail but is incomplete (Rosário, Pereira, & Mira da Silva, 2012). The main cause is the limited scope which is to provide "guidelines for quality and/or environmental management systems auditing" (ISO 19011, 2002).

ISO 19011 provides a process with four phases (the same described above), detailing each one in sub-phases which in turn are decomposed into atomic activities.

In spite of being incomplete, this ISO is a good basis for our work.

3.7 IT Audit Bodies and Standards

The main bodies of IT audit function are showed in Table 2 (the description of each body was collected in the respective web-site). These bodies are accepted by all as a reference in the area of IT audit, providing standards and certification for auditors. In our research is important to know what these bodies can provide in terms of IT AM process since they are seen as best practices providers. Some of these bodies, such as American Institute of Certified Public Accountants (AICPA) or Government Accountability Office (GAO), provide best practices that, although was based on IT audit, can't be used in our work since they don't provide information about the process itself. In spite of we don't use directly the standards of these bodies in our proposal, it is important that they here mention in Table 2 since they belongs to reference institutes in the area of IT audit.

[3] Law, Act, ISO, Framework etc.

Table 2. Main IT Audit Bodies

Name	Acronym	Description
Information Systems Audit and Control Association	ISACA	ISACA provides practical guidance, benchmarks and other effective tools for all enterprises that use IS. Through its comprehensive guidance and services, ISACA defines the roles of IS governance, security, audit and assurance professionals worldwide. **(https://www.isaca.org)**
American Institute of Certified Public Accountant	AICPA	AICPA is the national professional organization of Certified Public Accountants, with more than 370,000 members in 128 countries in business and industry, public practice, government, education, student affiliates and international associates. **(http://www.aicpa.org)**
Institute of Internal Auditors	IIA	IIA is an international professional association which is the internal audit profession's global voice and principal educator. Members work in internal auditing, RM, governance, internal control, IT audit, education, and security. Also educational institutes such as MIT are member of IIA. The IIA in North America comprises 157 chapters serving more than 70,000 members. **(https://na.theiia.org/)**
Government Accountability Office	GAO	GAO is the audit, evaluation, and investigative arm of the United States Congress. It is part of the legislative branch of the United States government. **(http://www.nist.gov/index.html)**
National Institute of Standards and Technology	NIST	NIST is a measurement standards laboratory, which is a non-regulatory agency of the United States Department of commerce. **(http://www.nist.gov)**

The standards that provide useful information to our work are described in Table 3.

Table 3. Main IT Audit Standards and Frameworks

Name	Type	Provided by	Reference
International Standards For The Professional Practice Of Internal Auditing	Standard	IAA	(The Institute of Internal Auditors, 2010)
Control Objectives for Information and Related Technologies (COBIT)	Framework	ISACA	(IT Governance Institute, 2007)
Information Technology Infrastructure Library (ITIL)	Framework	Office of Government Commerce	(Taylor, Iqbal, & Nieves, 2007)
ISO/IEC 27001 - Information Technology - Security Techniques - Information Security Management Systems – Requirements	ISO	ISO	(ISO 27001, 2005)
ISO/IEC 38500 – Corporate Governance of Information Technology	ISO	ISO	(ISO 38500, 2008)
ISO/IEC 19011 - Guidelines for quality and/or environmental management systems auditing	ISO	ISO	(ISO 19011, 2002)

We use these standards to elicit requirements to our IT AM process (Section 4), complementing them with main IT and audit literature.

3.8 Theoretical Background

In this section we will provide the necessary theoretical foundation to understand the basis of our proposal. The next sub-section detailed the foundations that support the constructs and models developed.

3.8.1 Business Process Model Notation

Business process modeling is key component of Process-Aware IS (Mendling, Dongen, & Aalst, 2007). Process models can serve as a conceptual representation of the system, or as a specification of an executable workflow process (Mendling, Dongen, & Aalst, 2007). Nowadays, business process modeling is a key technology to bridge the gap between business and IT (Takemura T. , 2008). There are difficulties in the communication between business personnel and IT staff. Business process modeling bridges this gap by describing business processes in a notation that is understandable not only by business persons but also rigorous enough for IT persons to develop or implement an IT system (Takemura T. , 2008).

The specification of BPMN notation does not include formal semantics (Takemura T. , 2008; Sun, Song, & Wen, 2008). Also, BPMN does not provide any meta model for abstract syntax nor formal semantics (Takemura, 2008).

3.8.1.1 Petri-Nets

Petri-Nets (PN) is a formal modeling language that allows processes analyzes (Dijkman, Dumas, & Ouyang, 2007). By the definition of PN's it is possible to understand that this language solve the limitations referred about BPMN since PN include formal semantics.

3.8.1.2 YAWL Nets

YAWL is a state-based formal model language that is based on PN (Sun, Song, & Wen, 2008), but that solves some conversion limitations of them (see Section 5.1). Since YAWL is based on PN, it also provides a firm basis for the formal analysis of real-world services (Sun, Song, & Wen, 2008).

3.8.2 Archimate

Archimate are a high-level modelling language used to describe the enterprise architectures (EA) (Lankhorst, 2009). The Archimate has three main layers which are (Lankhorst, 2009):

- Business layer about business processes, services, functions and events of business units.

- Application layer supports the business layer with application services which are realized by (software) application components.

- Technology layer offers infrastructural services needed to run applications, realized by computer and communication devices and system software.

The Archimate language has the concept of viewpoints. A viewpoint defines abstractions on the set of models representing the EA, each aimed at a particular type of stakeholder and addressing a set of concerns (Lankhorst, 2009).

3.8.3 Information Architecture

In the context of Archimate, the information architecture (IA) is part of the business layer (Lankhorst, 2009). IA is the modeling of a structure or the organization of information (McNay, 2003) which is represented by information entities. An information entity is a concept relevant to the organization business that is important to save electronically (Marques, Borges, Sousa, & Pinho, 2011). IA can be viewed as a structured set of multidimensional interrelated elements that support all information processes (Watson, 2000). Nowadays, organizations perceive the importance of linking business architecture to IA, (Kamath, 2011). With this linkage, it is possible to manage the changes needed by the business and maximize the benefits from the IT investments (Kamath, 2011). However, the current ad-hoc IA in place within many organizations cannot meet an organization's future needs because it has an incoherent framework, incompatibilities, missing elements, few and poorly understood standards, uneven quality and unnecessary duplications (Watson, 2000).

3.8.3.1 Information Structure Viewpoint

The Information Structure viewpoint is basically identical to the traditional information models created in the development of almost any IS (Lankhorst, 2009). It shows the structure of the information used in the enterprise or in a specific business process or application, in terms of data types or (object-oriented) class structures. Furthermore, it may show how the information at the business level is represented at the application level in the form of the data structures used there, and how these are then mapped onto the underlying infrastructure.

3.8.4 Information Systems Architecture

Information Systems architecture focuses on identifying and defining the applications[4] and data considerations that support the Business Architecture, by defining views that relate to information,

[4] In Archimate applications and informations systems represent the same concept. So, we use both to express the same idea

knowledge, application services, etc. (Lankhorst, 2009). Archimate presents only one layer - application architecture - to describe the IS architecture.

3.8.4.1 Create, Read, Update and Delete Matrix

Create, Read, Update and Delete (CRUD) matrixes were introduced in the 1970s in information engineering and related methods (Lankhorst, 2009). They are communication models that represent communication interfaces among applications. An application is a software system used in some, but not all, business processes. It is developed to provide certain services in certain business processes, and therefore has particular user groups. In the context of this thesis, with the CRUD matrix it is possible to understand the needed applications to perform the IT AM process, the information that each system manipulate, and the relations between the systems. The CRUD also is important to prove the consistency between applications and IS (Lankhorst, 2009).

3.8.4.2 Application Cooperation Viewpoint

The Application Cooperation viewpoint shows the relations of a number of applications or components (Lankhorst, 2009). It describes the dependencies in terms of the information flows between them, or the services they offer and use. This viewpoint is typically used to create an overview of the application landscape of an organization.

3.8.4.3 Application Structure Viewpoint

The Application Structure viewpoint shows the structure of one or more applications or components (Lankhorst, 2009). This viewpoint is useful in designing or understanding the main structure of applications or components and the associated data.

3.9 Conclusion

This chapter gives us an overview of the IT audit scope. It is possible to realize that the audit is an essential function in the compliance structure because it is an important tool to ensure that the requirements and controls are well implemented. Besides that, this section shows that audit benefits are extensible to an even more embracing domain (GRC), positively affecting the governance of IT and risk management.

Focusing on process, we can say that the existing frameworks and literature are quite limited. The only aspect where there is a consensus is in the four phases in which an audit should be performed. However, these four stages, give very limited understanding of the process and a poor contribution to its implementation.

The standards provided by main IT audit bodies provide a set of best practices to improve IT audit. However, these practices are focused in the auditor conduct, providing a limited view of the whole process.

Only ISO 19011 provides a more descriptive process. For each one of the four phases it describes what each one must contain. However, it doesn't provide a detailed description of all needed activities to be carried out, not allowing by itself a complete process implementation.

A good addition to this ISO is present in literature where some IT audit books also propose a process. However, the process proposed by some authors is even more limited than that proposed by ISO 19011 in addition to not having the same scientific rigor. These books are based on very specific aspects of certain audit areas such as security, not giving a good focus in the overall process.

Thus we can argue that, in the frameworks or literature domain, there isn't a formal and complete description of the generic IT PM process yet.

Chapter 4

Proposal

In order to address the problem described in Section 1.1, the proposal of this thesis is the modelling of IT AM process, the necessary data to support them, expressing in information architecture, and the applications needed to manipulate the information and support the processes.

As stated in Section 2 this research is based on design science research, and the artefacts produced are focused on constructs and models. This chapter corresponds to the development of the build phase.

In our proposal we formalize the IT AM process by analyse the most important frameworks and literature of IT, eliciting information about the way of perform audits. We access all information that can represent IT audit activities, ways of group activities (processes, sub-processes, etc.), the flows between activities and others.

It is important to understand that by formalization we mean that we use the most used and accepted frameworks and literature to elicit IT audit activities that correspond to best practices and assess them to design a complete IT AM process. Using frameworks and literatures best practices recommendations we can propose standardized activities that can be ordered to obtain a complete formal process.

So, our proposal starts with an analysis of the main frameworks and literature to elicit the sub-phases, roles, activities and data included in the IT AM process. We need to leverage these informations, to design our models. We use the audit worldwide accepted phases as the basis of our work (described in section 3.6). To each phase we need to analyze frameworks and main literature to elicit sub-phases. Then, a similar procedure is done to elicit activities. Sub-phases have associated multiple activities and if we join the three in a hierarchical way, we have the basis of processes, sub-processes and tasks in the proposed IT AM Process. Combining roles with the activities we can understand what each one do and combining activities with data we can understand which data is manipulated in each task and by whom, knowing the role behind the task.

As a result, with the analyses of the described information we can design the IT AM process in BPMN, describing a way of organizations perform their audits. We also propose an IA that describes the

information manipulated in the process. Nowadays, organizations perceive the importance of linking business architecture to IA, (Kamath, 2011). With this linkage, it is possible to manage the changes needed by the business and maximize the benefits from the IT investments. Finally, a IS architecture is designed so that organizations know what are the systems needed to support audit procedures.

Next sections describe in detail the construction of these artefacts.

4.1 IT Audit Sub-Phases

IT AM process can be described as a set of phases and sub-phases, each one with a well defined purpose (Senft & Gallegos, 2009). We use the phases described in Section 3.6 as the basis for our constructs, using them as the major processes of the IT AM Process. Then, to develop our solution we analyze some of the most known frameworks of the area as well as some of the most relevant literature and we obtain the sub-phases which are one more construct to the process design. The sub-phases elicit are described in Table 4.

Table 4. IT AM Phases and Sub-Phases

Phases	Sub-Phases	Description	Frameworks / References
Planning	Establish audit objectives	Determination of what is intended to be accomplish with the audit accordingly with the requirements analysis	(Davis, Schiller, & Wheler, 2011), (Wu, Shao, Ho, & Chan, 2008), (Carlin & Gallegos, 2007) (ISO 19011, 2002)
	Establish audit scope and schedule	Scheduling of audit in cooperation with the audit entity	(Senft & Gallegos, 2009), (Grembergen & Haes, 2009) (Davis, Schiller, & Wheler, 2011), (Davis, Schiller, & Wheler, 2011) (ISO 19011, 2002)
Preparation	Audit team selection	Selection of auditors to perform the audit	(ISO 19011, 2002)
	Obtain preliminary background of audited areas	Performance of a preliminary survey of the area to be audited to understand what the audit will entail	(Senft & Gallegos, 2009) (Davis, Schiller, & Wheler, 2011)
	Define procedures	Preparation of audit procedures list for the area being audited	(Senft & Gallegos, 2009) (ISO 19011, 2002)
	Audit support documents preparation	Development of standard audit checklists and other support documents for the areas being audited	(Grembergen & Haes, 2009) (Davis, Schiller, & Wheler, 2011) (ISO 19011, 2002)

Execution	Kick-off meeting	Performance of a kick-off meeting with the audited entity to communicate what is in and out of audit scope, and also establishment of procedures needed to perform the audit	(Davis, Schiller, & Wheler, 2011) (ISO 19011, 2002)
	Collection of evidences and issues	Collection of information to assess the actual state of audited areas and elicit issues	(Senft & Gallegos, 2009) (Grembergen & Haes, 2009) (Davis, Schiller, & Wheler, 2011), (Davis, Schiller, & Wheler, 2011) (ISO 19011, 2002) (ISO 19011, 2002)
	Audit findings analysis and recommendations elaboration	Analysis of collected information and proposal of recommendations and action plans	(Senft & Gallegos, 2009) (Grembergen & Haes, 2009) (Davis, Schiller, & Wheler, 2011), (Davis, Schiller, & Wheler, 2011) (ISO 19011, 2002) (ISO 19011, 2002)
	Closing meeting	Performance of a closing meeting with the audited entity to communicate what is the main findings	(Senft & Gallegos, 2009) (Grembergen & Haes, 2009) (ISO 19011, 2002)
Reporting	Audit report preparation, approval and distribution	Writing of an audit report which document all information about the audit and approval and distribution of the audit report	(Senft & Gallegos, 2009) (Grembergen & Haes, 2009) (Davis, Schiller, & Wheler, 2011), (Davis, Schiller, & Wheler, 2011) (ISO 19011, 2002) (ISO 19011, 2002)

As we see, the table provides a list of sub-phases and its description. To order these sub-phases we related each one of them to one of the four phases which we describe in Section 3.6.

4.2 IT Audit Roles

The same analyze of the most known frameworks of the area as well as some of the most relevant literature was performed to elicit the main roles of IT AM process. The audit roles as well as the references from where we elicit them are listed in Table 5.

Table 5. IT AM Roles

Role	Reference
Audit Manager	(Senft & Gallegos, 2009) (ISO 19011, 2002) (Tarantino, 2009) (De Haes & Grembergen, 2008) (Steinberg, 2011) (Thomson Reuters, 2011) (Davis, Schiller, & Wheler, 2011) (IT Governance Institute, 2007)
Audit Team	(Senft & Gallegos, 2009) (ISO 19011, 2002) (De Haes & Grembergen, 2008) (Grembergen & Haes, 2009) (Davis, Schiller, & Wheler, 2011) (Davis, Schiller, & Wheler, 2011)
Audited Entity	(Tarantino, 2009) (De Haes & Grembergen, 2008) (Thomson Reuters, 2011) (Grembergen & Haes, 2009)

We just elicited the essential roles which have associated a high number of references. So, we rejected all the roles that just have a low number of references associated.

4.3 IT Audit Activities

With a more deep analysis of the main literature and frameworks of the area, we identified what we consider to be the main activities for IT AM that we list in Table 6 as well as the correspondent references. Since there are a high number of activities (54), here we just provide an example of them. The complete table can be seen in Appendix A.

Table 6. IT AM Activities and Responsibilities

Responsibility/ Activities	References
Periodically conduct internal audits to verify anyone follow relevant guidelines for professional behavior, and process compliance	(ISO 38500, 2008) (Taylor, Iqbal, & Nieves, 2007) (The Institute of Internal Auditors, 2010)
Obtain assurance of compliance and adherence to all internal policies derived from obligations	(COBIT 4.1 Framework, 2007) (The Institute of Internal Auditors, 2010)
Audit must contribute to the improvement of risk management processes in the firm	(Tarantino, 2009) (Davis, Schiller, & Wheler, 2011) (The Institute of Internal Auditors, 2010)
Plan and agree audit requirements	(ISO 27001, 2005) (Senft & Gallegos, 2009) (Davis, Schiller, & Wheler, 2011) (ISO 19011, 2002) (The Institute of Internal Auditors, 2010)
Plan and agree audit activities	(ISO 27001, 2005) (The Institute of Internal Auditors, 2010)
Write an audit plan which must describe the objectives of an audit	(ISO 19011, 2002) (Senft & Gallegos, 2009) (Tarantino, 2009) (Thomson Reuters, 2011) (Davis, Schiller, & Wheler, 2011)
Write an audit plan which must describe the scope of an audit which describes the extent and boundaries of the audit, such as physical locations, organizational units, activities and processes to be audited	(ISO 19011, 2002) (Senft & Gallegos, 2009) (Tarantino, 2009) (Thomson Reuters, 2011) (Davis, Schiller, & Wheler, 2011)
Assign tasks to each team member accordingly with specific processes, functions, sites, areas or activities.	(ISO 19011, 2002) (Senft & Gallegos, 2009) (Grembergen & Haes, 2009) (Davis, Schiller, & Wheler, 2011) (The Institute of Internal Auditors, 2010)
Raise evidences using methods such as interviews, observation of activities and review of documents and elicit issues associated with them	(ISO 19011, 2002) (Senft & Gallegos, 2009) (Grembergen & Haes, 2009) (Davis, Schiller, & Wheler, 2011)
Perform a close meeting to present the audit findings and main conclusion to audited entity	(ISO 19011, 2002) (Senft & Gallegos, 2009) (Grembergen & Haes, 2009) (Thomson Reuters, 2011) (Davis, Schiller, & Wheler, 2011) (The Institute of Internal Auditors, 2010)

As the table shows, for each activity we provide more than one reference to have a strongly justification for each one of them. In the complete table (Appendix A) there are some exceptions to this rule, but after some analysis we understood that those activities should be considered.

4.4 IT Audit Management Process in BPMN

After the definition of our constructs artefacts (IT audit phases, roles and activities), we are able to design the IT AM process. Before we provide the BMPN diagrams we need to organize all the constructs. So, we analyse tables 4, 5 and 6 in order to relate them and provide a complete support to the BPMN's design. In Table 7 we provide the relationships between the referred tables. Note that we join identical activities from Table 6 (more specifically the Appendix A table) in order to reduce the complexity of the Table 7.

