Formalization of the IT Audit Management Process

Tiago Rosário
Instituto Superior Técnico, INOV
Lisbon, Portugal
tiago.rosario@ist.utl.pt

Abstract—Due to the numerous problems occurred in organizations, compliance needs to develop internal policies and procedures that ensure the adherence with a set of obligations. However, there is no guarantee that all entities meet the organization requirements, and an auditor is the last line of defense 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 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 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 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.

Keywords- Audit, IT Audit Management Process, Compliance, Formal Process.

I. INTRODUCTION

Over the last few decades, the damage made by the successive disasters leads to the rise of new laws and acts since weaknesses in regulations were a major contributing factor to the crisis occurrence [1].

Although the development of policies is a role that belongs to compliance management, there is no guarantee that all entities meet the organization requirements [2], and an auditor is the last line of defence to detect problems.

Audit allows organizations to guarantee a good internal control system since it is an independent and objective assurance activity that employs systemized methods to obtain evidences [3] and evaluate control system [4].

Currently, IT has become increasingly more important and began to be comprised in the organization’s business core processes [5]. So, it is crucial to achieve a good alignment of IT with business needs [6] which increase the necessity of more requirements in this area [7].

On the path to improve the alignment of IT with business needs, organizations use several best practices frameworks to reach their goals - not only in terms of performance but also in terms of being legislation compliant [7, 6]. However, these frameworks and literature isn’t complete in the area of IT audit [8]. So, it there’s not a complete IT audit management process (IT AM process) which organizations can implement on their organizations. So, the effectiveness of the audit is low since there is an excessive consumption of assets and resources [9].

Since the definition of formal procedures to perform audits can bring benefits to organizations [9], and knowing that IT has become crucial to the support, sustainability and growth of the business [10], 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 [8].

To model the IT AM process we use the Business Process Model Notation (BPMN). We also design the information and Information Systems (IS) architectures to understand what kind of data must be manipulated and how to do it.

The research methodology used is Design Science Research (DSR). Our constructs will be leveraged based on literature review and practitioners’ expertise. Afterwards we will integrate our constructs in order to achieve our models.

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 the BPMN.
- 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 with practitioners agree and accept the created models using the Moody & Shanks framework [11].
- Paper publication in a respectful international conference.
II. Problem

Nowadays organizations are facing an increasing number of regulations with which it is necessary to be compliant [9, 2]. Besides this, IT audit procedures also become more complex [12] since the way requirements are analyzed has also become more complex over the time [13]. So the way how audits are performed is affected [14]. Due to this fact, IT auditors’ effort is growing [13] but the degree of compliance achieved is decreasing [9].

To implement an efficient IT AM process that solves these problems, audit departments could use frameworks to elicit best practices in the way of perform audits. However, frameworks are seen as complex [15], too general [16], overlapping each other [17] [18], hard to implement [19] and they don’t propose a complete process [8].

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 [9]. To achieve these intents, activities need to be standardized and the IT AM process needs to be well defined [14, 9].

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 [8].

To conclude, we state that a pertinent hypothesis should be:

It is possible to design a complete, general and adaptable IT audit management process using the best practices provided by the most accepted IT frameworks and literature.

III. Research Methodology

The research methodology that will be used in this thesis is Design Science Research (DSR). Design science addresses research through the building and evaluation of artefacts designed to meet the identified business needs [20] instead of analysing existing IS in order to identify causal relations [21].

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 [22]. Models use constructs to represent a real world situation, the design problem and the solution space [23].

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 models which are the input of the third.

As advisable by March & Smith [24] 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 I).

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.

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” [10].

In order to leverage the IT audit sub-phases, IT audit roles, IT audit activities, IT audit data and IT AM information entities we will use extensive literature review. The approach used in this paper follows the concept-centric methodology of IS literature reviews as outlined in [5].

Österle et al. [21] also point four principles that design-oriented IS research must comply with, and that we followed:

- **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.

<table>
<thead>
<tr>
<th>TABLE I. RESEARCH METHODOLOGY</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Build</strong></td>
</tr>
<tr>
<td>Constructs Definition:</td>
</tr>
<tr>
<td>- IT Audit Sub-Phases(^1)</td>
</tr>
<tr>
<td>- IT Audit Roles</td>
</tr>
<tr>
<td>- IT Audit Activities</td>
</tr>
<tr>
<td>- IT Audit Data</td>
</tr>
<tr>
<td>- IT AM Process Information Entities</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>- IT AM Process</td>
</tr>
<tr>
<td>- IT AM Information Architecture</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IV. RELATED WORK</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

**A. Governance, Risk, and Compliance**

IT audit is inserted in IT compliance domain which in turn belongs to Governance, Risk and Compliance (GRC) [25].

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

“GRC is an 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” [26].

The definition of GRC shows that Governance, Risk and Compliance are domains with too many relations between them.

Corporate governance needs to define and realize missions and goals, establish strategic direction, policies and objectives to that end, and monitor implementation [27]. Information technology governance (ITG) is part of corporate governance [6, 26]. It applies corporate governance concepts to drive and control IT in a strategic way, concerning about the value IT delivers to an organization [6]. 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 [28].

