



Universidade do Minho

Escola de Engenharia

Rui Pedro Figueiredo Marques

**Organisational Transactions with
Embedded Control**

**Programa de Doutoramento em Informática das
Universidades do Minho, de Aveiro e do Porto**



Universidade do Minho

This work was carried out under supervision of

Professor Henrique Manuel Dinis dos Santos

and

Professor Carlos Alberto Lourenço dos Santos

October 2014

The partial reproduction of this thesis is authorised only for research purposes, by written declaration of commitment by the interested party.

É autorizada a reprodução parcial desta tese, apenas para efeitos de investigação, mediante declaração escrita do interessado, que a tal se compromete.

University of Minho, 31 October 2014

Signature: _____

STATEMENT OF INTEGRITY

I hereby declare having conducted my thesis with integrity. I confirm that I have not used plagiarism or any form of falsification of results in the process of the thesis elaboration.

I further declare that I have fully acknowledged the Code of Ethical Conduct of the University of Minho.

University of Minho, 31 October 2014

Full name: Rui Pedro Figueiredo Marques

Signature: _____

*For my wife Carla
and for my son Salvador Filipe:
without you none of this would make sense.*

*Para a minha esposa Carla
e para o meu filho Salvador Filipe:
sem vocês nada disto faria sentido.*

AKNOWLEDGEMENTS

Although a doctorate is, by its academic purpose, an individual work, there are several kinds of contributions which must be highlighted. For this reason, I would like to express my heartfelt thanks to:

- Professor Henrique Santos by his valuable supervision and support in this work, as well as the learning he has transmitted to me until today;
- Professor Carlos Santos by his guidance, availability, encouragement and friendship from the very beginning;
- the Higher Institute of Accounting and Administration of the University of Aveiro which has greatly contributed to the success of this work because of the time allowed and the authorisation to use essential resources for the implementation of this work. I am grateful to everyone in this institute who have directly or indirectly contributed to make all of this possible;
- my parents because they have been and will always be a reference to my personal and professional education. In difficult times, they have showed me examples of persistence and dedication in their lives which I have always taken as references to follow;
- family members, friends and colleagues who have always been present to make my life more beautiful and easier;
- my wife, by the numerous exchanges of views, comments and criticisms to the work. Above all, by the invaluable support that has filled several gaps due to the circumstances, and by the patience and understanding revealed throughout these years;
- and to my son who was born during this process and has given me a strong vision that a brighter and happier future is always possible.

I am grateful to you all.

ORGANISATIONAL TRANSACTIONS WITH EMBEDDED CONTROL

ABSTRACT

The current highly regulated business environment has imposed organisations to increase their effort to monitor and manage their control mechanisms. This awareness has been propelled by the increasing emergence of new regulatory requirements on continuous monitoring and continuous auditing of organisational transactions. Furthermore, the successive well-known scandals in organisations, which have resulted in a very negative impact on their operational performance and also on their corporate image, have shown that the traditional audit process is not sufficient to meet the organisations' needs.

Thus, organisations have been looking for solutions to improve and strengthen their risk control structures so as to provide greater security in the effectiveness of risk management of their activities, namely on controlling, monitoring and auditing of organisational transactions. Then, the concept of Continuous Assurance has emerged because it is the set of services which, making use of technology, uses the information immediately from organisational transactions and produces audit results simultaneously or within a short period of time after the occurrence of relevant events.

Hence, this thesis focuses on the implementation of continuous assurance services in information systems in order to determine the degree of reliability with which transactions are carried out, mitigating the organisational risk. Therefore, this thesis aims to contribute to a new vision of organisational auditing focused on assurance services in transactions executed and supported exclusively in a digital format according to an ontological model of organisational transactions.

The motivation and objective of this thesis led to some research challenges:

- Validate a set of characteristics that any information system with continuous assurance services must provide. The literature on this topic is not very explicit upon the metrics which should be taken into consideration during the evaluation of this type of information systems. Thus, the Delphi method was used to validate a set of essential and very important characteristics for information systems with continuous assurance. In addition, this work

contributes with a model comprising dimensions and metrics, which allows it to be used as a tool or as a set of guidelines to evaluate information systems with embedded control.

- Ensure the feasibility of development and the effective use of an information system with full continuous assurance services, having as support an ontological model, and which is considerably flexible and adaptable in order to be applicable to any organisational transactions. Following the Design Science methodology, a proposal of a solution is presented. This proposal includes requirements, a modular architecture and the development of a prototype. All these steps were supported by an ontological model of organisational transactions so that they could be represented in a very detailed, objective and comprehensive way. Furthermore, the solution was implemented in a simulated organisational environment and its results allow to conclude that the presented architecture is an effective solution since it provides continuous assurance to any organisational transactions, having as support an ontological model. Moreover, this work demonstrates that a repository which allows the instantiation of execution patterns (risk profiles) for each organisational transaction is an important element in information systems with continuous assurance services, as a source of references to support continuous monitoring, auditing and controlling of the risk associated with the execution of organisational transactions.

KEYWORDS: organisational transactions; continuous assurance; management information system; risk profiles.

TRANSAÇÕES ORGANIZACIONAIS COM CONTROLO EMBEBIDO

RESUMO

O atual contexto organizacional e de negócios está altamente regulado e tem imposto às organizações o aumento dos seus esforços para monitorizar e gerir os seus mecanismos de controlo. A consciência sobre esta realidade tem sido impulsionada pelo crescente aparecimento de novas exigências regulamentares sobre a monitorização e auditoria contínua das transações organizacionais. Além disso, os sucessivos escândalos de algumas organizações, que tão bem são conhecidos, e que resultaram num impacto muito negativo sobre seu desempenho operacional e, também, na sua imagem corporativa, têm demonstrado que o processo de auditoria tradicional não é suficiente para atender às atuais necessidades das organizações.

Assim, as organizações têm procurado soluções para melhorar e reforçar as suas estruturas de controlo de risco, de modo a proporcionar maior segurança na eficácia da gestão de risco das suas atividades, ou seja, no controlo, monitorização e auditoria das transações organizacionais. Então, o conceito de *Continuous Assurance* tem vindo a emergir porque refere-se ao conjunto de serviços que, fazendo uso da tecnologia, utiliza imediatamente a informação proveniente de transações organizacionais e produz resultados da auditoria, simultaneamente, ou, dentro de um curto período de tempo após a ocorrência de eventos relevantes.

Deste modo, esta tese centra-se na implementação de serviços de *Continuous Assurance* em sistemas de informação, a fim de determinar o grau de confiabilidade com que as transações são executadas, mitigando, assim, o risco organizacional. Portanto, esta tese pretende contribuir para uma nova visão de auditoria organizacional focada em serviços de *Continuous Assurance* em transações realizadas exclusivamente em formato digital, e em concordância com um modelo ontológico de transações organizacionais.

A motivação e objetivo desta tese levantou alguns desafios de investigação:

- A validação de um conjunto de características que qualquer sistema de informação com serviços de *Continuous Assurance* deve fornecer. A literatura sobre o tema não é muito explícita sobre as métricas que devem ser consideradas na avaliação deste tipo de sistemas de informação. Assim,

o método Delphi foi utilizado para validar um conjunto de características essenciais, e muito importantes, para sistemas de informação com serviços de *Continuous Assurance*. Além disso, este trabalho contribui com um modelo que inclui dimensões, requisitos e métricas, o que lhe permite ser utilizado como uma ferramenta ou como um conjunto de linhas de orientação para avaliar sistemas de informação com controlo embebido.