Table 7. IT AM Phases, Sub-Phases, Activities and Roles

Phases	Sub-phases	Responsibility/ Activities	Roles
Planning	Establish audit objectives	Plan and agree audit requirements	Audit Manager
		Write an audit plan which must describe the objectives	Audit Manager
	Establish audit scope and schedule	Determine the feasibility of the audit accordingly with the existent time and resources	Audit Manager
		Schedule audit and include this information in the audit plan document	Audit Manager
		Write an audit plan which must describe the scope of an audit which describes the extent and boundaries of the audit, such as physical locations, organizational units, activities and processes to be audited	Audit Manager
Preparation	Audit team selection	Perform team selection	Audit Manager
		Take into account the audit objectives, scope, criteria and estimated duration of the audit in the allocation of resources	Audit Manager
		The allocation of audit team should have in account the knowledge and competences of the auditors and their roles and responsibilities should be assigned accordingly with this knowledge	Audit Manager
		The allocation of audit team should have in account budget associated with the audit	Audit Team
		Appoint the audit team leader	Audit Team
	Obtain preliminary background of audited areas	Gain preliminary understanding about the audited areas	Audit Team
		Perform documents and information assess about relevant aspects of the audited entity	Audit Team
		Review the information relevant to audit assignments	Audit Team
	Define procedures	Plan and agree audit activities	Audit Team
		Establish the roles and responsibilities of the audit team members accordingly with the needed procedures to perform the audit	Audit Team
		Establish audit procedures	Audit Team
		Allocate resources to established audit procedures	Audit Team
		Automate audit procedures when possible	Audit Team
		Establish an audit criteria which are used as a reference against which conformity is determined	Audit Team
		Assign tasks to each team member accordingly with specific processes, functions, sites, areas or activities.	Audit Team

	Audit support documents preparation	Auditor should plan the application of audit techniques useful in a specific audit	Audit Team
		If needed, develop support documents which must be used to assess audit criteria compliance	Audit Team
		Prepare support documents such as checklists and audit sampling plans, and forms for recording information	Audit Team
Execution	Kick-off meeting	Perform a kick-off meeting so that audited entity know all the details behind audit	Audit Team, Audited Entity
		Perform an initial contact with the audited entity to explain the objectives, main procedures, to establish communication channels and request access to the needed information	Audit Team, Audited Entity
	Collection of evidences and issues	Raise evidences using methods such as interviews, observation of activities and review of documents and elicit issues associated with them	Audit Team, Audited Entity
		Perform automated tests when applicable and collect evidences to determine if requirements are being followed	Audit Team, Audited Entity
		Use SI audit tools when possible, to prevent any possible misuse or compromise	Audit Team, Audited Entity
	Audit findings analysis and recommendations elaboration	Evaluate evidences against the audit criteria to generate the audit findings	Audit Team
		Associate evidences to all audit findings	Audit Team
		Analyze all findings in an objective way, to assess if audit criteria is reached	Audit Team
		Develop a list of feasible recommendations accordingly with audit findings	Audit Team
		Develop a list of proposed action plans accordingly with audit findings	Audit Team
	Close meeting	Perform a close meeting to present the audit findings and main conclusion to audited entity	Audit Team, Audited Entity
		Perform a close meeting to discuss and explain the recommendations and action plans to audited entity	Audit Team, Audited Entity
Reporting	Audit report preparation, approval and distribution	Write an audit report that must include: audit objectives, audit scope, audited entity, audit team description, identification of the organizational and functional units or processes audited and the time period covered, dates and places where audit occurred, audit criteria's, findings and conclusions	Audit Team
		Ensure that audit report is reviewed, approved, and distributed to interested entities	Audit Team, Audit Manager
		Ensure review and approval of audit report, and ensure it distribution to the audit interested parties	Audit Team, Audit Manager
		Report to interested parts, the overall achievements of the audit	Audit Team, Audit Manager

As we see, now we have the basis for our process design since Table 7 includes a complete decomposition of the process. We have IT AM phases which is decomposed in sub-phases that by his side is decomposed in activities. Associated with each activity there are the roles that perform them.

Now, based in all above constructs, we present the reached IT AM process (Figure 4 to 7) which is composed by several sub-processes that will not be detailed in this section given to space limitations (see Appendix B to observe the complete process). Also due to these limitations, since internal and external audits are very similar, we only include the representation of the internal audit process BPMN. In fact, external audits are more complex, however, the surplus tasks of external audits are not crucial the design of a generic process (Rosário, Pereira, & Mira da Silva, 2012).

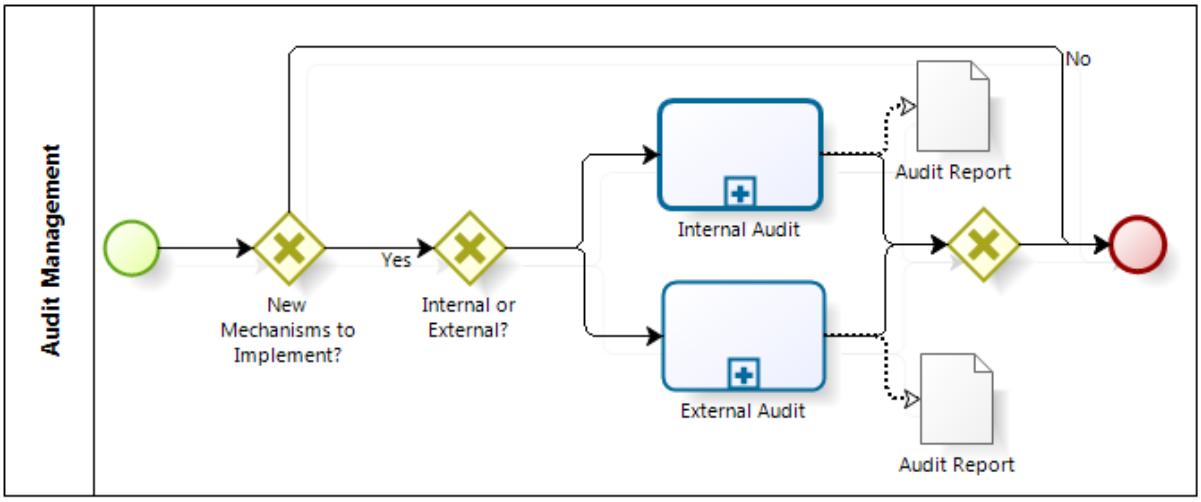

Figure 4. IT Audit Management Process

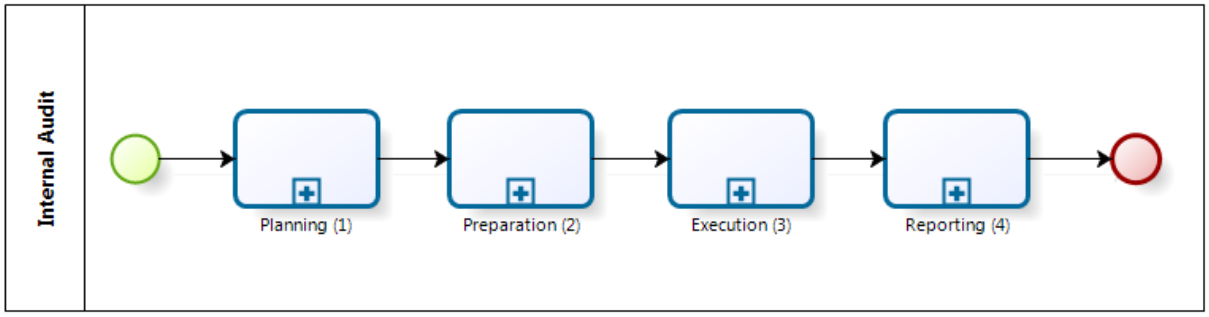

Figure 5. Internal Audit

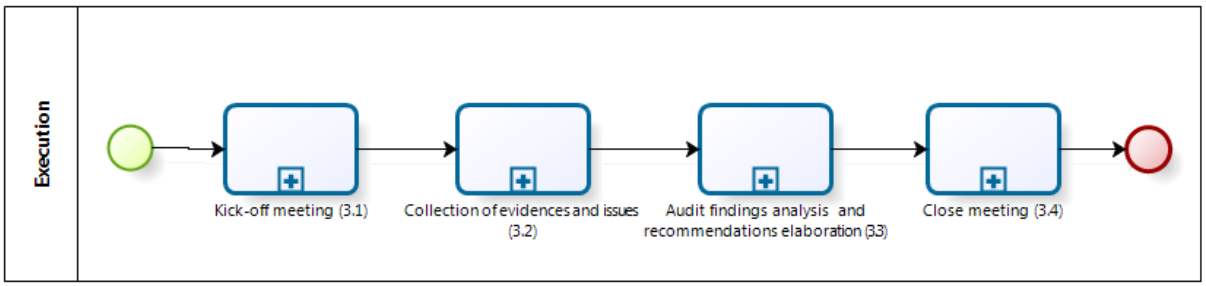

Figure 6. Execution

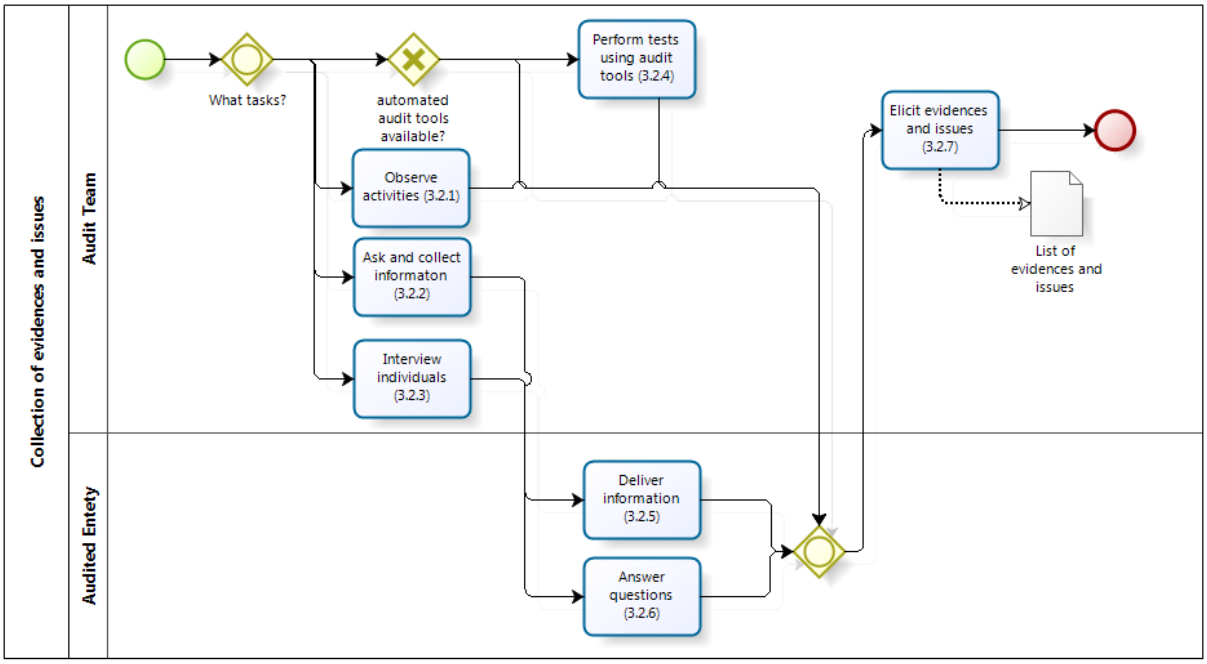

Figure 7. Collection of Evidences and Issues

Figures 4 to 7 shows examples of the proposed process. In figure 4 we demonstrate that it is crucial to have separate processes for internal and external audits. Then we focus on internal audit, providing the sub-processes that constitute it (Figure 5). It is important to understand that these sub-processes are the Table 7 first column). Then, these sub-processes are decomposed in others. In Figure 6 we provide an example of “Execution” which has four sub-processes associate. These sub-processes are the second row of Table 7. At last with more decomposition we obtain the atomic tasks which correspond to the activities in Table 7 third row. In Figure 7 we provide an example of “Collection of Evidences and Issues” sub-process decomposition. Also, the roles of Table 7 last column originate the actors of the process.

4.5 IT Audit Management Information Architecture

Nowadays, organizations perceive the importance of linking business architecture to IA (Kamath, 2011). With this linkage, it is possible to manage the changes needed by the business and maximize the benefits from the IT investments (Kamath, 2011). However, the current ad-hoc IA in place within many organizations cannot meet an organization’s future needs because it has an incoherent framework, incompatibilities, missing elements, few and poorly understood standards, low quality and unnecessary duplications (Watson, 2000).

Given such facts, we decided to develop the IA of IT AM since it allows organizations to better manage their audit related information.

4.5.1 Informational Entities

The entities represent business objects that can be seen as information or concepts that are necessary to support the business. The majority of entities are elicited from the constructs of Sections 4.1, 4.2 and 4.3.

Informational entities are the basis for modelling the IA since they represent information that is manipulated in processes. So, to provide a coherent IA we need to list all the entities elicited and provide a complete description. In Table 8 we can found this information.

Table 8. Informational Entities

Entities	Identifier	Description
Objectives	Objectives Description	Describe the objectives of an audit
Scope	Scope Description	Describe the scope of an audit such as physical locations, organizational units, activities and processes to be audited
Initial Date	Audit ID	Indicates the date in which audit will begin
Audit Plan	Audit ID	Document which contains all the details about audit objectives and scope
Finish Date	Audit ID	Indicates the expected date in which audit will be concluded. It is a derivate entity that is calculated using the initial date and duration entities
Duration	Audit ID	Indicates the expected duration of the audit
Audit Budget	Audit ID	Represents the amount available for carrying out the audit
Audit Team	List of Auditors Identification	Describe all the audit team members, including their knowledge, competences, and also the remuneration associated with each one
Audited Entity Information	Entity Name (Department, etc...)	Represents all the information about the audited entity (a department for example) which is relevant to audit execution
Audit Procedures	Procedure ID	Describe all the actions necessary to perform the audit
Audit Criteria	Name	Represents the audit criteria which is used as a reference against which conformity is determined (e.g. a security checklist that needs to be verified in the audit)
Support Documents	Type + Name	Documents which provide support in the execution of an audit such as checklists and audit sampling plans, and forms for recording information
Communication Channels	Name	Represent the communication channels that audit team and other roles formally establish to perform the audit (used in interactions between all actors)
Meeting Act	Name + Date	Document that reports what has been talked in a meeting
Evidences	Type + Name	Represents all the information that can be used to prove some finding in an audit execution
Issues	Issue ID	Represents all the potential problems founded in an audit execution
Findings	Finding ID	Represents all the information produced when audit team evaluate evidences against the audit criteria
Recommendations	Recommendation ID	Represents the recommendations given by the audit team accordingly with the elicit findings
Action Plans	Action Plan ID	Represents a set of steps that should be taken to implement recommendations
Audit Report	Name + Date	Document that provides all the information about an audit (aggregates other information entities)

The table also shows the identifiers of each entity. In this attribute it is necessary to clarify some decisions. The entities that are specific of an audit (audit plan, audit budget, etc.) can be represented by the same identifier. So we choose to attribute the audit ID to identify all these entities. This is possible because we have a relation of 1:1 between the audit and the entities.

By other side, there are entities that can belong to various audits. In this case they need a unique identifier. It is the case of audit team. A team is a set of auditors which also can compose the team in other audits. In this case, this team identifier is associated with various audits.

There is another possible situation. For example, an organization should document the procedures from all audits. When a new audit is prepared, auditors must read this information since it provides a good basis. However, the procedures can be insufficient to perform that specific audit. So, auditors need to complete the available procedures.

4.5.2 Information Structure Viewpoint

The information structure viewpoint shows the structure of the information used in the organization or in a specific business process or application (Lankhorst, 2009). Figure 8 shows the viewpoint.

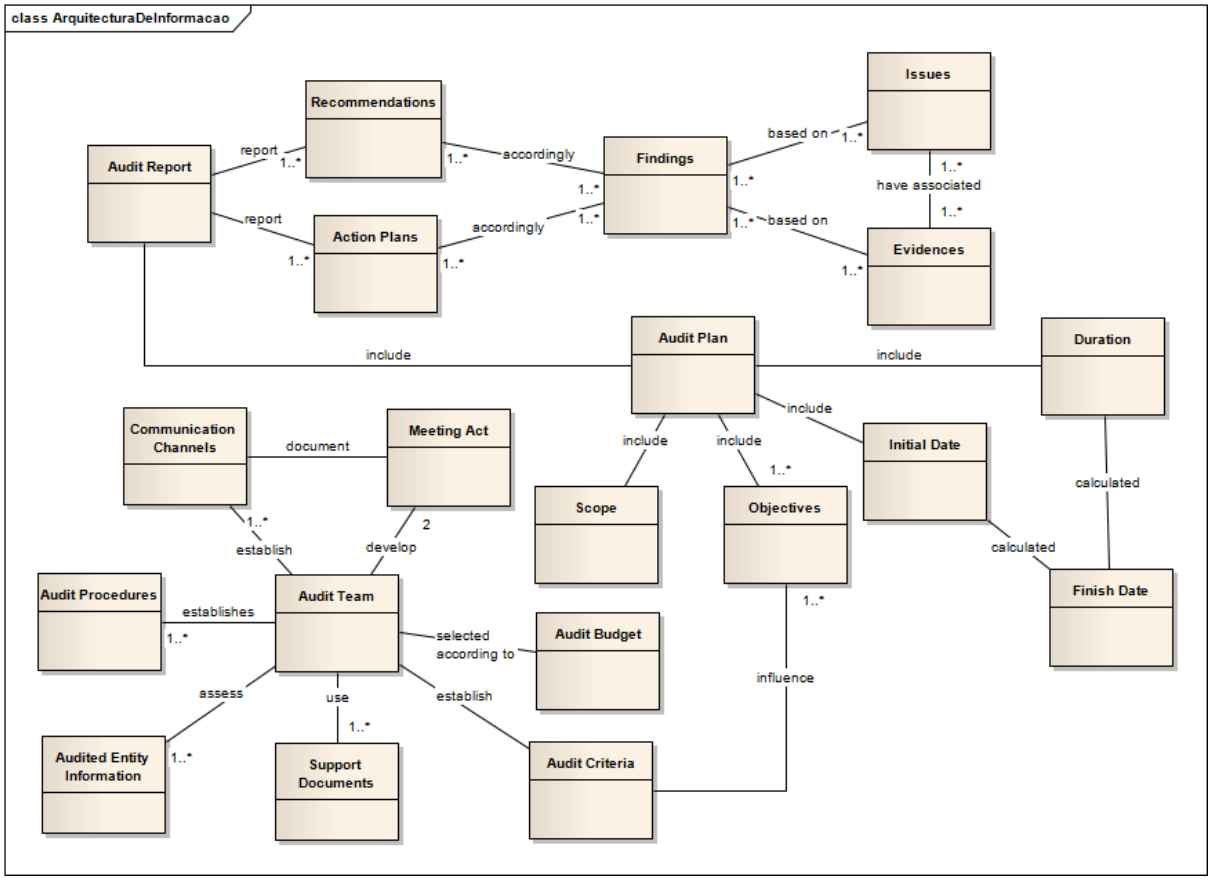

Figure 8. Information Structure Viewpoint

The model objects are those that we provide in Table 8. We represent all the entities and the relations between them including the derivate entities. We don't represent the identifier to maintain the simplicity of the Figure but they can be observed in Table 8.

4.6 IT Audit Management Information Systems Architecture

Information systems[5] architecture focuses on identifying and defining the applications and data considerations defining views that relate to information, knowledge, application services, and others. In our work, we have interests in relate the information entities with the processes that forming the IT AM process to elicit the applications necessary to implement the process in an organization.