Risk management (RM) provides organizations a programmatic way to deal with business uncertainty and the associated risk and opportunity [9]. It seeks to identify, assess, and measure risk and then develop countermeasures to handle it [29]. 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 to provide reasonable assurance regarding the achievement of entity objectives” [29].

**B. Compliance**

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 [9]. So, compliance must guarantee that the organization is following all its obligations, and thus is operating within the defined mandated and voluntary boundaries [30]. 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 [31].

---

\(^1\) IT Audit Phases are given in the Related Work section since it is not an our construct
For each new law or regulation, new internal policies and procedures are designed to deal with the rule specifications [32] and their good implementation is assessed by audit activity [6]. 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 [3].

Since IT is becoming pervasive in any organization of the world [5], IT decisions cannot be primarily based upon technology updates, storage capacity or cost savings independently of legal and compliance considerations [33]. So it is imperative for IT departments to ensure that their applications meet all compliance requirements that govern their products, services, and other activities [34].

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 [9].

C. Audit

Auditors are counsellors in advising on control issues as they relate to business processes [35], promoting the collaboration and integration of the corporate governance and modern internal controls [36].

Audit is an independent and objective assurance activity [3, 37] that employs systemized and standardized methods [9] to evaluate and improve the process of governance, risk management, control and treatment, so as to help the organization achieve its objectives [4].

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” [38].

Audit provides management with assurance, design and operation of the control processes in their organizations, which requires an impartial view [9]. 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 examination of evidence [9] intended to provide accurate and current information about the efficiency and effectiveness of policies and operations [14].
- **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 [14].
- **Oversight.** 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 [39].
- **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 [37].

Nowadays, IT auditors’ role is becoming crucial to organization success since their work evolved from monitoring and evaluation to the identification, consultation [36] and partnership of senior management [35]. IT Auditors are now, counsellors in advising on IT control issues as they relate to business processes [35], promoting the collaboration and integration of the corporate governance and modern internal controls [36]. They are also a partner in helping managers develop and implement the policies needed to attain information assurance [35]. So, IT audits ensure that organizations monitor how they do business and protect the interests of main stakeholders as managers, employees, customers, and investors [35].

D. 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” [3].

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 [8] that constitute an one direction flux [6] 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.
• **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.

V. **PROPOSAL**

In order to address the problem described in Section II, 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 III 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 assess 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 the IT AM process. We use the audit worldwide accepted phases as the basis of our work (described in section IV D). 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.

So, 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, [40]. With this linkage, it is possible to manage the changes needed by the business and maximize the benefits from the IT investments. Finally, a CRUD is designed so that organizations know what are the systems needed to automat audit procedures.

Next sub-sections describe in detail the construction of these artefacts.

A. **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 [14]. We use the phases described in Section IV D 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. An example of the sub-phases elicit are described in Table II.

<table>
<thead>
<tr>
<th>Phases</th>
<th>Sub-Phases</th>
<th>Description</th>
<th>Frameworks / References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Planning</td>
<td>Establish audit objectives</td>
<td>Determination of what is intended to be accomplish with the audit accordingly with the requirements analysis</td>
<td>[39], [41], [35], [3]</td>
</tr>
<tr>
<td></td>
<td>Establish audit scope and schedule</td>
<td>Scheduling of audit in cooperation with the audit entity</td>
<td>[14], [6], [39], [39], [3]</td>
</tr>
</tbody>
</table>

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 e describe in Section IV D.
B. 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 principal roles of IT AM process. The audit roles as well as the references from where we elicit them are listed in Table III.

<table>
<thead>
<tr>
<th>Role</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit Manager</td>
<td>[14] [3] [9] [10] [7] [37] [39] [3]</td>
</tr>
<tr>
<td>Audit Team</td>
<td>[14] [3] [10] [6] [39] [39] [3]</td>
</tr>
<tr>
<td>Audited Entity</td>
<td>[3] [9] [10] [37] [6]</td>
</tr>
</tbody>
</table>

We just elicited the essential roles which have associated a high number of references.

C. 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 IV as well as the correspondent references. Since there are a high number of activities (54), here we just provide an example of them.

<table>
<thead>
<tr>
<th>Responsibility/Activities</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plan and agree audit requirements</td>
<td>[42] [14] [39] [3] [38]</td>
</tr>
<tr>
<td>Assign tasks to each team member accordingly with specific processes, functions, areas or activities.</td>
<td>[3] [14] [6] [39]</td>
</tr>
<tr>
<td>Perform a close meeting to present the audit findings and main conclusion to audited entity</td>
<td>[3] [14] [6] [39] [38]</td>
</tr>
</tbody>
</table>

As table shows, for each activity we provide more than one reference to have a strongly justification for each one.

D. 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 II, III and IV in order to relate them and provide a complete support to the BPMN’s design. In Table V we provide an example of the relationships between the referred tables.