- A verificação da viabilidade de desenvolvimento e uso eficaz de um sistema de informação com serviços completos de *Continuous Assurance*, tendo como suporte um modelo ontológico, pretendendo ser um sistema bastante flexível e adaptável, a fim de ser aplicável a quaisquer transações organizacionais. Para tal, é apresentada uma proposta de solução seguindo a metodologia *Design Science*. Esta proposta inclui a apresentação de requisitos, de uma arquitetura modular, e do desenvolvimento de um protótipo. Todos estes passos foram apoiados por um modelo ontológico de transações organizacionais, para que estas possam ser representadas de forma detalhada, objetiva e abrangente. Além disso, a solução foi implementada num ambiente organizacional simulado e os seus resultados permitem concluir que a arquitetura apresentada é uma solução eficaz, uma vez que fornece serviços de *Continuous Assurance* às transações organizacionais. Além disso, este trabalho demonstra que um repositório que permita a instanciação de padrões de execução (perfis de risco) para cada transação organizacional, é um elemento importante em sistemas de informação com serviços de *Continuous Assurance* e visto como uma fonte de referências para apoiar a monitorização e auditoria contínua, e o controlo do risco associado à execução das transações organizacionais.

PALAVRAS-CHAVE: transações organizacionais; *Continuous Assurance*; sistemas de informação para a gestão; perfis de risco.

CONTENTS

| | |
|---|------|
| Aknowledgements..... | vii |
| Organisational Transactions with Embedded Control | ix |
| Transações Organizacionais com Controlo Embebido | xi |
| Contents | xiii |
| Index of Figures | xv |
| Index of Tables..... | xvii |
| List of Acronyms | xix |
| 1 Introduction | 1 |
| 1.1 Motivation | 3 |
| 1.2 Research Setting | 5 |
| 1.2.1 Related Work | 5 |
| 1.2.2 Research Problem | 15 |
| 1.2.3 Research Questions..... | 19 |
| 1.2.4 Research Methodology | 21 |
| 1.3 Objectives..... | 23 |
| 2 Fundamental Concepts | 25 |
| 2.1 Continuous Assurance..... | 27 |
| 2.1.1 Introduction..... | 28 |
| 2.1.2 Characteristics..... | 30 |
| 2.1.3 Objectives | 36 |
| 2.1.4 Constitution..... | 39 |
| 2.2 Conceptual Model of Transaction | 43 |
| 2.2.1 Introduction..... | 44 |
| 2.2.2 Ψ-THEORY | 48 |
| 3 Characteristics of Continuous Assurance | 61 |
| 3.1 Introduction | 61 |
| 3.2 Dimensions and Requirement of the Evaluation Model..... | 65 |
| 3.3 Model Validation..... | 70 |
| 3.3.1 The Delphi Method..... | 70 |
| 3.3.2 Evaluation Instrument..... | 79 |

| | | |
|-------|---|-----|
| 3.3.3 | Application of Delphi Method..... | 96 |
| 3.4 | Conclusion..... | 103 |
| 4 | Solution Proposal | 106 |
| 4.1 | Conceptual Design | 106 |
| 4.1.1 | The role of Enterprise Ontology | 115 |
| 4.2 | Solution Development..... | 117 |
| 4.2.1 | Internal Control Mechanisms..... | 117 |
| 4.2.2 | Real Online Transaction Repository..... | 119 |
| 4.2.3 | Risk Profiles Repository | 122 |
| 4.2.4 | Transaction Comparator and Outputs | 126 |
| 4.3 | Implementation..... | 141 |
| 4.3.1 | Object of Study | 141 |
| 4.3.2 | Methods | 150 |
| 4.4 | Results | 158 |
| 5 | Validation of Research Questions and Hypotheses | 171 |
| 6 | Conclusion and Future Work..... | 187 |
| | References..... | 193 |
| | Appendixes | 207 |
| | Appendix A – Questionnaires | 208 |
| | Appendix B – Pre-Test..... | 223 |
| | Appendix C – E-mails..... | 241 |
| | Appendix D – Results of Questionnaires..... | 245 |

INDEX OF FIGURES

| | |
|---|-----|
| Figure 1 - Continuous Monitoring, Auditing and Assurance (conceptual model) | 35 |
| Figure 2 - Continuous Assurance | 39 |
| Figure 3 - White-box model of an organisation..... | 50 |
| Figure 4 - Basic pattern of an organisational transaction | 51 |
| Figure 5 - Standard pattern of an organisational transaction | 51 |
| Figure 6 - Representation of the Distinction Axiom | 53 |
| Figure 7 - Ontological models | 55 |
| Figure 8 - Example of a Process Model | 56 |
| Figure 9 - Example of an Action Model | 57 |
| Figure 10 - Example of a State Model | 58 |
| Figure 11 - Example of a Construction Model | 59 |
| Figure 12 - Relationship between the proposed dimensions and CA..... | 63 |
| Figure 13 - Dimensions of the evaluation model..... | 64 |
| Figure 14 - Dimensions and requirement of the model and their metrics | 69 |
| Figure 15 - Flowchart of classic process of Delphi method | 73 |
| Figure 16 - Participants of pre-test by area..... | 86 |
| Figure 17 - Experience of participants of pre-test | 86 |
| Figure 18 - Scientific publications of participants of pre-test | 86 |
| Figure 19 - Status of answers of request for collaboration by area | 93 |
| Figure 20 - Composition of the Panel of Experts by Area | 94 |
| Figure 21 - Composition of the panel of experts by area (answers by experts) | 97 |
| Figure 22 - Experience of experts (answers by experts)..... | 97 |
| Figure 23 - Conceptual architecture of the proposed solution..... | 113 |
| Figure 24 - High-level relationship of internal control mechanisms and the Real Online Transaction Repository..... | 119 |
| Figure 25 - Entity-relationship model of the Real Online Transaction Repository | 121 |
| Figure 26 - Physical Model of the Real Online Transaction Repository | 123 |
| Figure 27 - Entity-relationship model of the Risk Profiles Repository | 125 |
| Figure 28 - Physical model of the Risk Profiles Repository | 127 |
| Figure 29 - Architecture of Transaction Comparator module | 128 |
| Figure 30 - Relationship between repositories | 129 |
| Figure 31 - Flowchart of Transaction Comparator | 131 |
| Figure 32 - Diagram of classes of the logic layer of Transaction Comparator module..... | 132 |

| | |
|---|-----|
| Figure 33 - High-level description on loading sequences of related operations (transactions) | 134 |
| Figure 34 - High-level description of the operation of the Transaction Comparator evaluating the executed transactions..... | 136 |
| Figure 35 - Conceptualisation of the interface of the system..... | 138 |
| Figure 36 - Interaction Model of a possible risk profile of a commercial transaction | 145 |
| Figure 37 - Legend for interpreting the process model | 145 |
| Figure 38 - Process model of a possible risk profile of a commercial transaction..... | 147 |
| Figure 39 - Boxplot of the interval of time of operations detection | 166 |
| Figure 40 - Boxplot of the interval of time of sending an e-mail alert..... | 167 |
| Figure 41 - Print screen of the interface of the prototype..... | 168 |
| Figure 42 - Amendments to the questionnaire (question 5) | 239 |