So, we began this section by provide a CRUD matrix to explicit the relations between the sub-processes of IT AM process and the IT AM Information architecture entities. Also, the CRUD matrix analyzes allows to elicit the applications (information systems) needed to perform an audit using our models and the relationships between those applications. This matrix was built in order to identify clusters that represent application solutions. The relation between sub-processes and information entities provides a more structured approach to the identification of application components needed to support the IT AM process.

Then, to better visualize the cooperation between the various applications we use the application cooperation viewpoint and, finally, we use application structure viewpoint to better show the relation between applications and the information that each one manipulates.

4.6.1 CRUD Matrix

In order to define consistently the necessary applications to support the processes, we present the CRUD matrix (Figure 9) that relates IT AM sub-processes with informational entities defined in the IA in Section 4.5 (see Appendix C to observe the initial matrix without the clustering analysis). In the matrix we just represent the sub-processes that is composed by atomic tasks (don't include any sub-processes). Due to our process decomposition, the other sub-processes have not atomic tasks. So, we guarantee that any relevant row or column is missing.

[5] In Archimate applications and informations systems represent the same concept. So, as before stated, we use both to express the same idea

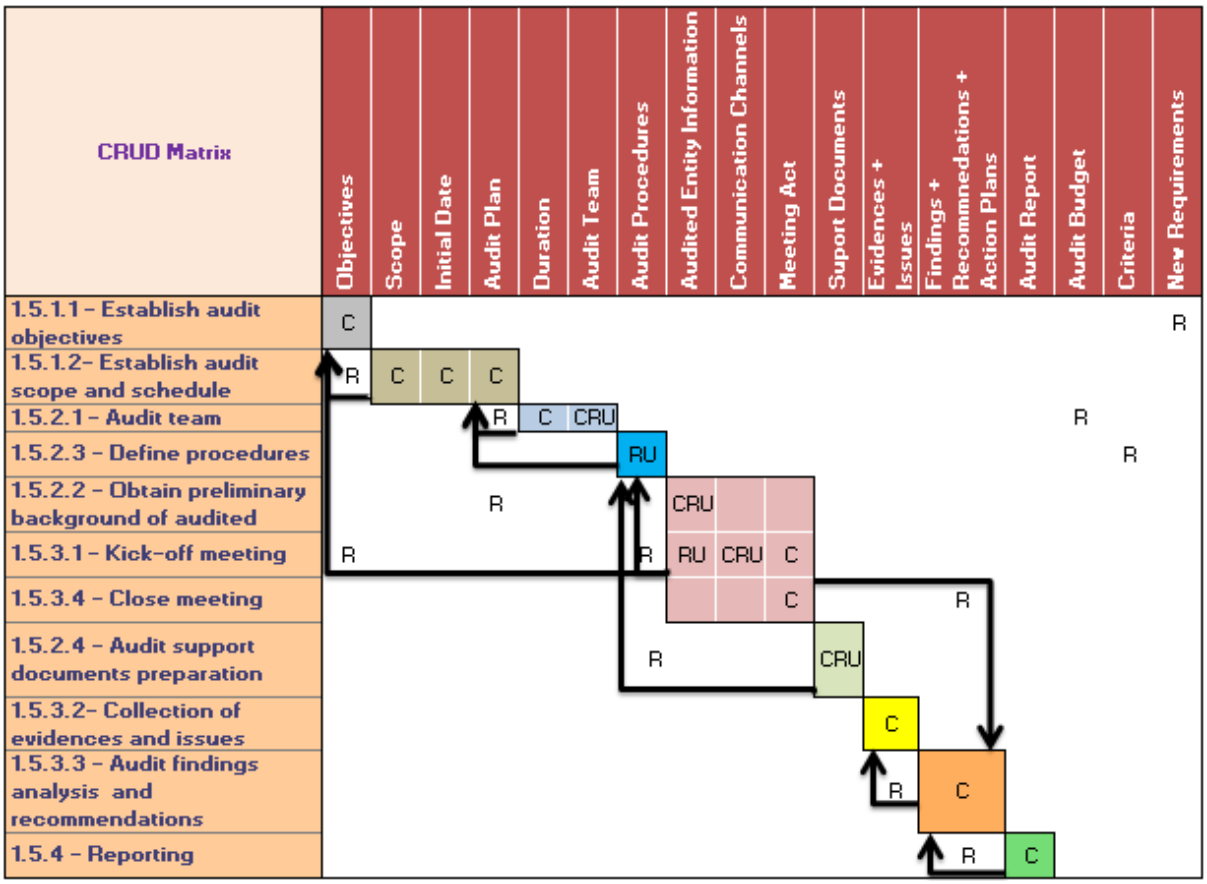

Figure 9. CRUD Matrix

In the CRUD Matrix we don't represent the derived entities (see section 4.5.1) since they are calculated using other entities.

To complete the description made we also propose a name for each application (Figure 10). The chosen names are representative of the information manipulated by them. We use these names in Section 4.6.2 and 4.6.3 models.

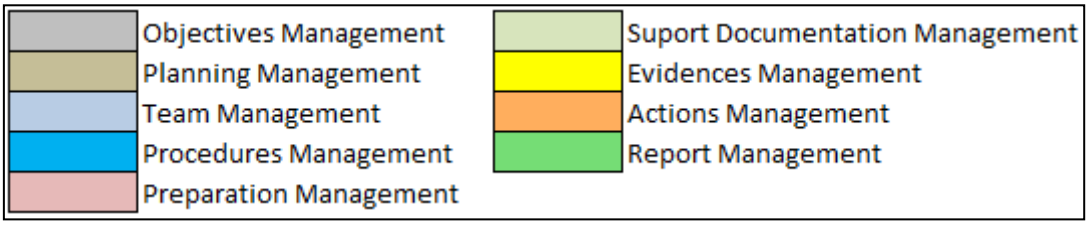

Figure 10. Application Components

The integration between applications was represented in the form of arrows in Figure 9, specifying the necessary accesses between applications. These integrations will be better justified in the description of the application behavior viewpoints.

4.6.2 Application Cooperation Viewpoint

The application cooperation viewpoint shows the relations between application components. It describes the dependencies in terms of the information flows between them, or the services they offer and use (Lankhorst, 2009). The viewpoint can be seen in Figure 11.

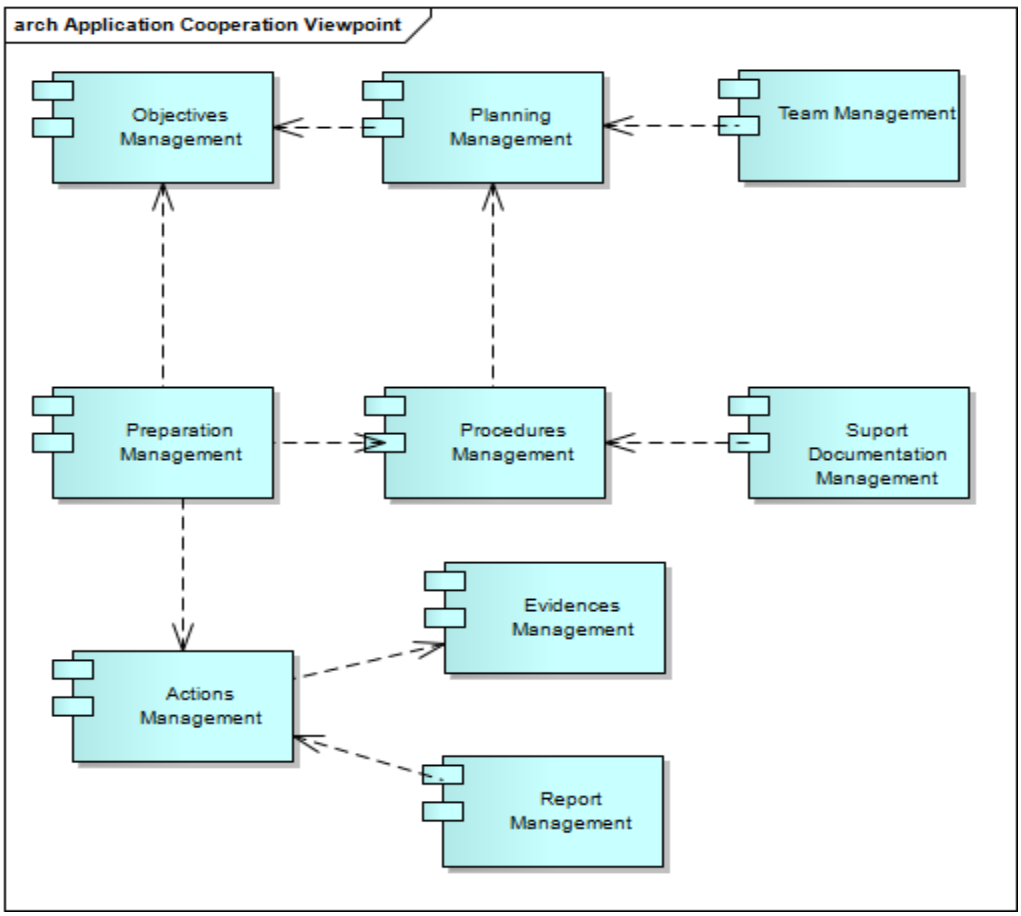

Figure 11. Application Cooperation Viewpoint

As stated in the description of each module, there are some dependencies between application components. In this viewpoint those dependencies are more simple to ascertain.

4.6.3 Application Structure Viewpoint

The application structure viewpoint shows the structure of one or more application components. This viewpoint is useful in designing or understanding the main structure of applications and the associated information. It describes the structure of the applications through the sharing of information. Figure 12 shows the viewpoint.

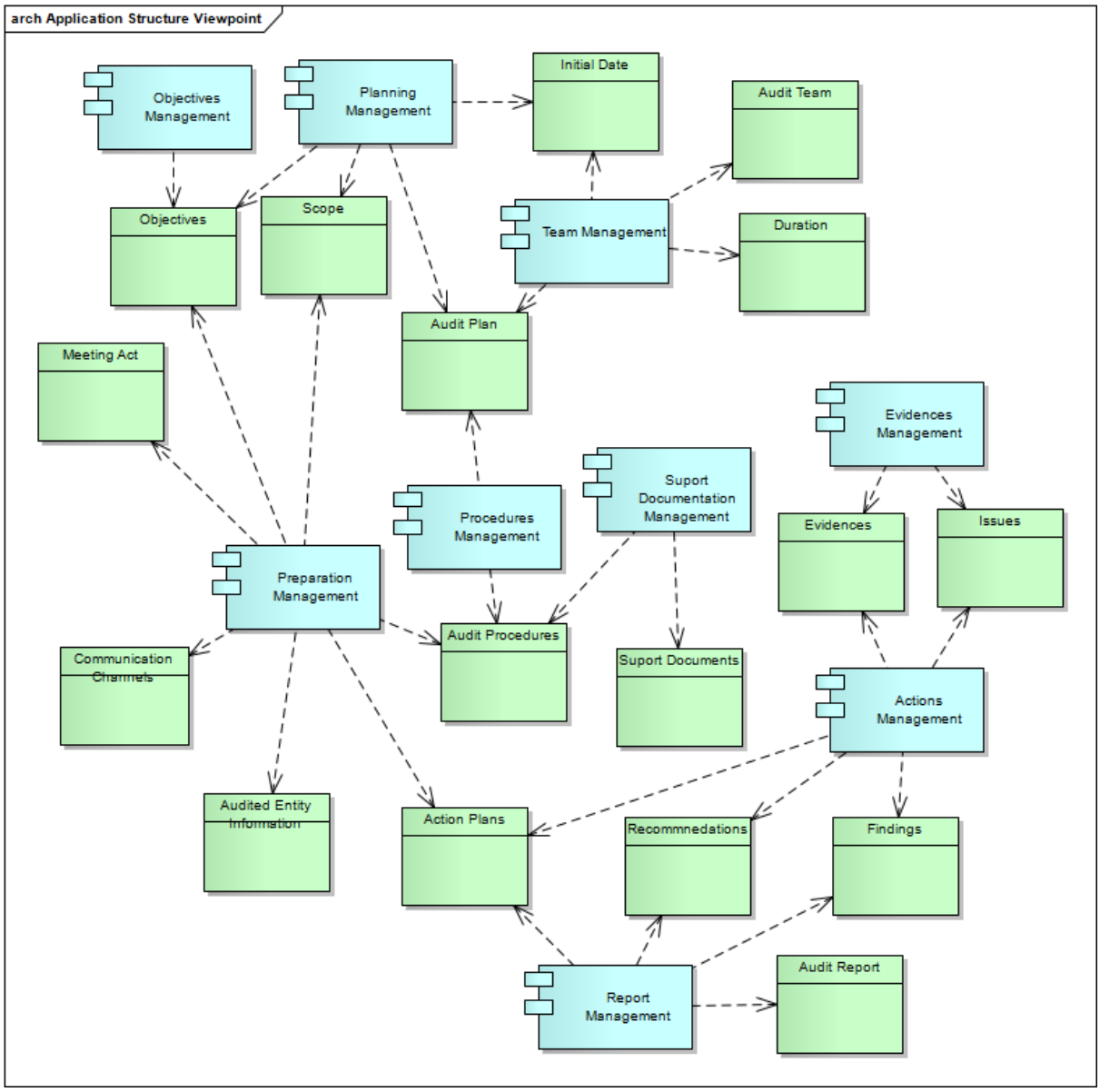

Figure 12. Application Structure Viewpoint

The viewpoint describes the structure of the applications through the sharing of information. We can observe the usage of mutual information between the application components which provides a better representation of the relations between them.

4.7 Conclusion

In this section we began by describe the constructs that supported our proposal (Sections 4.1, 4.2 and 4.3). Then, using these constructs we propose our models which include the IT AM process (Section 4.4), IT AM information Architecture (Section 4.5), and IT AM IS architecture (Section 4.6) with the particularity that the last model use the other two as his constructs. The proposed models should be used by organizations to perform their audits, ensuring that the process is based in a set of

best practices. In spite of the models are the basis for the implementation, organizations also could consult the constructs since they can show information in other perspective.

Audit departments must to perform the described IT AM process tasks in the suggested order and ensure that all the manipulated information is that present in IT AM information architecture. To understand the informational entity details, audit departments must consult Table 8. Then, to better realize their relations they must to consult Figure 8. The IT AM IS architecture ensure that all IT audit applications support the process in an efficient way. Each application support one or more sub-processes and audit departments can use the CRUD matrix (Figure 9) to have a general perspective of the informational entities, processes, and applications that respectively manipulate and support them. Then, to better understand the accesses made between applications Figure 11 should be consulted. Lastly, Figure 12 provides a more easy way to understand the informations accesses made by the applications.

Chapter 5

Evaluation

This chapter describes the evaluation phase of design science research (Section 2). The evaluation of our proposal is based on four parts which are complementary. In this way, we can better measure the quality of our models. The four parts of evaluation are:

- BPMN conversion to YAWL-nets. We use YAWL-nets which provide the same benefits of Petri-nets but without the same conversion limitations.
- Interviews with IT experts to elicit high-level requirements.
- Questionnaires response by IT audit practitioners to elicit detailed requirements.
- Scientific publication that provides feedback and approval by scientific community.

5.1 YAWL-Nets

The modeling language used was BPMN. However, the specification of BPMN notation does not include formal semantics (Takemura T. , 2008; Sun, Song, & Wen, 2008). BPMN does not provide any meta model for abstract syntax nor formal semantics (Takemura, 2008). Given such facts we used YAWL-nets that are based on PN (Sun, Song, & Wen, 2008), to determine if our BPMN model of the IT AM Process was soundness as well as its abstraction.

PN is a formal modeling language that allows processes analyzes (Dijkman, Dumas, & Ouyang, 2007). Indeed, some attempts at defining a formal semantics for a subset of BPMN have been done using PN (Sun, Song, & Wen, 2008; Verbeek & Aalst, 2000). However there are some limitations in converting BPMN to PN: (i) parallel multi-instance activities; (ii) exception handling in the context of sub processes that are executed multiple times concurrently; and (iii) OR-join gateways (Dijkman, Dumas, & Ouyang, 2007).

So, in our evaluation we used YAWL-nets which is a state-based language (Sun, Song, & Wen, 2008) that solves these limitations (Decker, Dijkman, Dumas, & García-Nanuelos, 2008). Since YAWL-nets are based on PN, it also provides a firm basis for the formal analysis of real-world services (Sun, Song, & Wen, 2008).

To evaluate the good construction of our BPMN diagrams, we convert BPMN's into YAWL-nets using a plug-in (BPMN2YAWL) and then we use YAWL editor (Sun, Song, & Wen, 2008) which has a verification tool (Ye, Sun, Wen, & Song, 2008). With the verification tool we can ensure a lot of properties such as the deadlock free, no dead task, proper completion, no OR-join and soundness, etc (Ye, Sun, Wen, & Song, 2008).

In Figures 13 is shown an example of the YAWL-nets created through the conversion of an IT AM Process part (Section 4.4). The totality of YAWL-nets obtained can be seen in Appendix D.

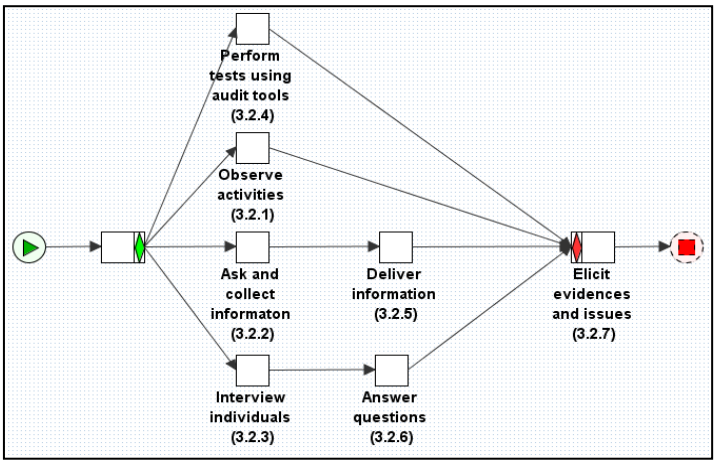

Figure 13. Collection of Evidences and Issues – Yawl Net example

The Yawl-editor didn't find nets problems which give us the certain that our process is well designed.

5.2 Interviews

We have already designed our solution based on the main literature and frameworks of the area which gave us a strong theoretical viewpoint. So, in order to provide some practitioner viewpoint, we evaluated part of our proposal by performing eight interviews at Portuguese organizations. We perform the interviews with long time specialists in the area of IT. With this part of evaluation we intend to obtain a set of essentials business requirements in audit responsibility. The focus is not on the atomic tasks but in high level requirements which is essential to reach audit goals and ensure that business necessities are achieved. Given the objective of this part of evaluation, the respondents don't need to be auditors but experts witch know what is important in audit function to the organization interests. The respondents should provide a set of essential requirements which our models should provide.

We used structured interviews to elicit IT audit requirements from the field, covering a diverse sample of organization types, sizes, and roles. Detailed information about the respondents is provided in Table 9. The respondents have a lot of experience in the area.