<table>
<thead>
<tr>
<th>Phases</th>
<th>Sub-phases</th>
<th>Responsibility/ Activities</th>
<th>Roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Planning</td>
<td>Establish audit objectives</td>
<td>Plan and agree audit requirements</td>
<td>Audit Manager</td>
</tr>
<tr>
<td></td>
<td>Establish audit scope and schedule</td>
<td>Write an audit plan which must describe the objectives</td>
<td>Audit Manager</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Determine the feasibility of the audit accordingly with the existent time and resources</td>
<td>Audit Manager</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Schedule audit and include this information in the audit plan document</td>
<td>Audit Manager</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Write an audit plan that must describe the scope of an audit</td>
<td>Audit Manager</td>
</tr>
</tbody>
</table>

Now we have the basis for our process design since Table V includes a complete decomposition of the process. Now, based in all above constructs, we present the reached IT AM process which is composed by several sub-processes that will not be detailed in this section given to space limitations. Figure 1 gives a small example.

In Figure 1 it possible to observe the sub-phases (sub-processes), roles (actors) and tasks (activities).
E. IT Audit Management Information Architecture

Nowadays, organizations perceive the importance of linking business architecture to IA [40]. With this linkage, it is possible to manage the changes needed by the business and maximize the benefits from the IT investments [40]. 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 [43].

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

Informational entities are the basis for the information architecture since they 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 previous sub-section. Table VI shows an example of the achieved entities.

<table>
<thead>
<tr>
<th>Entities</th>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Objectives</td>
<td>Objectives Description</td>
<td>Describe the objectives of an audit</td>
</tr>
<tr>
<td>Scope</td>
<td>Scope Description</td>
<td>Describe the scope of an audit such as physical locations, organizational units, activities and processes to be audited</td>
</tr>
</tbody>
</table>

The table also shows the identifiers of each entity.

F. IT Audit Management Information Systems Architecture

Information systems architecture focuses on identifying and defining the applications and data considerations. In order to define consistently the necessary applications to support the processes, we present a section of the CRUD matrix (Figure 2) that relates IT AM sub-processes with informational entities.

Figure 2. CRUD Matrix

The integration between applications was represented in the form of arrows

VI. Evaluation

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 petri-nets (PN). More specifically we use Yawl-nets which provide the same benefits of PN 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 (we don’t provide more details in this document).

A. Petri-Nets

The modeling language used was BPMN. However, the specification of BPMN notation does not include formal semantics [44, 45]. So, in our evaluation we used YAWL net which is a state-based language [45] that solves these limitations [46]. We convert the BPMN’s to Yawl nets and using the Yawl 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 [47].
The Yawl editor didn’t find problems in any net which give us the certain that our process is formally well developed.

B. Interviews

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.

With the interviews, we can draw some conclusions that provide insight into the current IT AM process. In Table VII we provide and example of the raised conclusions and the interviewees that supported them.

<table>
<thead>
<tr>
<th>Conclusion</th>
<th>Interviewees</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit objectives must be established according to the management’s needs.</td>
<td>1, 2, 3, 4, 5, 7</td>
</tr>
<tr>
<td>When a new audit begins, the audit team should assess information about</td>
<td>2, 3, 4, 5, 7</td>
</tr>
<tr>
<td>the oldest audits that may help to conduct the new one.</td>
<td></td>
</tr>
</tbody>
</table>

As we see, the reached conclusions are high level detailed since the respondents are not auditors. With these conclusions we raised a set of requirements that our process should implement.

C. 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.

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 [11]. The factors proposed in the Moody and Shanks framework are: completeness, integrity, flexibility, understandability, correctness, simplicity, integration and Implementability.

With the questionnaires we raise some conclusions. In table VIII

<table>
<thead>
<tr>
<th>Conclusion</th>
<th>Factor</th>
<th>Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>It is complete but to implement, organizations need to complement some</td>
<td>Completeness</td>
<td>IT AM Process</td>
</tr>
<tr>
<td>parts of the process accordingly with the type of audit</td>
<td></td>
<td>IT AM IS Architecture</td>
</tr>
<tr>
<td>The information listed is sufficient to perform the audit. But it is</td>
<td>Completeness</td>
<td>IT AM IS Architecture</td>
</tr>
<tr>
<td>necessary to understand that in reality the entity “Evidences” can be</td>
<td></td>
<td></td>
</tr>
<tr>
<td>any type of informations, so represent them as a unique entity can be</td>
<td></td>
<td></td>
</tr>
<tr>
<td>an abuse.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>It can be necessary to access other applications that don’t belong to</td>
<td>Completeness</td>
<td>IT AM IS Architecture</td>
</tr>
<tr>
<td>audit department.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
We also explain the changes made in our proposal in order to solve some problems that practitioners founded but here we don’t provide details about them due to the space limitations.

VII. 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. 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 & Shank 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 [48] 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 [17] was fulfilled too (frameworks overlap each other). Finally, also the limitations pointed by Rosário, Pereira and Mira da Silva [8] 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 the hypothesis of this thesis is confirmed. 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.

A. 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 based on both theoretical and practitioners’ viewpoints;
2. The formalizations of the IT AM Process taking into consideration the best of each framework.
3. We demonstrated that our IT AM Process is formal which proves its strong empirical validation.

B. 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 bigger 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.

C. Learning’s

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.

D. 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