INDEX OF TABLES

| | |
|--|-----|
| Table 1 - Authors of publications on Continuous Assurance | 27 |
| Table 2 - Authors of publications on Conceptual Model of Organisational Transactions | 43 |
| Table 3 - Objectives and components of Continuous Assurance | 62 |
| Table 4 - Metrics included in the first version of the questionnaire | 80 |
| Table 5 - Metrics included in the final version of the questionnaire | 87 |
| Table 6–Status of answers of request for collaboration by area | 93 |
| Table 7 - Consensus definition (using a 5 score scale)..... | 95 |
| Table 8 - Criteria for classification of the level of consensus | 95 |
| Table 9 - Dimensions and requirement of the model and their metrics after validation | 105 |
| Table 10 - Relationship between functional requirements, development considerations and the considered metrics of Continuous Assurance..... | 112 |
| Table 11 - Risk profiles defined in the Risk Profiles Repository | 149 |
| Table 12 - Indicators considered in the analysis of the reports of the prototype | 151 |
| Table 13 - Number of transactions, operations and analyses carried out during the case study | 159 |
| Table 14 - Number of risk profiles analysed by type | 159 |
| Table 15 - Table of frequencies of State 0..... | 163 |
| Table 16 - Table of frequencies of State 1..... | 163 |
| Table 17 - Table of frequencies of State 2..... | 163 |
| Table 18 - Table of frequencies of the interval of time of operations detection..... | 166 |
| Table 19 - Table of frequencies of the interval of time when sending an e-mail alert..... | 167 |
| Table 20 - Amendments to the questionnaire (question 2)..... | 238 |
| Table 21 - Amendments to the questionnaire (question 6)..... | 238 |
| Table 22 - Amendments to the questionnaire (question 1)..... | 239 |
| Table 23 - Distribution of answers of participants for Part I of questionnaire (1 st iteration)... | 246 |
| Table 24 - Distribution of answers of participants for Part II of questionnaire (1 st iteration) . | 247 |
| Table 25 - Distribution of answers of participants for Part I of questionnaire (2 nd iteration).. | 248 |
| Table 26 - Distribution of answers of participants for Part II of questionnaire (2 nd iteration) | 249 |
| Table 27 - Statistical data from answers for Part I of questionnaire (1 st iteration) | 250 |
| Table 28 - Statistical data from answers for Part II of questionnaire (1 st iteration)..... | 251 |
| Table 29 - Statistical data from answers for Part I of questionnaire (2 nd iteration) | 252 |
| Table 30 - Statistical data from answers for Part II of questionnaire (2 nd iteration)..... | 253 |

LIST OF ACRONYMS

| | |
|---------|---|
| AICPA | American Institute of Certified Public Accountants |
| BAM | Business Activity Monitoring |
| BPM | Business Process Management |
| CAAT | Computer Assisted Auditing Techniques |
| CCM | Continuous Controls Monitoring |
| CCM-AC | Continuous Controls Monitoring for Application Configuration |
| CCM-MD | Continuous Controls Monitoring for Master Data |
| CCM-SOD | Continuous Controls Monitoring for Segregation of Duties |
| CCM-T | Continuous Controls Monitoring for Transactions |
| CDA | Continuous Data Assurance |
| CEP | Complex Event Processing |
| CICA | Canadian Institute of Chartered Accountants |
| COBIT | Control Objectives for Information and Related Technology |
| COSO | Committee of Sponsoring Organisation of the Treadway Commission |
| CRMA | Continuous Risk Monitoring and Assessment |
| DBMS | Database Management System |
| DEMO | Design & Engineering Methodology for Organisations |
| DSMS | Data Stream Management System |
| ECA | Event Condition Action |
| ER | Entity-Relationship |
| ERP | Enterprise Resource Planning |
| IFAC | International Federation of Accountants |
| IIA | Institute of Internal Auditors |
| IQD | Interquartile Distance |
| ORM | Object-Role Modelling |
| IT | Information Technology |

| | |
|------|--|
| QoS | Quality of Service |
| SOX | Sarbanes-Oxley Act |
| SQL | Structured Query Language |
| XBRL | eXtensible Business Reporting Language |

1

INTRODUCTION

In the current context organisations face several challenges. Namely at the transactional level it has been found that organisational transactions have grown in volume and complexity (Verver, 2003). Organisational transaction means the simplest form of transformation, that is to say the building block of the processes which make up the organisation (C. Santos, 2009).

On the other hand, organisations are living in highly regulated business environments where a sustained effort to monitor and manage their control mechanisms is needed. However, the traditional audit process occurs mostly after the completion of transactions, which is not feasible to evaluate and validate all transactions in a comprehensive manner to meet the controls and regulations. Therefore, for many organisations there is a significant risk of errors and fraud and these are not detected in time, resulting in a negative impact on organisations, see, for example the current global financial crisis and successive well known scandals in some organisations, such as Lehman Brothers, A-Tec, Madoff, Kaupthing Bank, WorldCom, Enron, Parmalat and Tyco cases and many others (Bodoni, 2014; Cohen, Ding, Lesage, & Stolowy, 2010; Markham, 2006; Verver, 2003).

In addition, the increasing emergence of new regulatory requirements on this topic has made the trend and the need for improvement and strengthening of risk control structures grow in order to provide greater security in the effectiveness of risk management activities of the organisations, ensuring an appropriate management of key business risks and the effective operation of internal control systems (Morais, 2008).

The Sarbanes-Oxley Act, better known as SOX, (SOX, 2002) is one of the most well-known regulations, created in the United States of America in 2002 and motivated by corporate financial scandals, which aims to ensure the creation of

auditing mechanisms and reliable security organisations in order to mitigate the risks associated with organisational transactions, preventing fraud or ensuring that there are ways to identify them when they occur, thus ensuring transparency in the management of organisations.

Prior to SOX, there are other models and frameworks of reference, such as the COSO (Committee of Sponsoring Organisations of the Treadway Commission) and COBIT (Control Objectives for Information and related Technology). COSO is a U.S. joint initiative of private sector organisations for avoiding scams in the financial accounting of organisations dedicated to improving report securities, especially in the application of ethics and efficiency and in compliance with internal controls (L. Silva & Machado, 2008). COBIT is an internationally accepted IT (Information Technology) control framework that provides organisations with good practices that help in implementing an IT governance structure throughout the enterprise. This framework aims to bridge the gaps between business risks, control needs, and technical issues, providing the information that the organisation needs to attain its objectives and the reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected (Lankhorst, 2013). In Europe measures for the statutory auditing were also taken by Directive 2006/43/CE of the European Parliament and of the Council of 17th May 2006, transposed to Portuguese law by Decree-Law 224/2008 and 225/2008, both of 20th November, helping to improve the integrity and efficiency of financial statements and, accordingly, enhance the orderly functioning of markets.

Thus, any organisation must be sufficiently prepared to survive, regardless of exposure and of the large number of risks which is subject to by implementing an adequate system of Continuous Assurance in accordance with applicable legislative and regulatory framework. Continuous Assurance is presented as a set of services that using technology and data transactions produces audit results simultaneously or within a short period of time after the occurrence of relevant events.

1.1 MOTIVATION

As aforementioned in the introductory section, we are facing a scenario where there is the need to ensure that the execution of transactions is based on organisational records which are reliable and made in accordance with the objectives of organisations and in compliance with the internal and external regulations. With the emergence and great adhesion to ERP (Enterprise Resource Planning) systems since the last two decades, there was another concern: how can the transactions executed only on a digital format be audited, ensuring them a reliable character? According to the theory of auditing, an organisation does not only need an information system but also a system of internal control to ensure reliability of the recorded information and to control possible errors (Weigand & Moor, 2003). To this end, systems and controls have been developed, which when incorporated into the platform on which transactions are executed, facilitate the operations of auditing and monitoring. However, these controls should be tailored to the needs and to the level of risk tolerance of each transaction to be monitored and audited.

Along with this evidence, a study by PricewaterhouseCoopers (2007) examined various organisations and concluded that about 89% of participating organisations intended to adopt more solutions of Continuous Auditing and monitoring by 2012. Of this total, about 49% claimed to have these solutions fully implemented and operationally functional, and 35% expected that these solutions were under development. The tools of detection and prevention of fraud and of risk analysis and management are on the top of intentions with 81% and 71% respectively.

These aspects have propelled to create a new awareness of corporate governance and of the growing importance of monitoring and controlling the various organisational transactions. Organisational transaction means any activity performed within a business process of any organisation. And for this reason, to monitor and control organisational transactions means to analyse the state of the actions which are part of these transactions. The main objective of controlling and monitoring is to support the audit process (evaluate and validate) of the various transactions in order to detect any negative behaviours, (improper or incomplete operations, lack of crucial

procedures, unconformities, delays, incongruities and malfeasance) determining the degree of reliability with which organisational transactions are carried out.

Therefore, it is necessary to find solutions which allow organisations to evaluate monitor and validate their transactions continuously, and independently, preferably in a non-intrusive way. If this auditing is done in real time (in the shortest time possible after its execution) with some control mechanisms implemented and embedded in organisational transactions, it will be possible, in addition to evaluate and validate, to optimise the operational performance reducing the associated risks.