Table 9. Respondents Details

Id	Type	Area	Position	Work Experience
1	Telecommunications	Information Systems	Director	Manager of Operations, Data Base Administration and Technical Support from 2002 to 2010
				Sourcing and Staffing Manager since 2010
2	Consultant	IT Governance and Project Management	Senior Project Manager	SI Advisor from 1997 to 2001
				Process Manager from 2001 to 2005
				Practice Manager from 2009 to 2011 in the areas of IT Governance
				Senior Manager from 2009 to 2011 in the areas of IT Governance
3	Banking	Risk Management and IT Quality	Executive Administrator	Director in a IT Consulting firm from 1999 to 2000
				Software Administrator at IT Services from 2000 to 2003
				Administrator at an IT Consulting firm from 2003 to 2006 in the areas of SI Architecture, Risk Management and Processes and IT Quality
4	Banking	Standards and Operations	Executive Coordinator	Executive Coordinator from 1998 to 2012 in the area of Methodologies and Standards, Processes and Procedures, Organizational Good Practices, Control Department and Software Quality
5	Banking	Risk and Compliance	Director	Director at IT Risk and Compliance Department from 2007 to 2012
6	Banking	IT Management	Executive Manager	Software Development Manager from 2000 to 2005
				IS Architectures Manager Project Office Manager from 2008 to 2010
				IT Users Relationship and Logical Architecture Manager from 2010 to 1012
7	Consultant	IT Services Management	CEO	Quality Management in the implementation of systems from 1994 to 1997
				Perform of audits in IT Infrastructures and Systems from 1997 to 2001
				Design and Development of systems compliant with ISO 9001 from 1997 to 2001
				Audit manager in security area in some projects
				Coordinator to Audit and Quality area at *Instituto de Informática* from *Ministério do Trabalho e da Solidariedade Social* (MTSS) from 2001 to 2011
				CEO at an IT Services consulting firm
8	Consultant	IT Governance, EA and Enterprise Content Management	Business Practice Manager	Developer at a consulting firm from 2002 to 2003
				Consultant at a firm from 2002 to 2006
				Senior consultant at a firm from 2006 to 2008
				Product manager from 2009 to 2010 in the area of modeling (BPM) and product quality
				Project Manager from 2008 to 2011 in a consulting firm
				Business Practice Manager since 2011 in a consulting firm

To support the interviews, we designed a questionnaire in order to support and lead the discussion. The questionnaire, which can be seen in Appendix E, is divided into two sections. The first one elicits requirements associated to the relationship of the IT AM. The second section elicits requirements about how to support the IT AM process.

In the interviews, we used open-response questions because of the nature of the information we need to elicit. Complementarily, there are some questions in which respondents needed to give a list of required ideas. Furthermore, clarifications regarding the various concepts used by the respondents were sought during the conversation, so that later these descriptions can be examined and matched to the more standard designations. The interviews were conducted over a one month period. Each session lasted from 30 to 60 minutes and was transcribed into digital data for analysis.

5.2.1 Results Description

With the interviews, we can draw some conclusions that provide insight into the current IT AM process. In Table 10 we describe the raised conclusions and the interviewees that supported them. In the results' descriptions we rejected conclusions that were not pointed by more than one interviewee or ill-founded conclusions by respondents.

Table 10. Conclusions Raised

Nº	Conclusion	Interviewees
1	Audits are carried out mostly in the traditional manner. For example, audits are performed using excel spreadsheets, which are used as checklists.	1, 2, 3, 4, 5, 6, 7, 8
2	Risk and compliance departments should be independent and the audit department should be completely independent. However, it is essential that risk, compliance and audit departments are strongly related.	1, 3, 4, 5, 6
3	Audit is still seen as something negative by audited entities. The perception is that auditors serve only to encounter problems that affect the entities.	1, 3, 4, 5, 6
4	Audit objectives must be established according to the management's needs. When an audit is requested, there are specific needs by the entities who request it. So, the objectives should be established according to them.	1, 2, 3, 4, 5, 7
5	Audit report should include all the findings and recommendations proposed	1, 2, 3, 7
6	All the information needed should be collected, even if that implies to directly interact with the audited entity individuals.	2, 3, 7, 8
7	Related with the above conclusion, audit team members can access all the information needed, and use it as evidence when necessary.	2, 3, 7, 8
8	When a new audit begins, the audit team should assess information about the oldest audits that may help to conduct the new one.	2, 3, 4, 5, 7
9	Internal and external audits have separate processes. Actually, the activities behind both are very similar but in practice, internal audits are less formal, and some activities are not performing as theory suggests.	1, 3, 4, 5, 6
10	Internal audits results are compared to external audits and this is a type of evaluation made by an organization to internal auditors since external audits are seen as an accuracy audit.	1, 3, 6

As we see, the reached conclusions are high level detailed since the respondents are not auditors.

5.2.2 Requirements Elicited

We are then able to elicit the main requirements of the IT AM process based on practitioner's viewpoint. In Table 11 we can see a summary of the elicit requirements.

Table 11. Requirements Elicit

Req. N[a]	Conclusion	Elicit Requirement
1	1	Ensure a good selection of procedures necessary to perform audits.
2	2	Continuously request independent audits. Ensure a relationship between audit and risk management: audit needs to re-assess risks and test internal controls associated to them; an audit can find new threats that must be analyzed by risk management.
3	3	Ensure an efficient way to present audit results, i.e., reports should be prepared with accurate results. Even pointing out problems, auditors should propose recommendations and action plans in the audit report to help improve the audited entity.
	4	
	5	
4	6	During audit, the team must interview individuals and access information (risk reports, old audit reports, etc...). Audit teams can collect all the needed information and use it as evidence.
	7	
	8	
5	9	Design a separate process to internal audit.
	10	

These requirements are the basis for a good IT AM. In other words, IT AM process activities must ensure that these requirements are provided. If indeed they are provided, the process can ensure the needs of real organizations.

Looking at our proposal, we can note that the designed BPMN tasks ensure that these requirements are included in the proposed IT AM Process (Table 12).

Table 12. Mapping Between Elicit Requirements and BPMN Tasks

Concl.	Sub-Processes	Tasks
1	Establish audit objectives	Establish audit objectives
	Establish audit scope and schedule	Understand time needed to perform audit Understand resources needed to perform audit Define audit scope
	Obtain preliminary background of audited areas	Assess audited entity information Assess information about audit assignments
	Define procedures	Define audit criteria Plan audit procedures Understand if some procedures can be automatized Understand if some procedures can be automatized
	Audit support documents preparation	Understand the needed audit techniques Develop new support documents Choose support documents
2	Audit Management	-

	Establish audit objectives	Assess new requirements Analyze requirements
	Reporting	Write a detailed description of findings Write a detailed description of issues
3	Reporting	Write a detailed description of Recommendations Write a detailed description of proposed Action plans
4	Obtain preliminary background of audited areas	All
	Collection of evidences and issues	All
	Audit findings analysis and recommendations elaboration	All
5	Audit Management	-

Table 12 shows the tasks and sub-processes that guarantee the achievement of elicited conclusions. As a result, we can argue that all the conclusions are reached.

5.3 Questionnaires

In this part of evaluation we promote questionnaires with IT auditors. These questionnaires have the purpose of understand with practitioners agree with the created models: IT AM process, IT AM information and IS architectures. The focus is on the atomic tasks of the process, information and applications. So, the respondents need to be auditors which know how to perform an audit. Accordingly, we promote the questionnaires with five IT auditors with at least six months of intense activity in this function. With their experience they have to analyze our work and classify it accordingly with some factors provide by the data model quality framework provides by Moody and Shanks (Moody & Shanks, 2003). As opposed to Section 5.2, in this section we don't need to provide detail information about the practitioners because we just want to guarantee that they are professionals in the IT audit function. So, the only information that we ask to them is the actual function and the time they perform it.

The factors proposed in the Moody and Shanks framework are:

- **Completeness**. Completeness refers to whether the model contains all user requirements.
- **Integrity**. Integrity definition of business rules or constraints from the user requirements.
- **Flexibility**. Flexibility is defined as the ease with which the model can reflect changes in requirements without changing the model itself.
- **Understandability**. Understandability is defined as the ease with which the concepts and structures in the model can be understood;

- **Correctness**. Correctness is defined as whether the model conforms to the rules of the modeling technique (i.e. whether it is a valid model). This includes diagramming conventions, naming rules, definition rules, rules of composition and normalization.

- **Simplicity**. Simplicity means that the model contains the minimum possible entities and relationships.

- **Integration**. Integration is defined as the consistency of the model with the rest of the organization.

- **Implementability**. Implementability is defined as the ease with which the model can be implemented within the time, budget and technology constraints of the project.

The questionnaire, which can be seen in Appendix F, is divided into two sections. The first one analyzes the IT AM process. The second section analyzes the information and information system architecture.
In the questionnaires, questions have the intent to assess if each factor is reached. Complementarily, there is an open question in which respondents should give provide a complementary commentary about our work. This intends to elicit other details not reached with the previous questions. Each session lasted about 30 minutes and was performed in digital data for analysis.

Next, we discuss each one of the factors proposed in the Moody and Shanks framework and explain how our proposal reaches them. We also explain the changes made in our proposal in order to solve some problems that practitioners founded. To begin our analysis we summarize the main conclusions provide by practitioners in Table 13. We describe the conclusions (column 2), the Moody & Shanks factor to which it refers (column 3) to and the model in analysis (column 4).

Table 13. Practitioners Main Conclusions

Nº	Conclusion	Factor	Model
1	It is complete but to implement, organizations need to complement some parts of the process accordingly with the type of audit. For example, audits in the security domain need to complete it with specific procedures. The process doesn't clearly demonstrate that the Audit Report is delivery to the various stakeholders.	Compl.	IT AM Process (1)
2	The information listed is sufficient to perform the audit. "Evidences" entity can be any type of informations, so represent them as a unique entity can be an abuse.	Compl.	IT AM Information Architecture (2)
3	It can be necessary to access other applications that don't belong to audit department. Also, some entities listed such as "Evidences" entity usually are collected using other systems, so it is necessary to be careful when it is said that evidences are created in audit process.	Compl.	IT AM IS Architecture (3)
4	In the point of view of audit stakeholders, the proposed process can be changed enough without losing the integrity. It is important to have	Integ.	1

	mechanisms to support an adaption of the process by organizations.		
5	The information provided allows good integrity.	Integ.	2
6	Most of the reached applications manipulate few entities and processes. So, it is easier to maintain integrity. The bigger clusters (applications) are more critically since a change in one entity manipulated by them can compromise integrity.	Integ.	3
7	The proposed process is flexible enough since it is sufficient generic.	Flexib.	1
8	The information is generic enough and changes are easy to make.	Flexib.	2
9	As stated in point 6, there are a necessity of perform reads in other domains applications which influences negatively the model flexibility. Also, there is a high dependency between applications.	Flexib.	3
10	The visualization of the BPMN can be insufficient to understand the entire process since the meaning of some concepts (for example, “Evidences”) is not trivial. Also, the meaning of some tasks can be not easy to understand by just observing its name.	Under.	1
11	The descriptions ensure a good understand ability.	Under.	2
12	The applications names in some cases are not clearly enough. A good idea to improve these names is to observe the processes that one cluster (application) contains and give a name based on it.	Under.	3
13	The process is correct. Sometimes there are some details which are not present in the process. For example, some parts of internal audits are performed by external entities. This type of situations is not represented.	Correc.	1
14	All information is correct. It can be questionable if some information should be an informational entity such as “Initial Date”.	Correc.	2
15	The systems achieved seem correct.	Correc.	3
16	The process is easy to understand. Some sub-processes and tasks are too large which decreases their simplicity.	Simpl.	1
17	All entities have perceptible names. But the description is crucial to understand some of them in the point of view of a non-expert.	Simpl.	2
18	The systems achieved and they relations are simple to understand.	Simpl.	3
19	The process guarantee integrity but it is necessary to make a reservation: the designed BPMN don’t provide information about the main activities of audited entities. In the conduction of an audit it is necessary to understand that audited entity daily activities are harmed by auditors work in order to minimize them.	Integ.	1
20	All the information described can be used by all kind of organizations without interfering with other informations. The collect of evidences in a department can bring some difficulties due to them confidentiality.	Integ.	2
21	The proposed applications seem good. However it has some limitations in the way organizations can adapt the model. There are readings to applications that don’t belong to audit scope. So, organizations need to guarantee that they have that entities and applications to manage them.	Integ.	3
22	It is possible to implement the process since it is sufficiently generic to be adapted. In some cases, it can be needed a complementation with more procedures associated with some kind of audits. Also, some organizations, due to its size, can implement just part of the process.	Impl.	1
23	All the information described can be used by all kind of organizations.	Impl.	2
24	The systems achieved and they relations are simple to but it depends of the capacity of organization to develop them.	Impl.	3

Now we can discuss some of these conclusions to understand what are the improvements made. The next sections do it for each one of the factors and for all conclusions.

5.3.1 Completeness

Conclusion 1 – The first issue is solved throw the definition of procedures in each audit. In the sub-process “Preparation” we have a task call “Define procedures” that intend to solve this problem. We have this more generic task that ensures an adaption of audit procedures accordingly with the type of audit.

The second issue is pertinent but we don’t solve it directly. In the sub-process “Reporting” we provide a task called “Distribute report” which in spite of being more generic, indirectly guarantees that all the stakeholders receive the audit report.

Conclusion 2 – Since we intend to provide a general and adaptable process, we cannot decompose the entity evidences. It is impossible to represent all the possible information that can be used as evidence, so, we maintain the entity evidence. This decision don’t influence the quality of models since in the case of having multiple types of information, they have the same relations and purpose of the “Evidences” entity.

Conclusion 3 – The access to applications of other domains is already visible in the CRUD matrix (Figure 9) when we have columns only with reads (R). We assume that the entity “Evidences” is created in this process because we need to save some information about it. The saved information can be just a link or a document name.

5.3.2 Integrity

4 – As described in conclusion 1 first issue, we include mechanisms to support an implementation sufficiently adaptable such as the “Define procedures” task.

5 – Already good in the practitioners point of view.

6 – Since we have already a high number of clusters (applications of the CRUD matrix) with just a few entities to manipulate, we think that it is no necessary to make any improvement.

5.3.3 Flexibility

7 – Already good in the practitioners point of view.

8 – Already good in the practitioners point of view.

9 – The access of other applications is necessary and indispensable since audit is inserted in compliance domain. Consequently, some compliance related applications must to be access.

5.3.4 Understandability

10 – We propose three models to solve this kind of problems. If someone doesn't understand the meaning of a process detail, it can consult the information or IS architectures to complete their comprehension. Also, if some task name is not enough to understand it meaning, Table 7 should be consulted since it can provide a better and more complete description.

11 – Already good in the practitioners point of view.

12 – As suggested by some practitioners we changed the name of applications (Figure 10). Now the names are based on the sub-processes they contain.

5.3.5 Correctness

13 – Already good in the practitioners point of view. The missing details referred could compromise the process adaptability.

14 – Already good in the practitioners point of view. We decide to maintain entities such as "Initial Date". Despite it represents just a value we need to save this information and so, it is necessary to represent it in our models.

15 – Already good in the practitioners point of view.

5.3.6 Simplicity

16 – We changed some sub-processes and tasks names to make them simpler as suggest by practitioners.

17 – Already good in the practitioners point of view.

18 – Already good in the practitioners point of view.

5.3.7 Integration

19 – Already good in the practitioners point of view. The adaption to audited entity daily activities is impossible to represent since it is never the same.

20 – Already good in the practitioners point of view.

21 – The pointed limitation is already discussed in conclusion 9 from flexibility factor.

5.3.8 Implementability

22 – Already good in the practitioners point of view. The adaption to the type of audit is already solved with the definition of procedures by audit team in the task “Define Procedures”.

23 – Already good in the practitioners point of view.

24 – Already good in the practitioners point of view.

With all these changes we can argue that our proposal models are designed accordingly with the Moody &Shanks framework factors.

5.4 Scientific Publications

During the execution of this thesis, a scientific paper was published in an international conference. The details of the paper and conference name and ERA rating follows:

Formalization of the IT Audit Management Process (Rosário, Pereira, & Mira da Silva, 2012) was published at the Workshop on Models and Model-driven Methods for Service Engineering 2012 (3M4SE) which belongs to the Sixteenth IEEE International EDOC Conference (EDOC 2012) and is a rank B conference.

The paper describes parts from the proposal of this thesis it publication in an international conference brings valuable input for further research, feedback and approval by scientific community.

Chapter 6

Conclusion

With the evaluation of our proposal we can argue that our proposal brings benefits to the IT audit domain. The Yawl-nets conversion ensure the BPMN's good construction. The interviews with IT area experts guarantee that business requirements are achieved by our constructs as demonstrated in Table 12. Then, the questionnaires with IT auditors provide a detailed evaluation of our models which with some small modifications ensure their good quality since the Moody & Shanks factors are reached. Finally, the submission and acceptance of an article allows the approval by scientific community to complement practitioner's approval. Also, the communication of our work is reached with the scientific publication.

Since the evaluation shows the good model construction, we argue that the limitation pointed out by Goeken (Goeken & Alter, 2009) was fulfilled (frameworks lack theoretical foundations). Plus, with the merging of the frameworks in IT AM activities, we argue that the limitation stated by Pereira and Mira da Silva (Pereira & Mira da Silva, 2011) was fulfilled too (frameworks overlap each other). Finally, also the limitations pointed by Rosário, Pereira and Mira da Silva (Rosário, Pereira, & Mira da Silva, 2012) was solved since a complete IT AM process based on main frameworks and literature was achieved.

The acceptance of our models by practitioners and scientific community shows that it is possible to design a complete, general and adaptable IT AM process using the best practices provides by the most accepted IT frameworks and literature.

6.1 Contributions

Our work aims to contribute to the IT AM process design, so that it is possible to have a formal way of performing audits. Knowing that the formalization of audit tasks is a difficult goal to achieve, we believe that our work is another step to turn it a reality. The main contributes of this research are:

1. The formalization of the IT AM Process, useful and adaptable to all type of organizations, based on both theoretical and practitioners' viewpoints;

2. The design of a complete process where all the processes, tasks, roles and data represented are pointed by IT best practices frameworks or by the most relevant literature.

3. The achievement of an IT AM process which is designed accordingly with the factors proposed in the Moody and Shanks (Moody & Shanks, 2003) framework.

4. The conduction of a research which is based on the four principles pointed by Osterle et al (Osterle, et al., 2011) for design oriented IS research (see detailed description in Research Methodology – Section 2).

5. We demonstrated that our IT AM Process is formal which proves its strong empirical validation.

With these contributions and the evaluation made we are able to say that our work can help organization to achieve a more efficient way to perform their audits.

6.2 Limitations

Part of our proposal evaluation is based on the elicitation of requirements with IT experts to understand how audit function should influence the business. To achieve better results we can interview a higher number of people so that it is possible to ensure that there is no lack of requirements and to study other types of organizations. Also, practitioner's functions and type of industry where it operates is limited. So, we can improve the results achieved by increase the number of respondents and their characteristics.

The same idea could be apply in the questionnaires part of evaluation. But in this part it is not important to use different types of respondents since we just are interested in IT auditors.

6.3 Lessons Learned

With our work we learn that in spite of the high number of frameworks and literature, organizations still have difficult in implement some procedures crucial to their business. However, combining each one of them it is possible to improve the achieved results since they can provide a complementary contribution. It has the case of our proposal.

We also learn that the contribution of literature (theoretical) and practitioners (practical) is important since they provide a complementary input which allows a better models construction. The practitioners also are important in providing detailed models evaluation.

Finally, we learn that the all set of proposed models provide a better help in the implementation of IT Audit Management since each one of them have some interpretative limitations that are mitigated by the others as we saw in evaluation (Section 5).

6.4 Future Work

In the future, this research can be complete with a more empirical work. Primary we could observe in real organizations if their actual IT AM process is performed as designed here. If not, the observation of real audit activities could give us an idea of how ad-hoc is conducted audits and understand what the differences to our process are. Then, to observe our work in real situations we could implement the proposed IT AM process in order to understand if this implementation is easy to make as our models evaluation seems to demonstrate.

With the new implementation complete we can compare the old and the new process in order to understand the differences and the impact of them. To full evaluate our proposal in real world we need to repeat all this work in various places so that we can observe the effects of implement our proposal in organizations with different sizes, types of industries, etc.

References

Adrian, B., Beres, Y., & Shiu, S. (2008). Using Assurance Models in IT Audit Engagement. *Hewlett-Packard Development Company, L.P.*

Allen, D., & Faff, R. (2012). The Global Financial Crisis - some attributes and responses. *Accounting and Finance 52* (pp. 1–7). Steven Cahan, doi: 10.1111/j.1467-629X.2011.00416.x.

Bace, J., & Rozwell, C. (2006). Understanding the Components of Compliance. Gartner ID:G00137902.

Banca D'Italia. (2007). Supervisory Regulations: The Compliance Function.

Carlin, A., & Gallegos, F. (2007). IT Audit: A Critical Business Process. (pp. 87-89). doi:10.1109/MC.2007.246.

Chen, Z., Yoon, J., Frenz, C. M., & Compres, K. (2011). IT Governance, Compliance and Auditing Curriculum – A Pedagogical Perspective. *IEEE World Congress on Services (SERVICES)* (pp. 414 - 421). Washington DC: IEEE.

COSO. (2004). Enterprise Risk Management. Integrated Framework. www.coso.org.

Davis, C., Schiller, M., & Wheler, K. (2011). *IT Auditing: Using Controls to Protect Information Assets.* McGrawHill.

De Haes, S., & Grembergen, W. (2008). Analysing the Relationship between IT Governance and Business/IT Alignment Maturity. *Proc. of the 41st Hawaii International Conference on System Sciences (HICSS 08)* (pp. 428-428). United States: IEEE, doi: 10.1109/HICS.

Decker, G., & Barros, A. (2007). Interaction Modeling using BPMN. *Proc. of the 2007 international conference on Business process management (BPM'07)* (pp. 208-219). Germany: doi: 10.1007/BPM.2007.22.

Decker, G., Dijkman, R., Dumas, M., & García-Nanuelos, L. (2008). Transforming BPMN Diagrams into YAWL Nets. *Proceedings of the 6th International Conference on Business Process Management (BPM '08).* Berlin: Springer.

Dijkman, R. M., Dumas, M., & Ouyang, C. (2007). Formal Semantics and Analysis of BPMN Process Models using Petri Nets. *Computer and Information Science*, (pp. 1–30).

Godellawatta, G. (2009). Compliance after the global crisis. *Association of Professional Bankers SRI Lanka.*

Goeken, M., & Alter, S. (2009). Towards Conceptual Metamodeling of IT Governance Frameworks Approach – Use – Benefits. *Annual Hawaii International Conference on System Sciences (HICSS).* United States: IEEE.

Grembergen, W. V., & Haes, S. D. (2009). *Enterprise Governance of Information Technology: Achieving Strategic Alignment and Value.* Springer.

Griffin, P. A., & Lont, D. H. (2007). An Analysis of Audit Fees Following the Passage of Sarbanes-Oxley. *Asia-Pacific Journal of Accounting and Economics on Forthcoming (APJAE).* Hong Kong.

Gudivada, V. N., & Nandigam, J. (2009). Corporate Compliance and its Implications to IT Professionals. *International Conference on Information Technology: New Generations, ITNG*, (pp. 725-729). United States.

Hevner, A. R., & March, S. T. (2004). Design Science in Information Systems Research. *Management Information Systems Quarterly 28*, (pp. 75-105).

ISO 19011. (2002). *Guidelines for quality and/or environmental management systems auditing.*

ISO 27001. (2005). *Information technology - Security techniques - Information security management systems - Requirements.*

ISO 38500. (2008). *Corporate governance of information technology.*

IT Governance Institute. (2007). *COBIT 4.1 Framework.*

Kamath, S. (2011). Capabilities and Features Linking Business and Aplications Architecture. *2011 International Conference on Information Science and Applications (ICISA)* (pp. 1 - 7). Republic of Korea: IEEE.

Lankhorst, M. (2009). *Enterprise Architecture at Work - Modelling, Communication and Analysis.* Berlin: Springer.

Lewis, E., & Millar, G. (2008). The Viable Governance Model - A Theoretical Model for the Governance of IT. *International Journal on IT/Business Alignment and Governance.* Big Island, Hawaii.

Little, B. (2007). Whose Data is it Anyway? *Information Professional. Vol. 4, Issue: 3*, (pp. 38-40).

March, S. T., & Smith, G. F. (1995). Design and natural science research on information technology. *Decision Support Systems* , (pp. 251-266).

Marques, A. F., Borges, J. G., Sousa, P., & Pinho, A. M. (2011). An enterprise architecture approach to forest management support systems design: an application to pulpwood supply management in Portugal. *European Journal of Forest Research* (pp. 935-948). Verlag: Springer.

Mcdonough, A., & Sackmann, S. (2009). Compliance and Organization Value: How Markets React to Reported Lapses in Corporate Governance. *Organization Computing CEC '09 IEEE Conference on Commerce* (pp. 239-244). Austria: IEEE Computer Society.

Mcginnis, S. K., Pumphrey, L., Trimmer, K., & Wiggins, C. (2004). Sustaining And Extending Organization Strategy Via Information Technology Governance. *Hawaii International Conference on System Sciences.* Hawaii: IEEE Computer Society.

McNay, H. (2003). Information Architecture - Visual Displays. *Professional Communication Conference (IPCC)* (pp. 21-24). *IEEE International* .

Mendling, J., Dongen, B. F., & Aalst, W. M. (2007). Getting Rid of the OR-Join in Business Process Models. In: 11th IEEE International Enterprise Distributed Object Computing Conference. *11th IEEE International Enterprise Distributed Object Computing Conference* (pp. 3-14). New York: IEEE Press.

Moody, D. L., & Shanks, G. G. (2003). Improving the quality of data models empirical validation of a quality management framework. *Information Systems 28* , 619–650.

Morimoto, S. (2009). Application of COBIT to Security Management in Information Systems Development. *Fourth International Conference on Frontier of Computer Science and Technology (FCST).* China: IEEE.

Nicewicz-Modrzewska, D., & Stolarski, P. (2008). ITIL implementation roadmap based on process governance. *European University of Information Systems (EUNIS).* Denmark.

Osterle, H., Becker, J., Frank, U., Hess, T., Karagiannis, D., Krcmar, H., et al. (2011). Memorandum on design-oriented information systems research. *European Journal of Information Systems (EJIS) 20* , 7 - 10.

Pai, P. F., Hsu, M. F., & Wang, M. C. (2007). Computer-Assisted Audit Techniques based on an Enhanced Rough Set Model. *Sixth International Conference on Networked Computing and Advanced Information Management (NCM)* (pp. 207 – 212). South Korea: IEEE.

Pereira, R., & Mira da Silva, M. (2010). A Maturity Model for Implementing ITIL v3. *6th World Congress on Services (SERVICES-1).* United States: IEEE.

Pereira, R., & Mira da Silva, M. (2011). A Maturity Model for Implementing ITIL V3 in Practice. *15th IEEE International Enterprise Distributed Object Computing Conference Workshops (EDOCW).* Finland: IEEE.

Pereira, R., & Mira da Silva, M. (2012). Towards an Integrated IT Governance and IT Management Framework. *Accepted to 16th International Conference on En-terprise Distributed Object Computing, EDOC.* Beijing, China.: IEEE.

Racz, N. W. (2010). A Frame of Reference for Research of Integrated. *De Decker, B., Schaumuller-Bichl, I. (eds.) CMS 2010. LNCS, vol. 6109* (pp. 106–117). Heidelberg: Springer.

Radovanovic, D., Radojevic, T., Lucix, D., & Sarac, M. (2010). IT audit in accordance with Cobit standard. *Proc. of the 33rd International Convention on MIPR (MIPRO 10)* (pp. 1137-1141). Switzerland: IEEE.

Rosário, T., Pereira, R., & Mira da Silva, M. (2012). Formalization of the Audit Process Management. *Accepted to 15th IEEE International Enterprise Distributed Object Computing Conference Workshops (EDOCW).* China: IEEE.

Sahibudin, S., Sharifi, M., & Ayat, M. (2008). Combining ITIL, COBIT and ISO/IEC 27002 in Order to Design a Comprehensive IT Framework in Organizations. *Second Asia International Conference on Modeling & Simulation (AICMS).* Malaysia.

Schermann, M., Ohmann, T., & Krcmar, H.. Explicating Design Theories with Conceptual Models: Towards a Theoretical Role of Reference Models. *J. Becker, H. Krcmar & B. Niehaves, eds., Wissenschaftstheorie und gestaltungsorientierte Wirtschaftsinfor.*

Schon, D. A. (1983). *Reflective practitioner: How Professionals Think in Action.* New York: Basic Books.

Searcy, D., Woodproof, J., & Behn, B. (2003). Continuous Audit: The Motivations, Benefits, Problems, and Challenges Identified by Partners of a Big 4 Accounting Firm. *Proc. of the 36th Annual Hawaii International Conference on System Sciences (HICSS03)* (p. 10). United States: IEEE, doi: http://10.1109.

Senft, S., & Gallegos, F. (2009). *IT Control and Audit.* 3rd ed.: Taylor & Francis Group.

Simon, H. A. (1996). *The Sciences of the Artificial.* Massachusetts: MIT Press.

Steinberg, R. M. (2011). *Governance, Risk Management, and Compliance: It Can't happen To Us - Avoiding Corporate Disaster While Driving Success.* EUA: John Wiley & Sons.

Sun, S., Song, W., & Wen, L. (2008). Formal Semantics of BPMN Process Models using YAWL. *Intelligent Information Technology Application on Second International Symposium (IITA)* (pp. 70-74). IEEE.

Takemura, T. (2008). Formal Semantics and Verification of BPMN Transaction and Compensation. *Asia-Pacific Services Computing Conference* (pp. 284-290). New York: IEEE Press.

Tao, L. J. (2011). On How to Improve Organization's Internal Audit. *2nd International Conference on Management Science and Electronic Commerce* (pp. 1258–1260). China: IEEE.

Tarantino, A. (2009). *Governance, Risk and Compliance Handbook: Technology, Finance, Environmental and International Guidance and Best Practices.* United States: John Wiley & Sons.

Taylor, S., Iqbal, M., & Nieves, M. (2007). *ITIL:TSO publications, Norwith.*

The Institute of Internal Auditors. (2010). International Standards For The Professional Practice Of Internal Auditing. USA.

Thomson Reuters. (2011). *Fundamental of GRC - The Connected Roles of Internal Audit and Compliance.*

Verbeek, H., & Aalst, W. (2000). Woflan 2.0: A Petri-net-based Workflow Diagnosis Tool. *In: Nielsen, M., Simpson, D. (eds) Application and Theory of Petri Nets* (pp. 475–484). Berlin: Springer-Verlag.

Vicent, P., & Mira Da Silva, M. (2011). A Conceptual Model for Integrated Governance, Risk and Compliance. *23rd International Conference on Ad-vanced Information Systems Engineering* (pp. 199-213). London: Springer.

Watson, R. W. (2000). An enterprise information architecture- a case study for decentralized organizations. *Proceedings of the 33rd Hawaii International Conference on System Sciences.* Hawaii: IEEE.

Webster, J., & Watson, R. T. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. *MISQ*, (pp. 13-23).

Weill, P., & Ross, J. W. (2004). *IT Governance – How Top Performers Manage IT Decision Rights for Superior Results.* USA: Harvard Business Press, B, M.

Wu, C. H., Shao, Y. E., Ho, B. Y., & Chan, T. Y. (2008). On an Agent-based Architecture for Collaborative Continuous Auditing. *Proc. of the 12th International Conference on CSCW in Design (CSCWD 2008).*

Yang, L. (2011). Study on the improvement of the Internal Audit Work in IT Environment. *Fourth International Symposium on Knowledge Acquisition and Modeling (KAM)*, (pp. 233 – 236).

Ye, J. H., Sun, S. X., Wen, L., & Song, W. (2008). Transformation of BPMN to YAWL. *Proc. of the 2008 International Conference on Computer Science and Software Engineering (CSSE '08)* (pp. 354-359). doi: http://10.1109/CSSE.2008.980.

Appendixes

Appendix A – IT Audit Management Activities

Responsibility/ Activities		Frameworks/ References
1	Periodically conduct internal audits to verify anyone follow relevant guidelines for professional behavior, and process compliance	(ISO 38500, 2008) (Taylor, Iqbal, & Nieves, 2007) (The Institute of Internal Auditors, 2010)
2	Regularly evaluate the extent to which IT satisfies obligations (regulatory, legislation, law, contractual), internal policies, standards, and professional guidelines ensuring that are timely, comprehensive, and suitable for the evaluation of the extent of satisfaction of the business	(COBIT 4.1 Framework, 2007)(ISO 38500, 2008) (Taylor, Iqbal, & Nieves, 2007)
3	Ensure that all actions relating to IT are ethical	(ISO 38500, 2008) (The Institute of Internal Auditors, 2010)
4	Ensure auditors independence which constitutes the base of the audit impartiality	(ISO 19011, 2002) (The Institute of Internal Auditors, 2010)
5	Regularly evaluate the organization's internal conformance to its system for governance of IT	(ISO 38500, 2008) (The Institute of Internal Auditors, 2010)
6	Regularly check SI for compliance security implementation standards	(ISO 27001, 2005)
7	Obtain assurance of compliance and adherence to all internal policies derived from obligations	(COBIT 4.1 Framework, 2007) (The Institute of Internal Auditors, 2010)
8	Ensure that there are executing all security procedures to achieve compliance with security policies and standards	(ISO 27001, 2005)
9	Assess/Reviewing performance against agreed-upon targets	(COBIT 4.1 Framework, 2007) (Taylor, Iqbal, & Nieves, 2007)
10	Report performance	(COBIT 4.1 Framework, 2007) (Taylor, Iqbal, & Nieves, 2007)
11	Monitor the performance of independent reviews, audits and examinations	(COBIT 4.1 Framework, 2007) (Taylor, Iqbal, & Nieves, 2007)
12	Audit must contribute to the improvement of risk management processes in the firm	(Tarantino, 2009) (Davis, Schiller, & Wheler, 2011) (The Institute of Internal Auditors, 2010)
13	Appoint a audit manager to communicate with of board of directors	(Senft & Gallegos, 2009)
14	Perform internal and external audits in a similarly way. The differences should remain in the formality of the process (external audit is more formal) and in the objectives (external audit also compromise audits to obtain certification). Also, external audits represents a more complex process.	(Senft & Gallegos, 2009) (Tarantino, 2009)
15	Plan and agree audit requirements	(ISO 27001, 2005)(Senft & Gallegos, 2009) (Davis, Schiller, & Wheler, 2011), (ISO 19011, 2002) (The Institute of Internal Auditors, 2010)
16	Plan and agree audit activities	(ISO 27001, 2005) (The Institute of Internal Auditors, 2010)
17	Use SI audit tools when possible, to prevent any possible misuse or compromise	(ISO 27001, 2005) (ISO 38500, 2008)
18	Associate evidences to all audit findings	(ISO 19011, 2002) (Senft & Gallegos, 2009)

19	Analyze all findings in an objective way, to assess if audit criteria is reached	(ISO 19011, 2002) (Senft & Gallegos, 2009)
20	Write an audit plan which must describe the objectives of an audit	(ISO 19011, 2002) (Senft & Gallegos, 2009) (Tarantino, 2009) (Thomson Reuters, 2011)(Davis, Schiller, & Wheler, 2011)
21	Write an audit plan which must describe the scope of an audit which describes the extent and boundaries of the audit, such as physical locations, organizational units, activities and processes to be audited	(ISO 19011, 2002) (Senft & Gallegos, 2009) (Tarantino, 2009) (Thomson Reuters, 2011) (Davis, Schiller, & Wheler, 2011)
22	Write an audit report that must include: audit objectives, audit scope, audited entity, audit team description, identification of the organizational and functional units or processes audited and the time period covered, dates and places where audit occurred, audit criteria's, findings and conclusions	(ISO 19011, 2002) (Davis, Schiller, & Wheler, 2011) (Senft & Gallegos, 2009) (De Haes & Grembergen, 2008) (Davis, Schiller, & Wheler, 2011)
23	Ensure that audit report is reviewed, approved, and distributed to interested entities	(ISO 19011, 2002) (Davis, Schiller, & Wheler, 2011)
24	Establish audit procedures	(ISO 19011, 2002) (Senft & Gallegos, 2009) (Tarantino, 2009) (The Institute of Internal Auditors, 2010)
25	Allocate resources to established audit procedures	(ISO 19011, 2002) (Senft & Gallegos, 2009) (Tarantino, 2009) (Grembergen & Haes, 2009)
26	Perform team selection	(ISO 19011, 2002)
27	Schedule audit and include this information in the audit plan document	(ISO 19011, 2002) (Senft & Gallegos, 2009) (Tarantino, 2009) (Grembergen & Haes, 2009)
28	Develop a list of feasible recommendations accordingly with audit findings	(Tarantino, 2009) (Grembergen & Haes, 2009)
29	Develop a list of action plans accordingly with audit findings	(Tarantino, 2009) (Grembergen & Haes, 2009)
30	Automate audit procedures when possible	(Senft & Gallegos, 2009) (Tarantino, 2009) (Davis, Schiller, & Wheler, 2011)
31	Perform automated tests when applicable and collect evidences to determine if requirements are being followed	(Tao, 2011) (Tarantino, 2009)
32	Perform a kick-off meeting so that audited entity know all the details behind audit	(Senft & Gallegos, 2009) (De Haes & Grembergen, 2008) (ISO 19011, 2002)
33	Gain preliminary understanding about the audited areas	(Tarantino, 2009) (Senft & Gallegos, 2009) (Grembergen & Haes, 2009)
34	Auditor should plan the application of audit techniques useful in a specific audit	(Senft & Gallegos, 2009) (Davis, Schiller, & Wheler, 2011), (ISO 19011, 2002)
35	The allocation of audit team should have in account the knowledge and competences of the auditors and their roles and responsibilities should be assigned accordingly with this knowledge	(ISO 19011, 2002)
36	The allocation of audit team should have in account budget associated with the audit	(ISO 19011, 2002)
37	Audit manager should appoint the audit team leader	(ISO 19011, 2002)
38	Report to interested parts, the overall achievements of the audit	(Tarantino, 2009) (Thomson Reuters, 2011) (Grembergen & Haes, 2009)
39	Ensure review and approval of audit report, and ensure it distribution to the audit interested parties	(Tarantino, 2009) (Thomson Reuters, 2011) (Grembergen & Haes, 2009)