The main motivations of this thesis are those aspects of security and control of digital data and the mechanisms of internal control, which ensure reliability to transactions and to organisational information. These motivations have led the survey on the work related to this topic, which appears below, in order to understand what has been investigated and implemented at the level of monitoring, auditing and controlling of organisational transactions, especially those which are performed on digital records.

1.2 RESEARCH SETTING

This section is structured in four parts in order to contextualise the research inherent to this thesis, namely: Related Work, Research Problem, Research Questions and Research Methodology.

The section Related Work gives an overview about some paradigms and concepts associated with the monitoring and auditing at the level of execution of the organisational transactions and processes. Some researches and applications related to the topic are also presented. Thus, the concepts and works which are here evinced are contributes which help to recognise the comprehensiveness of the subject of this thesis. This section also helps to understand the problem domain and some issues which have been raised over the years in order to provide organisations with better solutions and services which continuously assure the reliability of their transactions.

The section Research Problem presents the issues that the extent literature review on related works upon this topic arose and the definition of the problem that is considered to be studied and researched in this thesis.

The section Research Questions identifies a set of questions and hypotheses which this thesis intends to answer through the validation of the research hypotheses. Furthermore, these research questions, hypotheses and their responses and validation constitute the scientific contributions of this thesis.

Finally, the section Research Methodology presents the methods which were used to carry out this research, specifying the different methods for every research questions and hypotheses.

1.2.1 Related Work

This section, as the name suggests, makes a brief state of the art on various topics related to the motivation of this thesis. Thus, this section begins by presenting some of the most significant risks an operational information system can be prone to and in which it can play a part within an organisation, based on the experiences of controlling and auditing of organisational information systems. Subsequently, some concepts associated with systems or mechanisms which have emerged with the

objective to address these organisational risks are presented as well as some cases of real application and their results. Hence, this section gives an overview of the main topics related to the theme of this thesis.

Musaji (2002) has identified a list of negative situations that operational information systems are vulnerable to during the execution of organisational transactions, and stated that some attentiveness is needed when you want to implement a system of monitoring, auditing and controlling of organisational risk. These negative situations are:

- Erroneous or falsified data input - the false or wrong data entry is the most common cause of undesirable results in an application. Vulnerabilities occur wherever data is collected, manually processed, or prepared for entry to the computer. Some examples of this situation: inconsistent source data values may be undetected; incomplete or poorly data records may be accepted as if they were complete records; records in one format may be interpreted according to a different format; an user of the system may fraudulently add, delete, or modify data to obtain benefits; lack of document operations may allow some of the data or transactions to be lost without detection or allow extra records to be added; records about the data entry personnel may be modified during data entry; data that arrive at the last minute or under emergency condition may not be verified prior to processing; records in which errors have been identified may be revised without verification of the full record.
- Misuse by authorised end users - it may happen that a user does not use the system in accordance with the legitimate exercise of their duties. Some examples of this situation: a user of the system may convert confidential information to an unauthorised use; a user whose job requires access to individual records in a file may compile a complete list of the file and then make unauthorised use of it; information may be altered by an unauthorised end user; an authorised user may use the system for personal benefit; a supervisor may manage to accept and enter a fraudulent transaction; a

dissatisfied employee may destroy or modify records, possibly in such a way that backup records are also corrupted and useless; an authorised user may accept a bribe to modify or obtain information.

- Uncontrolled system access - organisations expose themselves to risks if they do not set controls regarding the access to the system and data. Some examples of this situation: data or programs may be stolen or destroyed; individuals may not be adequately identified before they are allowed to enter the IT area; remote terminals may not be adequately protected from unauthorised users; an unauthorised user may access to the system via an authorised user's password; passwords may be inadvertently revealed; a user may leave a logged-in terminal unattended.
- Ineffective security practices for the application, like for example, poorly defined criteria for authorised access; repeated payments to the same party may go unnoticed because there is no review; inadvertent modification or damage of data may occur when trainees are allowed to work on live data.
- Communications system failure - information being transmitted over communication lines is vulnerable to accidental failures and to intentional interception and modification by unauthorised parties.
- Intentional acts, like for example, communication lines may be monitored by unauthorised individuals; data may be intentionally changed by individuals tapping the line (requires some sophistication, but it is applicable to financial data); false data may be inserted into the system and true data may be deleted from the system.

Considering the possible risks identified, control measures have been provided in order to mitigate the negative effects associated with these situations of organisational risk. Some information systems already have some specific and personalised mechanisms of controlling and monitoring embedded in order to protect their information resources (including hardware, software, firmware and data) from all threats and risks, ensure accuracy and reliability of data held or generated by operational information systems and ensure operational reliability, as well as the

accurate and timely performance of the system. The objectives of these control mechanisms are various (Musaji, 2002):

- authorisation (transactions are properly authorised);
- timeliness (transactions are performed on a timely basis);
- accuracy (transactions are accurately processed);
- completeness (all existing transactions are recorded);
- validity (all recorded transactions are valid);
- classification (transactions are properly classified);
- reporting (transactions are properly summarised and reported);
- security (assets, including software programs, data, human resources, computer facilities, etc. are safeguarded against damage, theft, and so forth);
- integrity (system and data integrity is maintained);
- availability (system availability is assured);
- controlling and auditing (system controlling and auditing is maintained);
- maintenance (system maintenance is assured);
- usability (system usability is assured);
- efficiency (system economy and efficiency are maintained).

In addition to the internal control mechanisms specific to each information system, other systems, solutions and concepts, have emerged to address this need of organisational controlling, monitoring and auditing. The first two concepts intended to refer are BAM (Business Activity Monitoring) and BPM (Business Process Management). BAM (McCoy, 2002) allows that events generated by various applications and systems of an organisation, or by services of inter-organisational cooperation, can be processed in real time in order to identify critical situations in the performance indicators, with the aim to obtain a better insight into the business activities, and thus improving their effectiveness. BAM identifies and analyses in real time the cause-effect relationships between events, enabling the system and/or staff to take effective and proactive measures in response to specific identified scenarios, allowing, for example: the early detection of abnormal events in business processes as

a whole, or some of their constituent parts; identification of poorly designed business processes; analysis of occurred failures and the respective impacts on business processes, infrastructure, applications or flows; risk assessments which help to predict the compliance of various organisational situations, such as deadlines, insufficient data or failure rates; the automatic deduction of action plans; provision of information organised by implementing customised dashboards for rapid understanding of problematic or decision making situations; and definition and implementation of alerts for better control of operational risks in real time, allowing faster reactions in specific situations (Brandl & Guschakowski, 2007; McCoy, 2002).

In turn, according to Van der Aalst *et al.* (2003), BPM is defined as “supporting business processes using methods, techniques and software to design, enact, control and analyse operational processes involving humans, organisations, applications, documents and other sources of information”. The BPM systems are complex assemblies of software components and tools that together provide features which allow us to develop, deploy and implement solutions based on business processes. Moreover, they enable the visualisation, monitoring and management of events within the business process, and allow the highest-level visualisation of the state of the execution of business processes, reducing the causes of the occurrences of exceptions (Brandl & Guschakowski, 2007).

Another interesting concept to present here is CEP (Complex Event Processing), which includes methods, techniques and tools to process events in real time. CEP analyses a series of data in real time and identifies patterns and generates events that can be processed and treated. This processing is done in memory and its logic is defined by a series of queries on all received data (Oliveira, 2011; Roth, Schiefer, Obweger, & Rozsnyai, 2010). CEP provides a paradigm to collect and process data flowing through an organisation in real time in order to automate and accelerate decision cycles, facilitating an agile approach to keep the underlying business logic adaptable to changing business needs. It is useful knowledge obtained from high-level, taking the low-level events as a starting point. (Roth et al., 2010).

However, CEP had its roots in the communities of active databases (Rizvi, 2005; Wiederkehr, 2007; Zimmer & Unland). These communities have developed concepts

such as ECA (Event Condition Action) and DSMS (Data Stream Management System). The ECA rules are based on the detection of specific events without user intervention or external applications, by automating the database engine in such a way that, under the pre-established rules, it would be able to evaluate the conditions faced to input events, and if the condition was true, actions would triggered in response of these events (Dayal, Hsu, & Ladin, 1990; Joonsoo, Hyerim, Suk-Ho, & Yeongho, 2004). The use of the DSMS for managing a data stream is similar to DBMS (Database Management System) for managing a conventional database. Typically, a query to a database is executed once, returning a result set for a given period in time. In contrast, a DSMS runs a continuous query on the data flow and the results are thus always up to date throughout the production of events (D. J. Abadi et al., 2003; Arasu et al., 2004). Subsequently, the CEP has been implemented in several areas: BAM, BPM, among others. While the CEP employs the "inbound" approach to process the flow of events as a source of input data, in contrast, the databases take an "outbound" processing approach. The difference lies in the fact that while the "outbound" processing requires the storage of all data prior to processing, the first one enables data to be processed as soon as they are received and then stored (Oliveira, 2011; Roth et al., 2010).

In short, CEP is capable of processing high amount of data from different sources; operates in bitstream; has low latency; has limited processing window and can handle different types of operations on data, such as filtering, correlation, aggregation and association patterns.

Researchers from the Brandeis University, Brown University, and Massachusetts Institute of Technology carried out the project Aurora (D. J. Abadi et al., 2003). This project was designed to handle and manage a very large amount of data streams and allows its users to create their own queries from a set of available operators. These operators are connected to other operators or may simply provide results. These operators may derive from the output data from other operators or external data sources. Aurora is capable of optimising the query considering the QoS (Quality of Service) indexes provided by the operators and other indexes and system inputs specified by the users. This was a precursor of other identical monitoring works of

data flow, e.g. Medusa (Balazinska, Balakrishnan, & Stonebraker, 2004) and Borealis (D. Abadi et al., 2005). Like Aurora, the project STREAM (Arasu et al., 2004) is a Data Stream Management System. The STREAM supports a large number of declarative continuous queries over continuous data streams and/ or over traditional data repositories. The monitoring is done by controlling the results of queries made.

The work EasyCredit (Brandl & Guschakowski, 2007; Greiner, Duster, Pouatcha, & Ammon, 2006) is an example of successful implementation in the banking sector. It is a system like BAM, using the concept of CEP and the pipeline used in the management and monitoring of credit transactions in real time.

Some works on this topic were also found. Here event monitoring is done using log records. Within this group of works surveyed, one of them uses mining tools and CEP to analyse records of a database log in real time, and presents the sequence and the model of the transactions analysed (Oliveira, 2011). Furthermore, using mining techniques on log records, the possibility of recognition of events was demonstrated. It is able to link events that are not associated a priori with any workflow or process model to a new model, in other words it contributes for the discovery of new process and transactional models (Ferreira & Gillblad, 2009).

Another work of reference (Ferreira, Alves, & Thom, 2011) describes an approach for automating the discovery of patterns of activity in organisational process models through an ontology. This discovery of patterns is done through a mapping between the elements collected in the processing of the process and the elements of the ontology. This is done primarily to verify if the process contains the necessary elements to meet the definition of each process pattern.

However, when we are discussing this subject it is indeed to mention the concept Continuous Assurance, because it approaches this problem domain in a very complete way, since it is directly related to continuous monitoring, continuous auditing and continuous risk assessment of organisational transactions.

Continuous Assurance is made up of three components: CCM (Continuous Controls Monitoring) to monitor the operation of internal control mechanisms; CDA (Continuous Data Assurance) to verify the integrity and validity of data; and CRMA (Continuous Risk Monitoring and Assessment) to estimate the risk. Indeed, this was a

moment that propelled a thriving research and developments in this area (M. Vasarhelyi, M. Alles, & K. T. Williams, 2010).

In 1999, the term Continuous Assurance began to arouse much interest when a joint committee of the AICPA (American Institute of Certified Public Accountants) and the CICA (Canadian Institute of Chartered Accountants), took up the issue of Continuous Assurance and defined the term as a set of services which enables independent auditors to provide written assurance on a subject matter using a series of auditors' reports issued simultaneously with, or a short period of time after, the occurrence of events underlying the subject (M. Vasarhelyi et al., 2010).

Some years later, in 2006, a Pricewaterhousecooper survey (PricewaterhouseCoopers, 2006) concluded that Continuous Assurance triggered corporate sensitivity to its adoption because in 2005 only 35% had a Continuous Auditing or monitoring processes in place or were planning to develop one, and this value increased to 50% in 2006. It is also interesting to observe that this survey registered that 56% of respondents said that their Continuous Auditing processes include both manual and automated elements, 41% indicated their processes are entirely manual, and 3% reported having fully automated processes. Relatively to the Continuous Auditing cycle, 57% respondents answered that it is quarterly, 34% focus on monthly monitoring activities, while only 9% focus on daily applications of their Continuous Auditing processes.

Another study in the same year by IIA (Institute of Internal Auditors) and ACL (ACL, 2006) also showed similar results: 36% of surveyed organisations confirmed that they implemented a Continuous Assurance approach in all their business processes or simply in some selected areas, and 39% intended to implement in the near future. However, there is an important conclusion to retain in this study, which states that regardless of the reasons that organisations may have had to neglect the continuing auditing in the past, the recent regulations, the stimulus for real time monitoring and reporting of financial information and the ability to automate the traditional audit methods have encouraged strongly its adoption.

In 2007, a review article (Brown, Wong, & Baldwin, 2007) on this subject included a survey of more than 60 articles on the topic covering several categories: motivation

for change, theoretical concepts, technology, applications, cost/benefit factors, and case studies. It can be concluded that Continuous Assurance was still a concept for most organisations and a goal for the future. The implementation of systems with continuous assurance services was residual when comparing with continuous monitoring and continuous auditing systems. These latter systems presented high levels of maturation regarding their implementation in the inquired organisations.

The issues discussed in relation to the motivations which are driving and revealing Continuous Assurance include: the growing of complexity and amount of data, the growing of electronic exchange of information and outsourcing, the integration of the value chain; reports available on Web and the users' desire for reliable information and disclosed more frequently, more timely and more detailed; XBRL (eXtensible Business Reporting Language) reports, and the need for disclosure of updated information imposed by the Sarbanes Oxley Act (section 409) (Brown et al., 2007).

Some products and solutions in the field of Continuous Assurance have been recently made available in the market. These solutions are mostly developed by well-established CAAT (Computer Assisted Auditing Techniques) manufacturers and vendors such as ACL, Caseware IDEA, Approva and Oversight Systems, which begin to position themselves in this still emerging market. Despite the fact that these vendors call their products as Continuous Assurance solutions, these products focus more on the component CDA. The implementation of CCM solutions is very complex due to significant differences in the types of business objects, process configurations and controls and then it is not cost-effective. Thus, these solutions have developed some very specific CCM sub-routines targeted at specific enterprise systems. The two pioneering offerings in this field, by Approva and VIRSA, were targeted at SAP. Approva has extended its offerings to target other ERP systems (e.g. Oracle E-Business Suite). Such extensions are quite laborious since they require customisation for each new enterprise system (M. Vasarhelyi et al., 2010).

Although Continuous Assurance is not a concept firmly established yet, it is clear that it is maturing, both in practice and in research, and therefore, the findings measured in the existing implementations are used to improve future conceptual models (M. Vasarhelyi et al., 2010). Nevertheless, Continuous Assurance can be

applied in various organisational branches. In the public sector, the health service, social security institutions, tax administration, banking can be stated as examples. In the private sector, any organisation can benefit from an implementation of Continuous Assurance, although those with greater resources are more able to bear it and keep it, for example, the areas of banking and telecommunications (Alles, Tostes, Vasarhelyi, & Riccio, 2006).