40	Establish an audit criteria which are used as a reference against which conformity is determined	(ISO 19011, 2002) (Senft & Gallegos, 2009) (Grembergen & Haes, 2009)
41	Develop support documents which must be used to assess audit criteria compliancev	(Senft & Gallegos, 2009) (ISO 19011, 2002)
42	Determine the feasibility of the audit accordingly with the existent time and resources	(Tarantino, 2009) (Davis, Schiller, & Wheler, 2011), (ISO 19011, 2002)
43	Take into account the audit objectives, scope, criteria and estimated duration of the audit in the allocation of resources	(ISO 19011, 2002) (Davis, Schiller, & Wheler, 2011),
44	Perform an initial contact with the audited entity to explain the objectives, main procedures, to establish communication channels and request access to the needed information	(ISO 19011, 2002) (Davis, Schiller, & Wheler, 2011) (The Institute of Internal Auditors, 2010)
45	Perform documents and information assess about relevant aspects of the audited entity	(Senft & Gallegos, 2009) (ISO 19011, 2002)
46	Establish the roles and responsibilities of the audit team members accordingly with the needed procedures to perform the audit	(ISO 19011, 2002) (Senft & Gallegos, 2009)
47	Assign tasks to each team member accordingly with specific processes, functions, sites, areas or activities.	(Senft & Gallegos, 2009) (Grembergen & Haes, 2009), (Davis, Schiller, & Wheler, 2011), (ISO 19011, 2002)
48	Review the information relevant to audit assignments	(ISO 19011, 2002) (Senft & Gallegos, 2009)
49	Prepare work documents as necessary for reference and for recording audit proceedings	(ISO 19011, 2002) (Senft & Gallegos, 2009)
50	Prepare support documents such as checklists and audit sampling plans, and forms for recording information	(ISO 19011, 2002) (Senft & Gallegos, 2009)
51	Raise evidences using methods such as interviews, observation of activities and review of documents and elicit issues associated with them	(ISO 19011, 2002) (Senft & Gallegos, 2009) (Grembergen & Haes, 2009)(Davis, Schiller, & Wheler, 2011), ,
52	Evaluate evidences against the audit criteria to generate the audit findings	(ISO 19011, 2002) (Senft & Gallegos, 2009) (Davis, Schiller, & Wheler, 2011)
53	Perform a close meeting to present the audit findings and main conclusion to audited entity	(ISO 19011, 2002) (Senft & Gallegos, 2009) (Grembergen & Haes, 2009) (Davis, Schiller, & Wheler, 2011), (The Institute of Internal Auditors, 2010)
54	Perform a close meeting to discuss and explain the recommendations and action plans to audited entity	(ISO 19011, 2002) (Grembergen & Haes, 2009)(Davis, Schiller, & Wheler, 2011),

Appendix B – IT Audit Management Process (BPMN)