Siemens has made an effort in this area and it has been experimenting successfully some aspects of Continuous Assurance. This effort is mainly aimed at ensuring the integrity of its large ERP systems and their automated modules with audit functions. Their ERP systems cover a large number of configurable controls which can be enabled or disabled at a given point in time. Siemens's project proposes a methodology to monitor and evaluate the daily configuration of various settings of existing controls through the use of CCM, a component of Continuous Assurance. In addition, Siemens conducted a study and concluded that 68% of its audit activities could be automated, eliminating the periodical cycles yearly, monthly, weekly or daily, providing a monitoring, evaluation and continuous auditing fully automated. The actions which correspond to the remaining 32% cannot be automated because their nature does not allow to be formalised, for example, they are based on documentation or manual processes. Thus, an independent system was developed for interacting with read-only operations with the existing information systems and for reporting system and alarms in case of emergency. These implementations have ensured the effectiveness, efficiency and a timely character to the audit procedures. (Alles, Brennan, Kogan, & Vasarhelyi, 2006; Alles, Kogan, & Vasarhelyi, 2008; M. Vasarhelyi et al., 2010).

Also according to Vasarhelyi (2010), one of the biggest banks in Brazil, Itaú Unibanco, with more than 1400 branches has implemented measures for Continuous Assurance since 2000, proving the viability and benefits of these measures. This institution has a CDA (another component of Continuous Assurance, which verifies the integrity of the data circulating in organisational information systems), a system which daily analyses more than five million accounts and generates about six thousand alerts a month. This system aims to increase productivity with efficiency and

quality and its mission is to assess the risks and controls automatically and continuously in order to identify exceptions, anomalies, trends and indicators of risk; advise about controls, risk assessment; and contribute to the corporate governance. These features include all products, processes and services which enable data extraction and analysis. The taken approaches are of detection (routines to detect possible errors), of deterrence (routines to inhibit inappropriate behaviour and events), financial (routines to reduce or avoid losses), of compliance (routines to ensure compliance with applicable laws, policies and standards).

An organisation in the steel industry with 234 industrial and commercial units, present in 10 countries and with shares in New York Stock Exchange was forced to implement measures of Continuous Assurance in accordance with SOX requirements. Although the organisation has been forced to hire specialised personnel to keep these measures of Continuous Assurance functional, in particular, personnel who are able to manage, evaluate and test the implemented internal controls mechanisms and the adopted audit measures, ensuring that they are conform and appropriate to U.S. SOX law, it was found that after these measures, all processes had to be documented and information started to be disclosed in time and with their integrity ensured. It was also felt that these measures held the participants responsible, inhibiting the occurrence of fraud (Hargadon & Fanelli, 2002).

Apart from these, there are many other implementations which have demonstrated the benefits of Continuous Assurance in several organisational areas: providers of health services (Alles et al., 2008), telecommunication companies (Alles, Tostes, et al., 2006), trade and logistics (Coderre, 2005), financial institutions and accounting (Coderre, 2005; Littlely et al., 2010), food companies (Littlely et al., 2010); carriers (Littlely et al., 2010), among others (Oringel, 2010; M. Vasarhelyi et al., 2010).

1.2.2 Research Problem

The survey on related works upon the topic of this thesis provides evidence that the broadening of the scope of auditing for Continuous Assurance is going on. There is also a tendency for the need to evaluate and validate in real-time due to the pressure from the stakeholders of organisations so that they are provided with financial

information which allows them to operate in the capital market with minimum risk. Thus, it is concluded that auditing, monitoring and other assurance services applied to organisational transactions is a research topic of interest, because it meets the current concerns of organisations and the recommendations of the recent rules regarding the organisational auditing and monitoring in order to mitigate the risks associated to the execution of transactions.

To this end, it is necessary to continuously monitor transactions in real time (the closest to the occurrence according to the rhythm of the transaction), creating an additional layer of control (preferably non-intrusive), which works with operating information systems and that ensures the compliance of the execution of transactions, making it possible to estimate and assess potential risks of transactions executions. Furthermore, a key of an effective system with continuous assurance services is the ability to adapt the filters according to the tolerance of risk of each organisation or to regulatory requirements. Therefore, depending on the exception occurred, notifications or alerts can be generated immediately and sent to the responsible for the transactions or organisation or, alternatively, a report which will be subject to an evaluation (Verver, 2003).

Moreover, from the literature review some issues were noted with regard to the implementation of services of the three components of Continuous Assurance (CCM, CDA and CRMA) in information systems. These issues focus on the fact that the information systems presented as service providers of Continuous Assurance are not on their essence, i.e. most of these solutions only provide services related to the component CDA. The implementation of CCM solutions is very complex due to significant differences in the types of business objects. Therefore, the existing CCM solutions are customised for particular information systems or specific to certain areas or organisations.

Regarding the component CRMA, its process and implementation are still vague and ad hoc. Its process is not always effortless when it comes to: dividing a transaction or organisational process in manageable parts to audit and estimate risk; understanding the basic risk profile of each of the parts, and creating all possible

scenarios of organisational risk profile of each of the parts; and creating all possible scenarios of organisational risk.

From the foregoing, it is to highlight the importance of presenting the possibility of providing information systems with continuous assurance services, with the main functionalities of the three components (CCM, CDA and CRMA), for any transaction types or organisational areas. In other words, it is relevant that the main continuous assurance services may be developed in an information system and that the latter may be implemented and applied to various organisational transaction types. Thus, the information system is no longer specific to a particular ERP or organisational area, but adaptable and able to be parameterised to any organisational context.

The use of an ontological model, intended to be validated with this thesis, capable of representing organisational transactions in a coherent, comprehensive, consistent and concise way is the key to solve these issues. “Enterprise Ontology” (Dietz, 2006b) is the model used in this thesis due to its characteristics and wide application in various fields, as shown in section 2.2. Hence, the ontological representation of each transaction becomes the object of the information system. If the information system is modelled to be able to understand this object, it is also able to be used in every type of transactions represented according to the ontological model. Therefore, the customisation of algorithms for monitoring, analysis, auditing and risk assessment of specific transactions is eliminated. The representation of organisational transactions according to the adopted ontological model is the requirement for parameterisation and adaptation of the information system to organisational contexts.

The adoption of a model for ontological representation of organisational transactions supports the improvement of assessment and estimation of risk associated with the execution of transactions, since the organisational transactions come to be represented by the essential events that compose them. These events are manageable parts which allow the construction of risk profiles of organisational transactions, and subsequently, the effective continuous identification of the risk associated with the execution of the transaction. Alongside this, risk profiles refer to the classification of different types of behaviour that may occur in the execution of one transaction. In this thesis, two terms are considered to characterise risk profiles: negative profiles, which

refer to all unwanted behaviours during the execution of transactions, like for example incomplete or poorly executed operations, lack of crucial procedures, non-conformities, delays, incongruities and malfeasance; and positive profiles, which refer to all valid and appropriate events (Denning, 1987; C. Santos, 2009; Toscano, 2009).

Given the foregoing, this thesis focuses on answering to the implementation of continuous assurance services in information systems, having as support an ontological model to represent any organisational transactions.

A solution with assurance services capable of monitoring organisational transactions supported by enterprise information systems with the level and detail that an ontological model provides is an innovative vision. Also considering that there may be different risk profiles for each organisational transaction, the development of a repository that contains and maintains the risk profiles of the transactions to monitor and audit, following the ontology, makes this challenge even greater in the theme of Continuous Assurance applied to organisational transactions.

The development of a solution in accordance with the aforementioned brings with it other challenges: the design of a wide range of internal control mechanisms embedded in organisational transactions (supported by an ERP system), particularly in the various stages and the events that characterise them (according to the ontology) and the design of an instrument that is capable of receiving information from the internal control mechanisms and evaluate in real time (the closest to the occurrence) the state of execution of the transaction, according to the risk profiles defined in the Risk Profiles Repository.