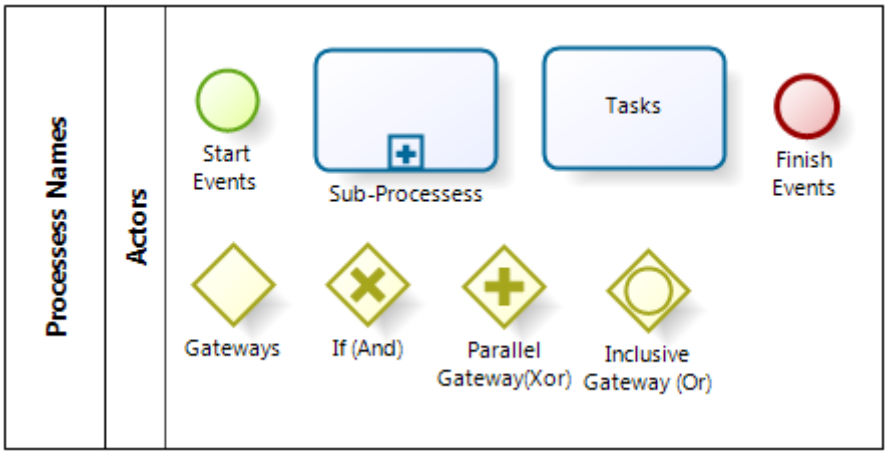

Figure 14. IT AM Process - Legend

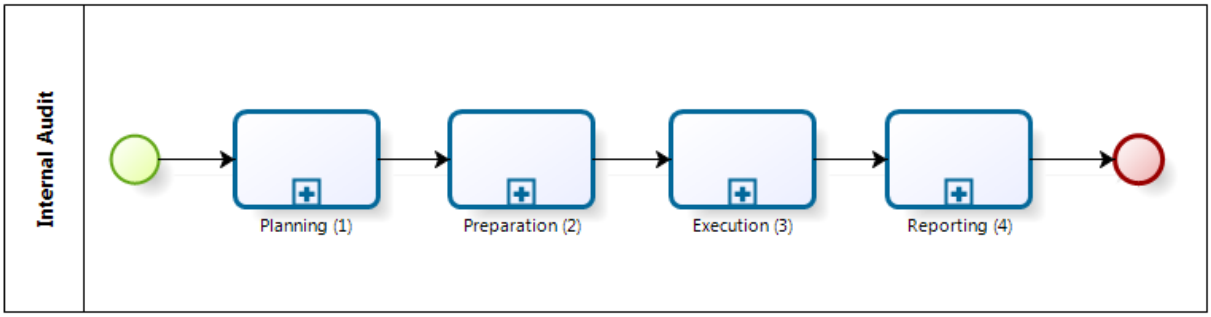

Figure 15. IT AM Process - Internal Audit

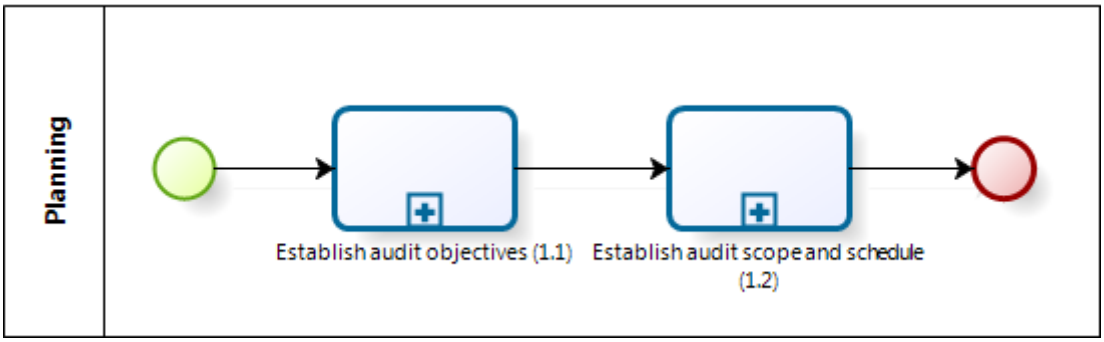

Figure 16. IT AM Process - Planning

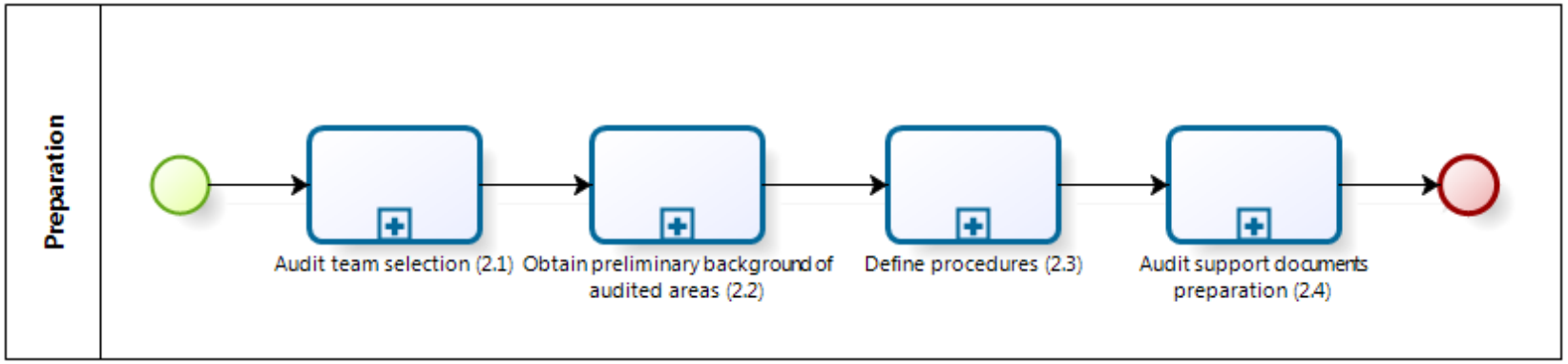

Figure 17. IT AM Process - Preparation

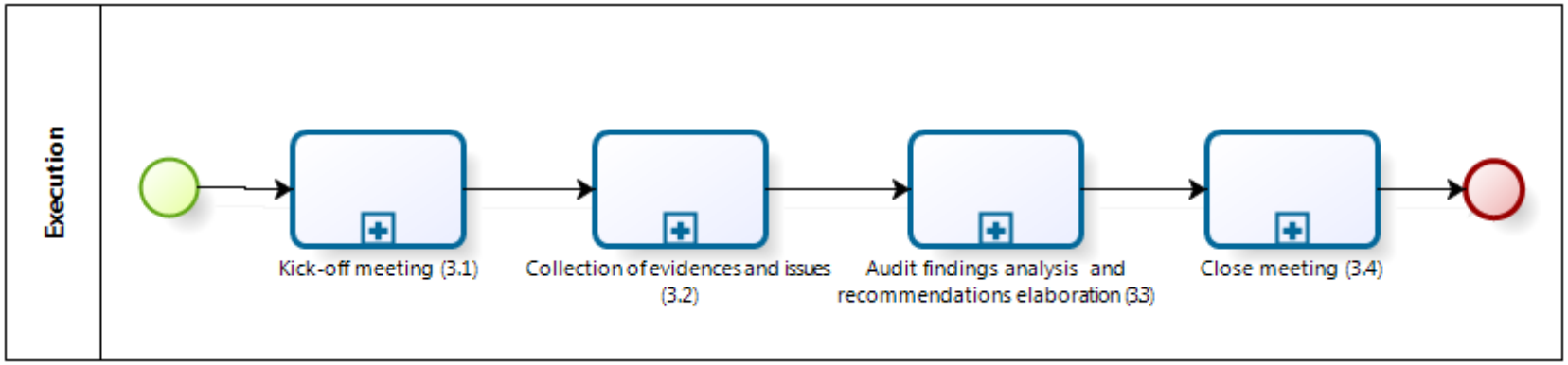

Figure 18. IT AM Process - Execution

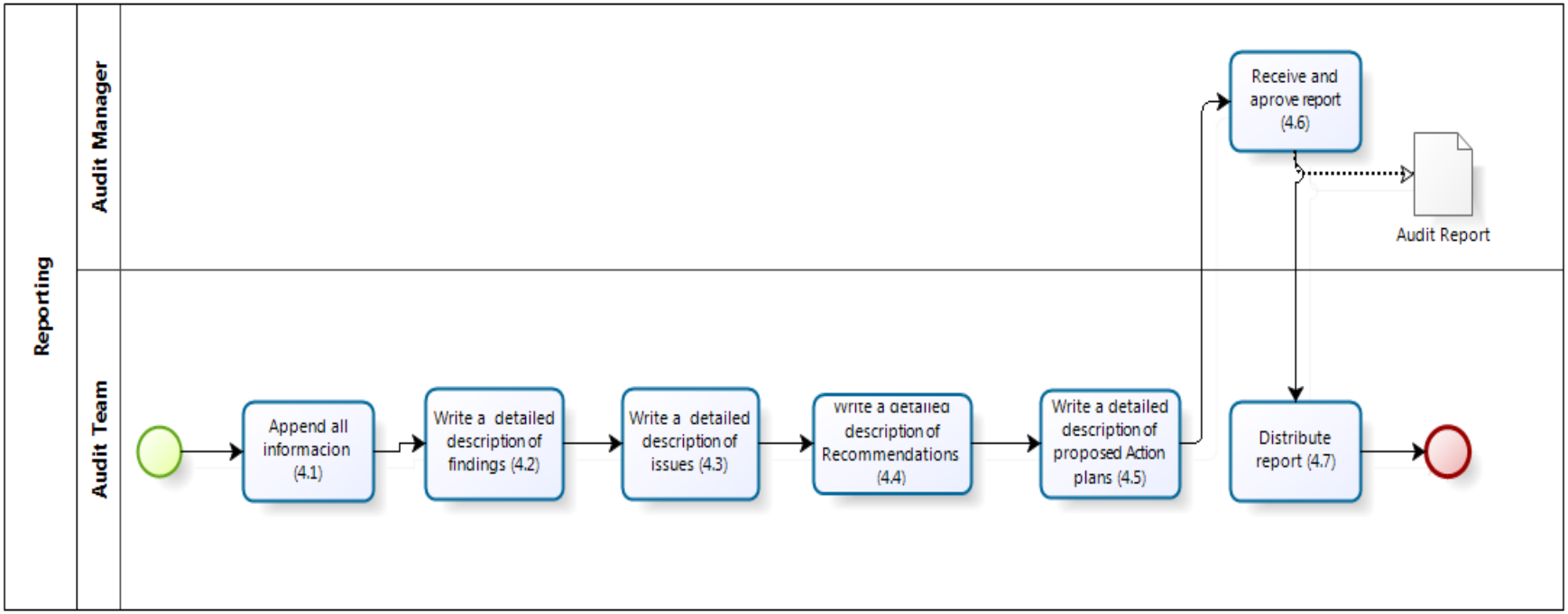

Figure 19. IT AM Process - Reporting

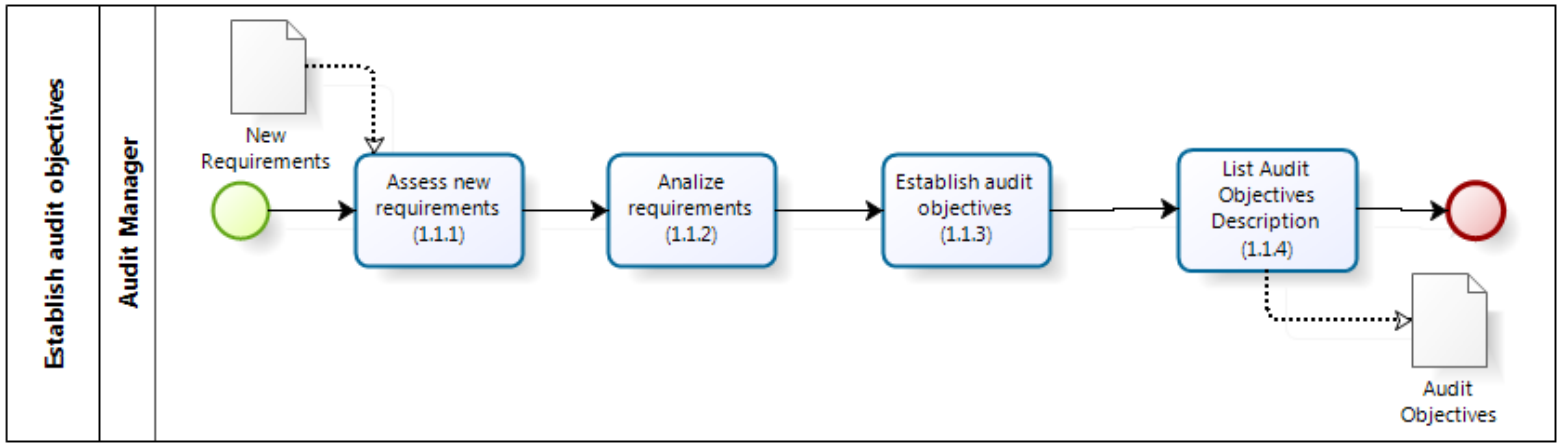

Figure 20. IT AM Process - Establish Audit Objectives

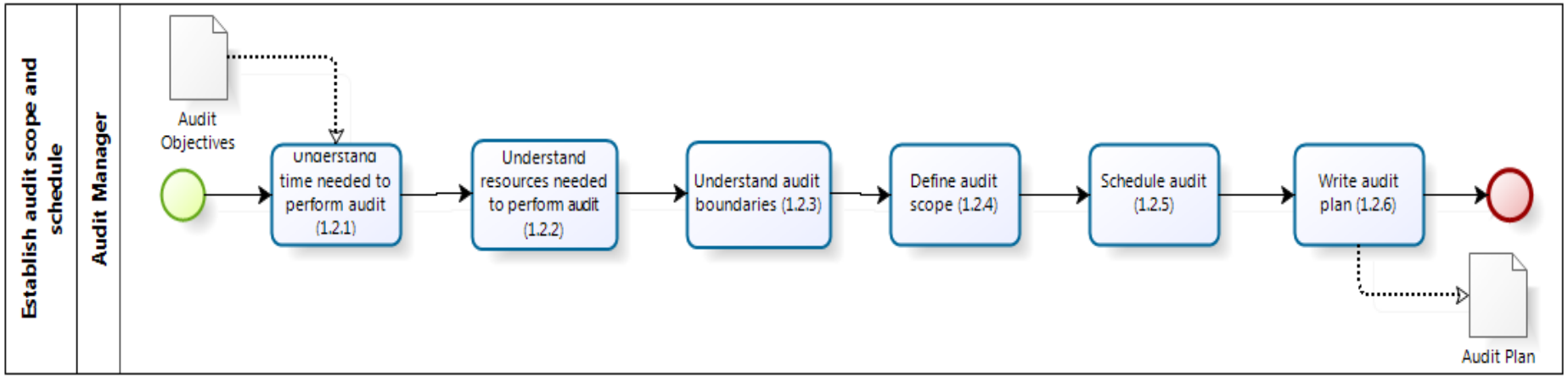

Figure 21. IT AM Process - Establish Audit Scope and Schedule

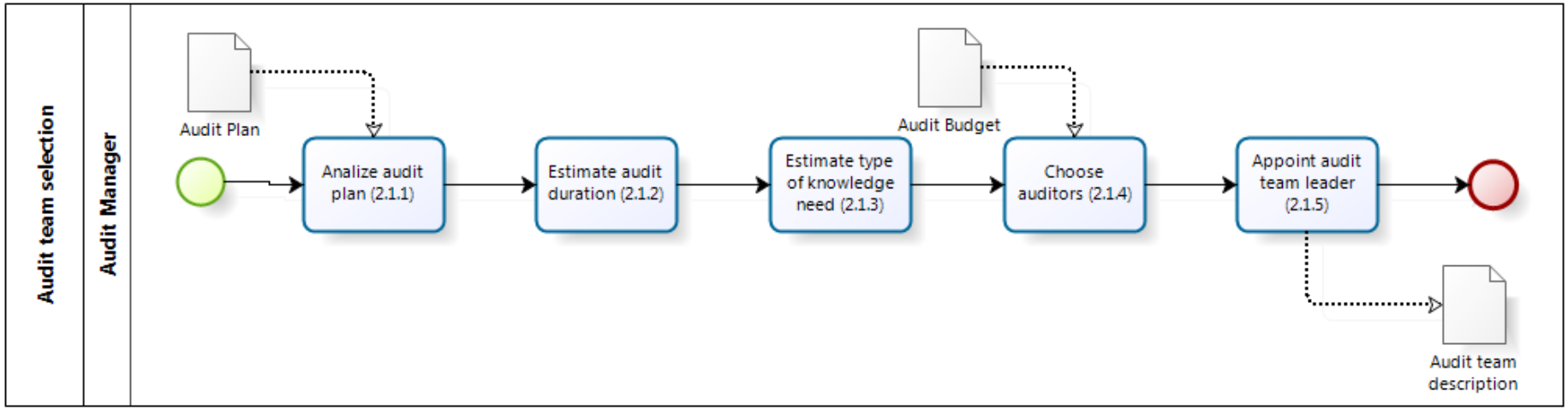

Figure 22. IT AM Process - Audit Team Selection

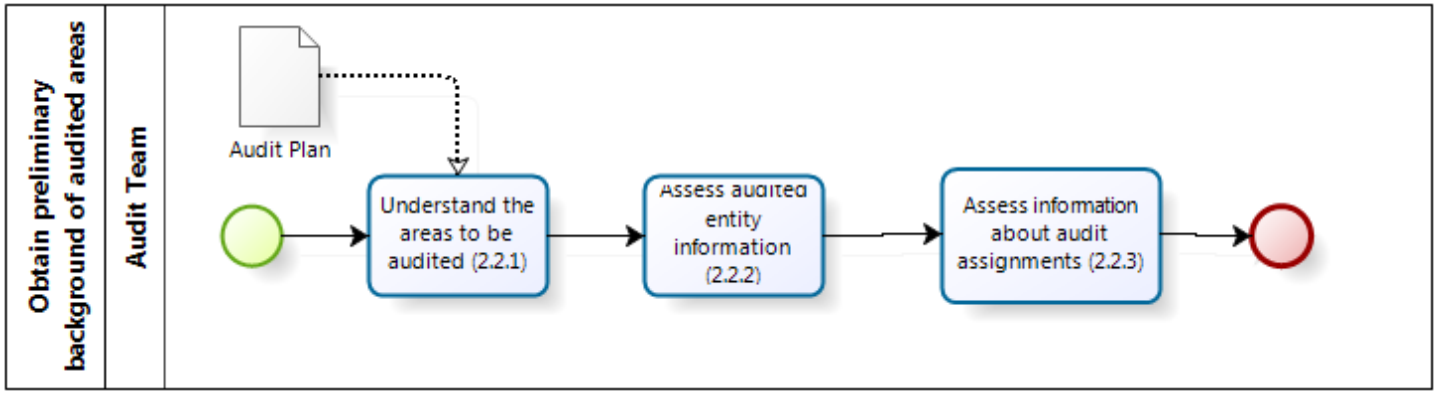

Figure 23. IT AM Process - Obtain Preliminary Background of Audited Areas

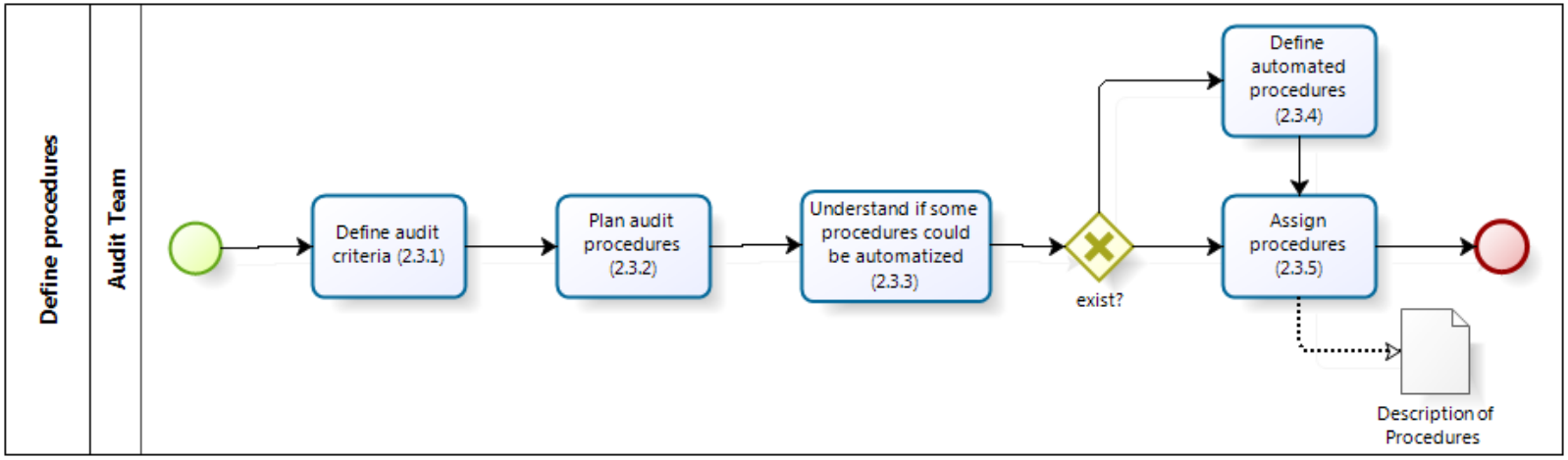

Figure 24. IT AM Process - Define Procedures

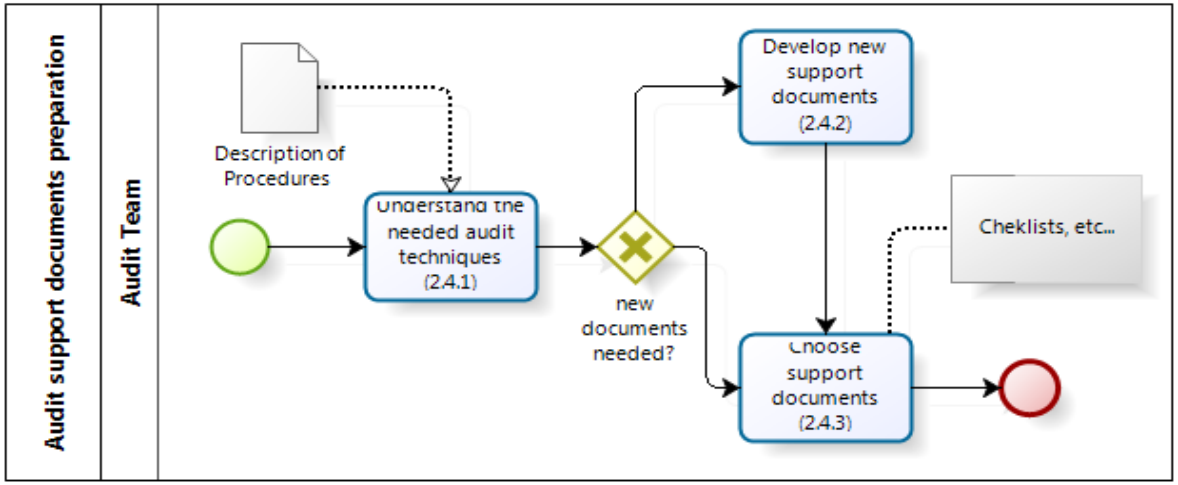

Figure 25. IT AM Process - Audit Support Documents Preparation

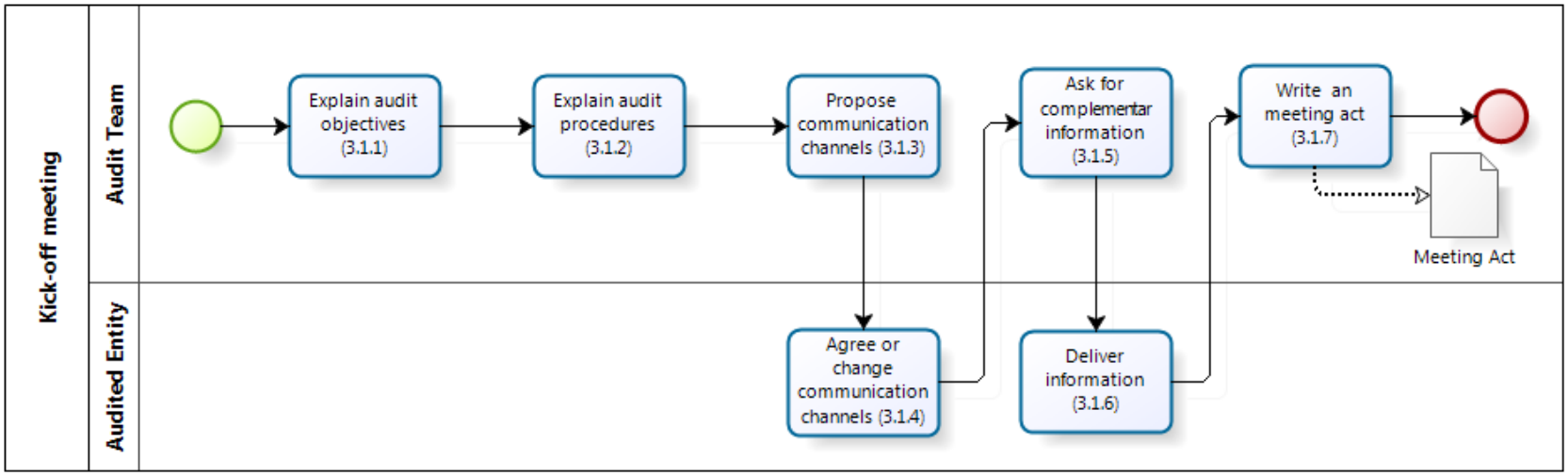

Figure 26. IT AM Process - Kick-Off Meeting

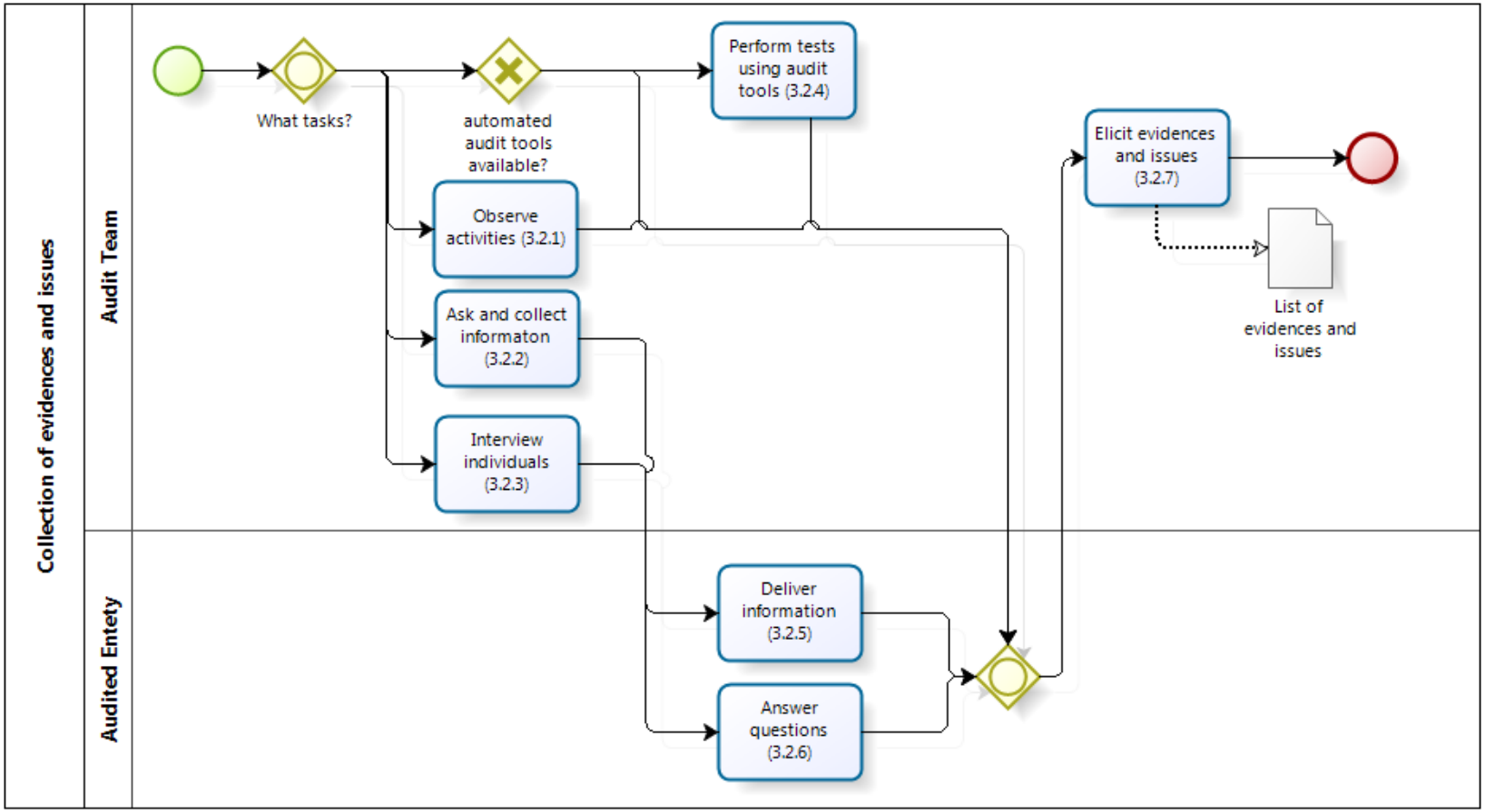

Figure 27. IT AM Process - Collection of Evidences and Issues

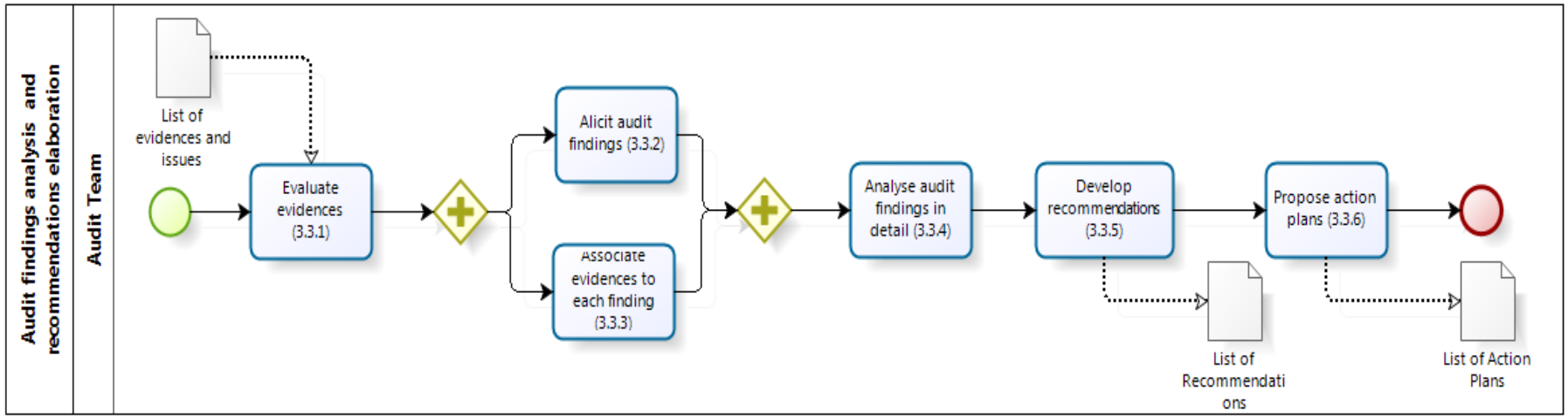

Figure 28. IT AM Process - Audit Findings Analyses and Recommendations Elaboration

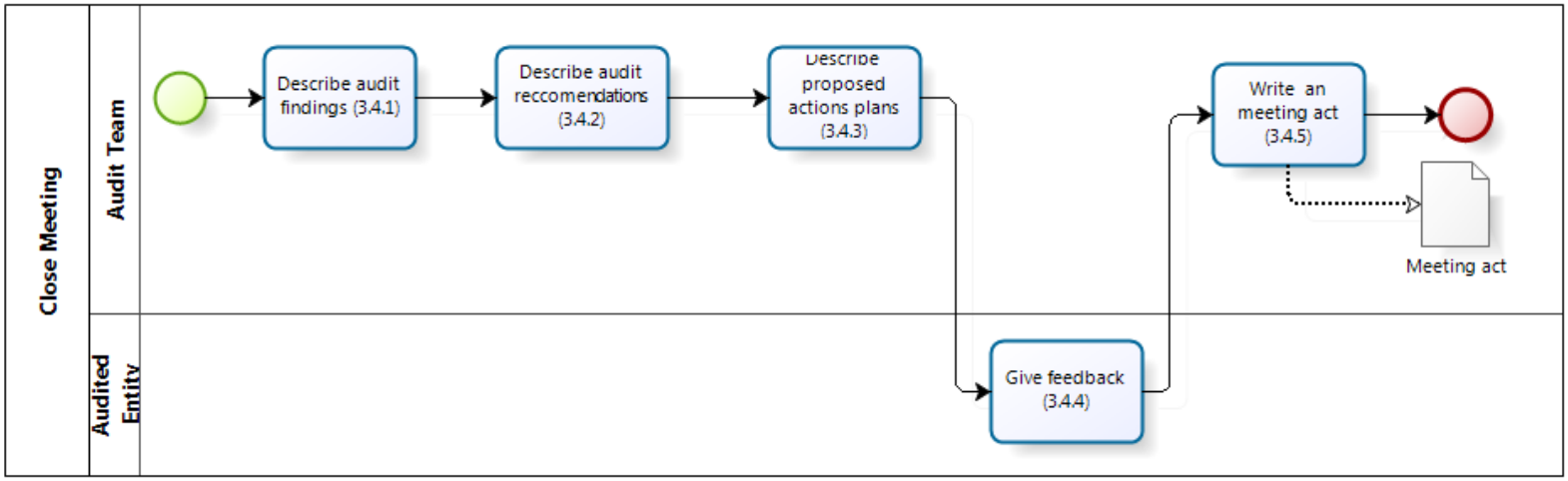

Figure 29. IT AM Process - Close Meeting

Appendix C – CRUD Matrix without Analysis

CRUD Matrix	Objectives	Scope	Initial Date	Audit Plan	Duration	Audit Team	Criteria	Audit Procedures	Audited Entity Information	Communication Channels	Meeting Act	Suport Documents	Evidences	Issues	Findings	Recommnedations	Action Plans	Audit Report	Audit Budget	New Requirements
1.5.1.1 - Establish audit objectives	C																			R
1.5.1.2- Establish audit scope and schedule	R	C	C	C																
1.5.2.1 - Audit team selection				R	C	CRU													R	
1.5.2.2 - Obtain preliminary background of audited areas				R					CRU											
1.5.2.3 - Define Procedures							R	RU												
1.5.2.4 - Audit support documents preparation								R				CRU								
1.5.3.1 - Kick-off meeting	R							R	RU	CRU	C									
1.5.3.2- Collection of evidences and issues													C	C						
1.5.3.3 - Audit findings analysis and recommendations elaboration													R	R	C	C	C			
1.5.3.4 - Close meeting											C				R	R	R			
1.5.4 - Reporting															R	R	R	C		