This view of monitoring, controlling and auditing of organisational transactions is innovative since no reference to any implementations of risk profiles repository in the aforementioned way was evident in the literature review. Another innovative aspect of this view is the attempt to provide assurance services to organisational transactions following the structure of an ontology, which presents the transaction at a very low level, at its essence, contrary to what happens in most monitoring of transactions that occur at a high level (for example, compare whether a completed transaction followed a set of established procedures).

This work aims to contribute to a new vision of organisational auditing focused on assurance services in transactions executed and supported exclusively in digital format, typically ERP systems, from the most elementary steps and actions which comprise the essence of organisational transactions (according to ontological model presented in section 2.2).

The effectiveness of a solution with the previously defined characteristics is the motivation of this thesis and the research problem it aims to answer.

1.2.3 Research Questions

To address the problem stated above, the following research question was arisen:

Q1 - Is it feasible to develop information systems with continuous assurance services applicable to any organisational transaction represented by an ontological model and executed exclusively in digital format?

This first research question led us to formulate two other research questions:

Q2 - What are the essential and the most important characteristics of an information system with continuous assurance services?

Q3 - How to develop an information system with continuous assurance services, enabling it to be applicable to any organisational transactions?

To answer these research questions, firstly we defined how to answer question Q2, i.e. identify the essential and the most important features and functionalities to be considered in the developing of information systems with continuous assurance services. Based on the fundamental concepts (section 2.1), a model was designed to evaluate information systems with continuous assurance services. It provides a set of dimensions and requirements and their metrics allow us to evaluate the outputs of an information system and assess whether it provides continuous assurance services. This model has been validated by a panel of experts, as shown in chapter 3 of this thesis.

Some aspects considered in the definition of the research problem, which were provided by the review of related work, have been taken into consideration to answer the research question Q3. This research question is mainly connected with aspects of

providing an architecture or artefacts which enable the application of continuous assurance services to any type of organisational transactions digitally executed in the operational information systems. And from this perspective, the design and development of a risk profiles repository was conceived in order to simultaneously characterise the organisational transactions according to an ontological model and serve as a reference for continuous monitoring, auditing and controlling of the data and the risk associated to the execution of organisational transactions in operational information systems. Because of the innovative character of the design of this repository, its validation is required. Hence, the research hypothesis that follows has been defined and is associated to the latter research question (Q3):

H3.1 - The development of a risk profiles repository of organisational transactions represented by an ontological model is feasible and supports information systems with continuous assurance services.

The first research question (Q1) led us to design a proposal of solution of an information system architecture which supports the continuous assurance services for organisational transactions which are executed exclusively in digital format and represented by an ontological model. From the proposed architecture, a prototype was developed and a case study was deployed which allowed us to answer to this research question. Therefore, the research hypothesis that follows has been defined and is associated to the latter research question (Q1):

H1.1 - The proposed information system provides functionalities related to continuous assurance services.

This research hypothesis aims to demonstrate that the information system developed according to the proposed solution provides functionalities and outputs associated to the dimensions and requirements defined in the model proposed to evaluate information systems with continuous assurance services. This evaluation model results from research question Q2, whose answer provides the essential and the most relevant features and functionalities of information systems with continuous assurance services.

In short, the research was guided by the following three research questions (Q1, Q2 and Q3) and two research hypotheses (H1.1 and H3.1):

Q1 - Is it feasible to develop information systems with continuous assurance services applicable to any organisational transaction represented by an ontological model and executed exclusively in digital format?

H1.1 - The proposed information system provides functionalities related to continuous assurance services.

Q2 - What are the essential and the most important characteristics of an information system with continuous assurance services?

Q3 - How to develop an information system with continuous assurance services, enabling it to be applicable to any organisational transactions?

H3.1 - The development of a risk profiles repository of organisational transactions represented by an ontological model is feasible and supports information systems with continuous assurance services.

1.2.4 Research Methodology

Through the analysis of the presented research problem and the defined research questions and hypotheses, we conclude that the research within this thesis is classified by a quantitative approach, because it is a research which produced data quantitatively measurable and possible to be objectively and statistically analysed to validate the research hypotheses and answers the research questions (Mauch & Park, 2003; Myers, 1997b; Patton, 2002). The quantitative approach is justified because there was the deployment of a prototype that has provided the collection and analysis of some data that may lead to findings about the adopted solution and its feasibility from the technological point of view, and because in the development of the various modules of the proposed architecture there will always be the attempt to establish relationships of action-reaction type in the experiments (Grilo, 2008; Myers, 1997a).

For the classification of the interpretation of research, the positivist epistemology was adopted, because it is used to objectively observe and analyse the results of scientific research from the technological point of view (Babbie, 1993).

To conduct the research, Design Science and Survey are the methodologies which best suit the research questions. To conduct the research associated with research questions Q1 and Q3, the Design Science methodology was used, because this methodology is fundamentally associated with the problem-solving paradigm, and its main objective is the design and evaluation of IT artefacts intended to solve an identified organisational problem. (A. Hevner & Chatterjee, 2010; A. R. Hevner, 2007; A. R. Hevner, March, Park, & Ram, 2004; Peffers et al., 2006).

To conduct the research associated with research question Q2, the survey methodology was used, because it enables to objectively determine values and relations between variables or phenomena, validate hypotheses, test theoretical propositions in an objective way and confirm and quantify results (Grilo, 2008).

Finally, the observation and the measurement were appropriate research techniques to analyse the results and validate the raised research hypotheses associated to research questions Q1 and Q3. The observation technique is based on the observation of a set of phenomena in order to collect data, on a systematic basis, about the behaviour of the prototype (Coolican, 2004; Quivy & Campenhoudt, 1998). The measurement technique is justified, because some quantitative measures related to the results and outputs of the prototype were carried out in order to validate some research hypotheses.

The Delphi method was used in the research of question Q2, because it aims to collect the opinion of a panel of experts to validate a set of statements, providing the answer to this research question (Linstone & Turoff, 1975; Skulmoski, Hartman, & Krahn, 2007).

1.3 OBJECTIVES

This thesis focuses on a topic of high organisational interest, namely, continuous monitoring, continuous auditing and controlling and assessment of risk of organisational transactions and the way they are performed. As aforementioned in previous sections, organisations have been making efforts to implement methods and systems which enable them to increase reliability of their business transactions and processes and, at same time, to be in accordance with their organisational objectives and in compliance with the internal and external regulations.

Associated with this concern, it has been noticed that information systems with features and functionalities of monitoring, auditing and risk controlling present some problems, like for example those which have continuous assurance services are dependent on some ERP systems or other very specific operational information systems, or they are prepared to work only in a few business areas, or they are not very flexible to adapt or they are incomplete because they provide only part of the assurance services.

Thus, this thesis has as main objective to present a possible and innovative solution, enabling the bridging between those issues through the provision of continuous assurance services. This thesis particularly focuses on the topic of implementation of continuous assurance services in information systems applicable to any organisational transactions, regardless of their type, dimension, business area or operational information system in which they are executed, having as support an ontological model to represent organisational transactions.

This research culminated with the development of a prototype of an information system with continuous assurance services in accordance with the proposal of a conceptual and functional architecture, and with the analysis of the results of this prototype collected through its deployment in simulated organisational environment. Thus, this thesis contributed to:

- a more comprehensive and better understanding upon the essential and most important features and functionalities of an information system with continuous assurance services;

- the design, validation and presentation of a model comprising dimensions and metrics, which allows it to be used as a tool or as a set of guidelines to evaluate information systems with continuous assurance services;
- ensure the feasibility of development and the effective use of an information system with full continuous assurance services, having as support an ontological model, and which is considerably flexible and adaptable in order to be applicable to any organisational transactions;
- ensure the feasibility of development of a risk profiles repository of organisational transactions, based on an ontological model and database technologies;
- demonstrate that a risk profiles repository is an important element in information systems with continuous assurance services, as a source of references to support continuous monitoring, continuous auditing and controlling of the risk associated with the execution of organisational transactions.