Appendix D – Yawl-Nets

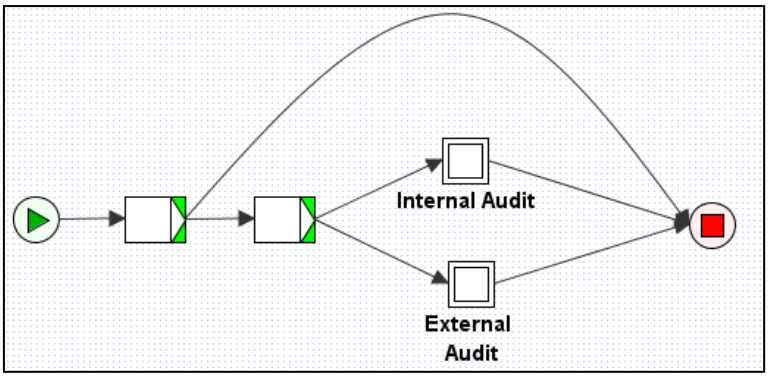

Figure 30. Yawl Nets - Audit Management

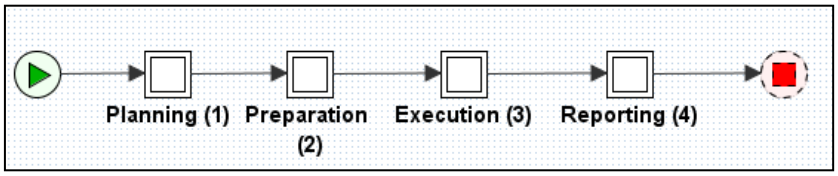

Figure 31. Yawl Nets - Internal Audit

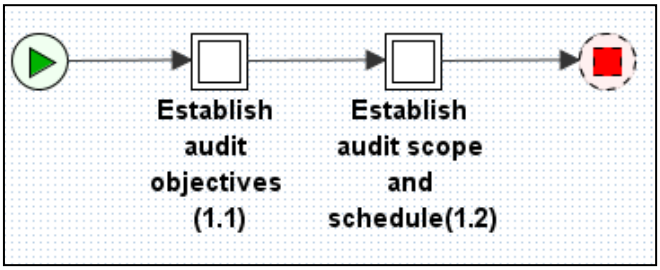

Figure 32. Yawl Nets - Planning

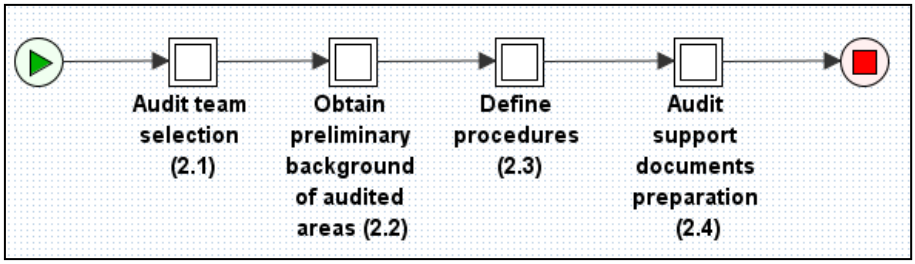

Figure 33. Yawl Nets - Preparation

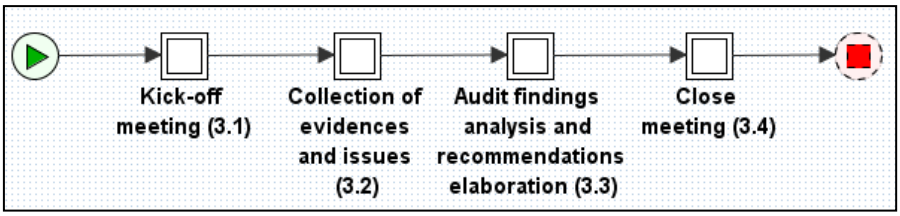

Figure 34. Yawl Nets - Execution

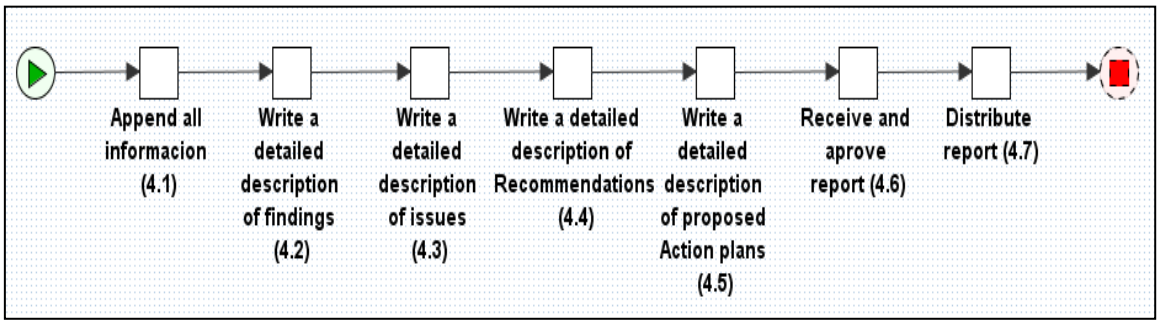

Figure 35. Yawl Nets - Reporting

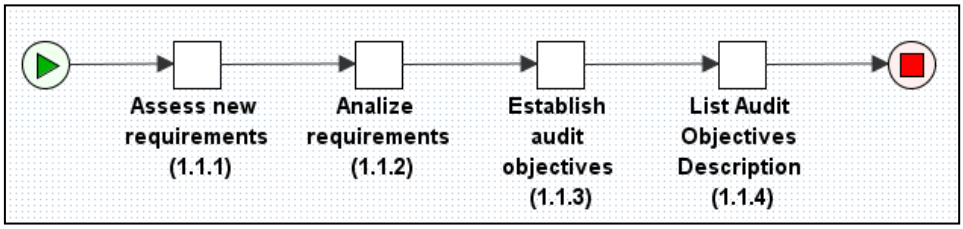

Figure 36. Yawl Nets - Establish Audit Objectives

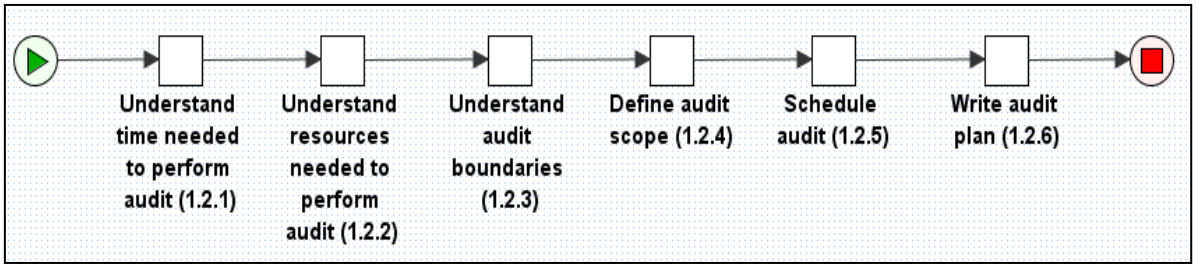

Figure 37. Yawl Nets - Establish Audit Scope and Schedule

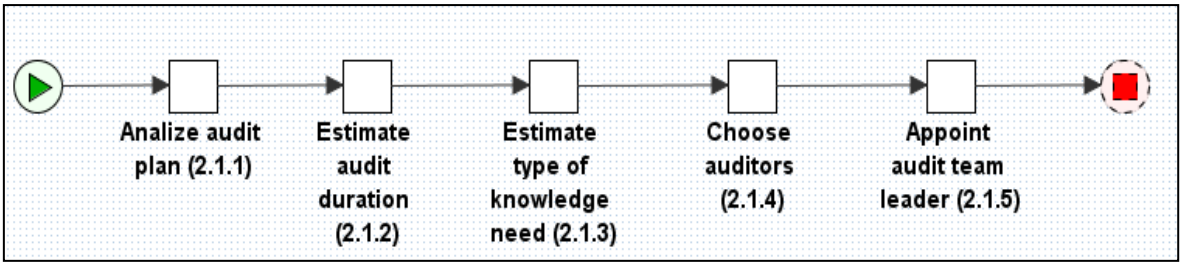

Figure 38. Yawl Nets - Audit Team Selection

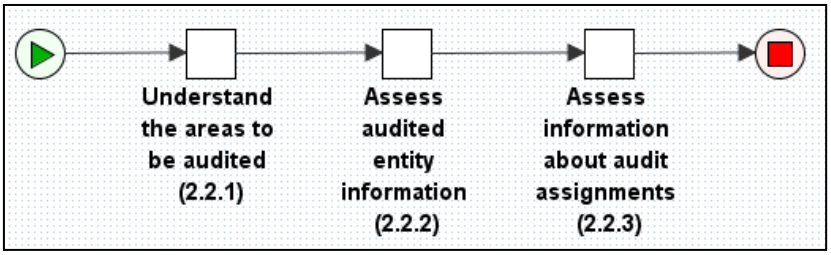

Figure 39. Yawl Nets - Obtain Preliminary Background of Audited Areas

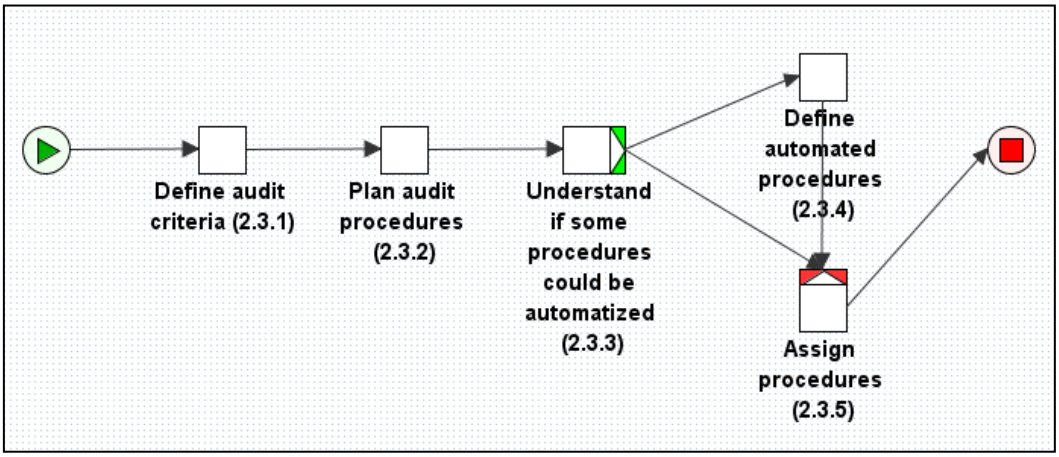

Figure 40. Yawl Nets - Define Procedures

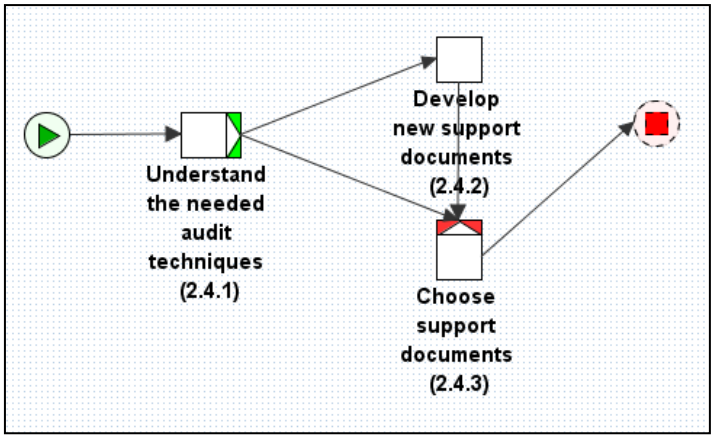

Figure 41. Yawl Nets - Audit Support Documents Preparation

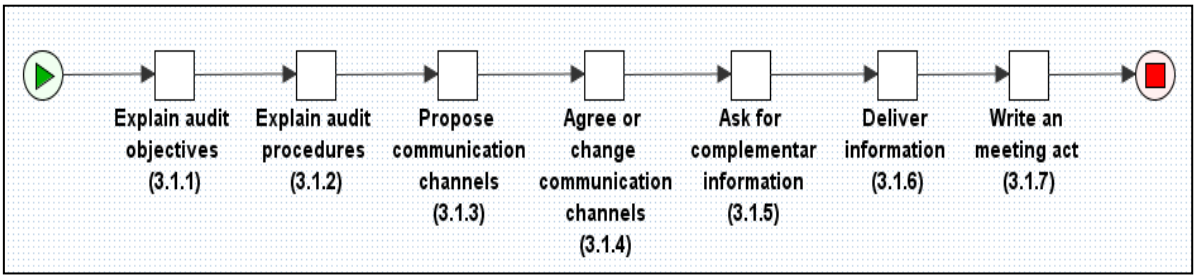

Figure 42. Yawl Nets - Kick-Off Meeting

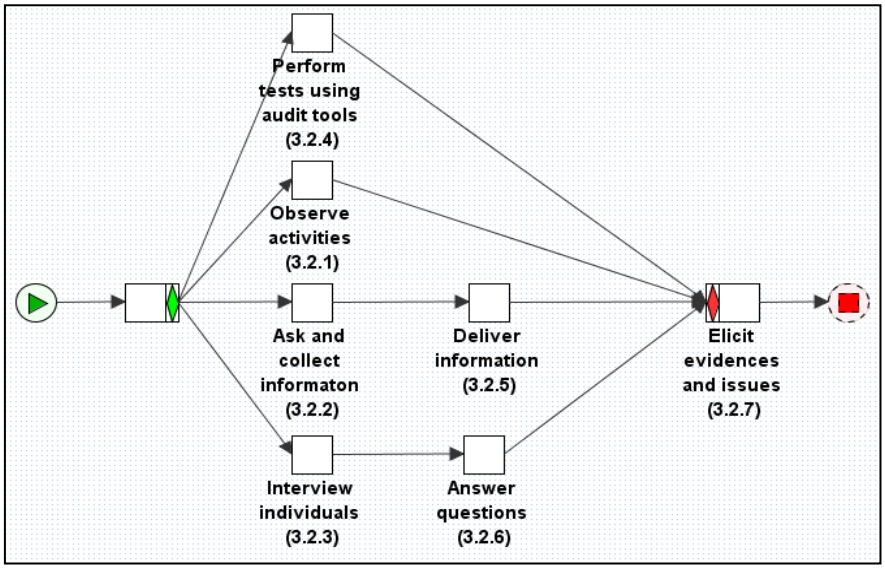

Figure 43. Yawl Nets - Collection of Evidences and Issues

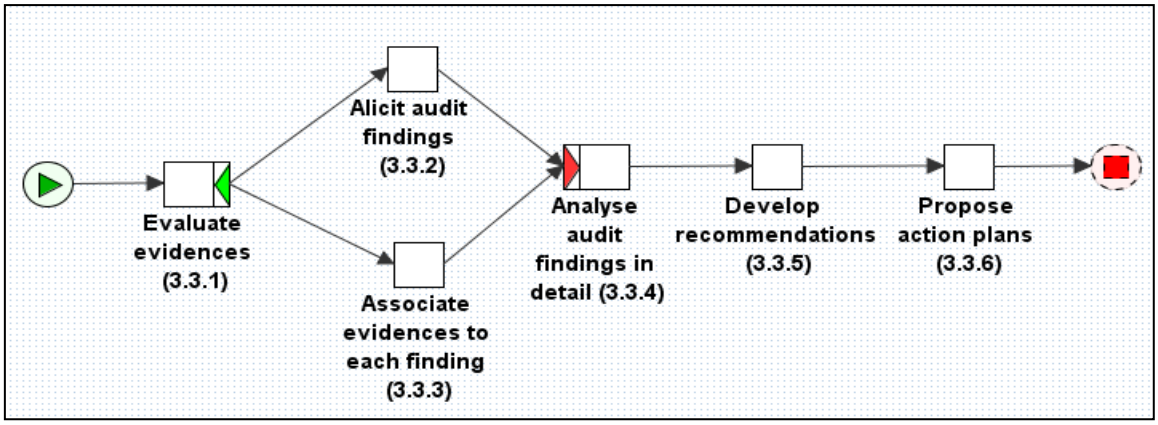

Figure 44. Yawl Nets - Audit Findings Analyses and Recommendations Elaboration

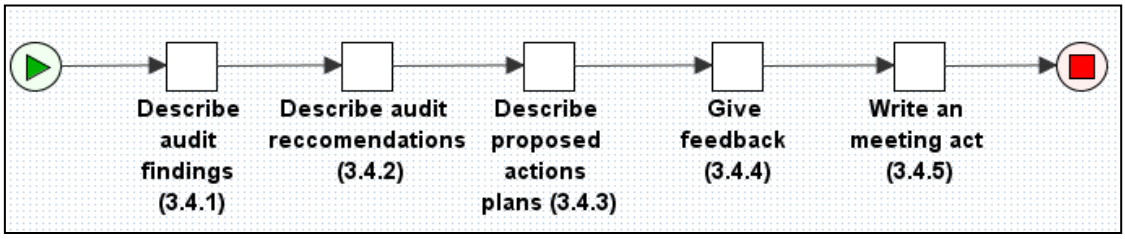

Figure 45. Yawl Nets - Close Meeting

Appendix E – Interviews Support Questionnaire

IT Audit – Support Questionnaire

This interview has the objective of elicit the main requirements of an efficient IT Audit Management Process.

Estimated duration: 30 to 60 minutes

1 Do you think that the actual IT audit management process is efficient? (time, resources, etc)?

2 Do you think that is possible to improve the actual IT audit management process? How?

3 Talking about automated procedures:

What are the advantages of having automated tasks in the process?	
What are the advantages of using tools to conduct audits?	
What are the main disadvantages?	

4 Talking about IT Audit requirements…

Refer between 5 to 10 essential requirements to conduct an audit.	Refer between 5 to 10 essential requirements in an audit tool.	What are the organizational assets which can benefits with audit function

5 Do you know any audit tool? Describe it.

Appendix F – Questionnaire

Questionnaire

(IT Audit)

Estimated Time: 30 Minutes

Aim

The aim of this research is to study the IT Audit Process. We want to understand what the main activities needed to perform audits are. To do this we design the IT audit process which needs to describe a complete process but also general enough so that it can be adapted by all organizations. We also want to know what kind of information is manipulated during this process and the information systems that manipulate that information.

Questions:

Observe the appendix 1 and answer the following questions

1. Please fill in the following table. If you need to refer to a task, use the number associated with it.

Question	Response
1 - All tasks represented in figure are understandable? What tasks don't you understand?	
2 - And the all process is simple enough to be understandable to a non-expertise in audit domain?	
3 - The tasks represented in figure are correct? What tasks are incorrect?	
4 - The Internal audit process showed is complete? In other words, there are tasks essential in the audit process which is not represented? What tasks?	

5 - The process described is implementable?	
6 **-** The process can be integrated in organization? In other words, the process can be integrated with other organization processes without interfering in them?	
7 - The process described can be adapted to all organizations?	
8 - The process described satisfies the needs of business? (e.g. process produces the right documents?	

Observe the appendix 2 and answer the following questions

2. Please fill in the following table. If you need to refer to a row, use the number associated with it.

Question	Response
1 – Do you understand all information entities and descriptions? What entities or descriptions don't you understand?	
2 – The table contains all the information needed in the audit process? If not, what other information is needed?	
3 – All information is useful? If not, what are the entities not useful?	
4 – The relations between the entities seem correct? And adaptable to the process in question 1?	

5 – The proposed applications seem correct? Are sufficient?	

Respondent's data

(This information is only used to prove that all respondents have experience on the area. The respondent's names and their companies are not referred in our research to protect personal information)

Function within the actual company:

Work experience (Years):

Thank you for your help!

Appendix 1 - IT audit process

(In the real questionnaire we provide the complete IT Audit Management Process as in Appendix B of this thesis. We don't put the process here since we already show it in that appendix)

Appendix 2 – Information manipulation during IT Audit Process

(In the real questionnaire we provide a complete description of IT Audit Information and Applications as in sections 4.5 and 4.6 of this thesis. We don't put the process here since we already show it in those sections)