2

FUNDAMENTAL CONCEPTS

This chapter aims to contextualise and to be a proper theoretical support of the main concepts related to this study. This chapter has two independent sections, the first ones, which, when analysed together, convey the necessary complementarity to understand the need for tools of monitoring and support to auditing of organisational transactions - the central theme of this thesis. The two axes of study are: Continuous Assurance, and Conceptual Model of Transaction.

The section "Continuous Assurance" is intended to help the understanding of the concept which gives the name to the section, its characteristics, evolution and some successful implementations. Finally, the last section presents an ontological view about an organisation and its transactions and processes. The inclusion of this topic in this chapter has proved to be relevant due to the characteristics of the central problem of this thesis. An ontological model is important because it helps to understand the essence of the organisational transactions and processes and their relationships and characteristics to understand how internal control mechanisms and Continuous Assurance services should be incorporated into their operations, in order to be possible to ensure an adequate controlling and an efficient auditing of the performed transactions.

Thus, understanding the benefits of implementing Continuous Assurance for organisations and their stakeholders, meeting the needs of controlling and monitoring organisational transactions, and with knowledge to analyse the essence of organisational transactions and their relationships with the remaining organisational elements, through the studied ontology, we have the information needed to understand that the incorporation of organisational controls on transactions is an important subject of study for combating organisational risk.

Fundamental Concepts

Finally, this chapter is concluded with the presentation of researches and applications related to the topic contextualised with some paradigms and concepts associated with the monitoring and auditing at the level of execution of the organisational transactions and processes.

2.1 CONTINUOUS ASSURANCE

This section has the intention to study the topic Continuous Assurance in order to understand its meaning, its main objectives by the organisational point of view, to make known the constituents of a solution of Continuous Assurance and the evolution which this type of solution has been undergoing, and to present some case studies of interest.

A survey of scientific publications using a variety of bibliographic databases of scientific works was made to study and develop this topic. In this survey, many publications which showed, from its title and keywords, content related to the purposes of this section were collected. The search term in bibliographic databases was "continuous assurance", resulting in the collection of a total of 50 scientific works (in their various categories).

This survey made accounts of the number of publications by the principal author and the number of citations that was possible to determine for this set of works. The result is shown in Table 1. From this table, the authors Alles, Vasarhelyi and Kuhn are distinguished by number of publications and the number of citations on this topic.

Table 1 - Authors of publications on Continuous Assurance

| Author | Number of Publications | Number of Citations |
|--|-------------------------------|----------------------------|
| Alles, M. | 7 | 181 |
| Vasarhelyi, M. | 5 | 80 |
| Kuhn, J. R. | 3 | 19 |
| Yeh, C. H. | 3 | 1 |
| Baksa, R. | 2 | 1 |
| Chan, D. Y. | 2 | 2 |
| Hunton, J. E. | 2 | 11 |
| Teeter, R. A. | 2 | 5 |
| Other authors with only a collected work | 24 | 141 |

From reading the abstracts of the publications collected, the authors' works cited in Table 1 indicate to be able to provide highly relevant information on this topic. In fact, the complete reading of the works of these authors have revealed that "Continuous Assurance" is worked in these publications, both in terms of clarity, both in terms of objectivity, richness, accuracy and completeness with which the subjects are exposed. And as such, these publications were chosen to be the core of the development of this section.

In addition to the influence and reference of these authors, this section also references other authors to include some special features to enrich the topic, namely, the need to develop the concepts of Continuous Auditing, Continuous Monitoring, and their relationship with Continuous Assurance.

2.1.1 Introduction

In the current organisational context in which competition is part of the daily life of organisations, there is a constant need for more timely, relevant and reliable information to help the management team to make decisions, achieve the planned objectives and foresee prospects for the future.

Thus, organisations are redesigning and reinventing themselves and undergo transformations in order to respond appropriately to a constantly changing environment, characteristic of the globalised world in which we live. In this context of change and increasing competitiveness in all market segments, organisations seek productivity gains and improvement of their methods and tools of management.

In this context, Continuous Assurance has been asserting itself and assuming an increasingly important role within organisations, as a function of management support and, in general, to ensure the economic and efficient use of resources and the effectiveness of organisations, areas where the effects of the impact of new risk factors caused by the constant change, fierce competition and widespread access to global information are more felt (Morais, 2008).

The audit was defined as a systematic process of objective obtaining and evaluating of evidences on organisational data and transactions to verify their concordance with the established standards and criteria. The communication of auditing findings to

stakeholders is a service of assurance. However, assurance is a much broader concept than the auditing because it includes all professional services that ensure the quality of the information or its context, for decision makers (Soltani, 2007). The IFAC (International Federation of Accountants) has defined the services of assurance as follows (IFAC, 2004, p. 150):

“Assurance engagement means an engagement in which a practitioner expresses a conclusion designed to enhance the degree of confidence of the intended users other than the responsible party about the outcome of the evaluation or measurement of a subject matter against criteria.”

Continuous Assurance is defined as the application of emerging information technologies to the standard techniques of auditing, both mandatory periodic auditing and internal auditing. In that view, Continuous Assurance presents itself as a new step in evolution of transaction auditing from manual techniques to automated methods. The term "continuous" does not mean real-time, but it means to be effective considering, respecting and being consistent with the pulse and rhythm of each organisational transaction and process. (Alles, Kogan, & Vasarhelyi, 2002; M. Vasarhelyi et al., 2010).

Continuous Assurance has thrived within organisations as a set of services involved in diagnosing certain situations, including the company's viability, allegations of fraud and illegal acts, assessing the economy, efficiency and effectiveness of organisations (Morais, 2008; M. Vasarhelyi et al., 2010). The known cases of fraud at companies like Lehman Brothers, A-Tec, Madoff, Kaupthing Bank, Enron, WorldCom, Adelphia, Global Crossing, Parmalat, Lucent, Tyco, Xerox, among others, led these organisations and their stakeholders to bankruptcy or to very compromising situations. The fraud has caused huge losses to investors in recent years, leading also to the loss of financial credibility and integrity. Similarly, the independent audit service also seems to have suffered a heavy blow because of these frauds. In this scenario, Continuous Assurance emerges as a set of services which aims to restore the credibility of the auditing, allowing at the same time organisations to meet the

requirements of regulations (Bodoni, 2014; Murcia, Souza, & Borba, 2008; M. Vasarhelyi et al., 2010).

2.1.2 Characteristics

Continuous Assurance is an aggregate of objectively provided assurance services, derived from continuous online management information structures – whose objective is to improve the accuracy of corporate information processes (Vasarhelyi, 2002; Zwick, Lettner, & Hawel, 2007).

The concept of Continuous Assurance refers to the set of services which, making use of technology, uses the information immediately and produces audit results simultaneously or within a short period of time after the occurrence of relevant events. In addition, Continuous Assurance allows analytical monitoring of business processes. Compared to the traditional auditing, Continuous Assurance is intended to be timely, more comprehensive, more accurate and more supportive to management (Alles, Kogan, & Vasarhelyi, 2003, 2004; Alles, Tostes, et al., 2006; Vasarhelyi, Alles, & Kogan, 2004).

Moreover, Continuous Assurance has provided a gradual change in audit practice for the maximum possible degree of automation. Given the emphasis on the transformation of the entire auditing system, the development of Continuous Assurance requires a fundamental reassessment of all aspects of auditing, in particular on how data is made available to the auditor, which checks and tests are necessary to carry out, how alerts are managed, what kind of reports are issued, how often and to whom are sent, and many other factors whose importance will be only noticed after the implementation of Continuous Assurance (M. Vasarhelyi et al., 2010).

The AICPA defines the services of Assurance as independent professional services which improve information quality or its context for decision makers. AICPA adds further that the services of Assurance can involve any type of information, financial or not, about discrete phenomena or about the processes or systems (internal control, for example) directly (as information about a product) or indirectly (such as information on some statement about a product), or even internal or external information to the decision maker (Alles et al., 2002).

According to IFAC, the subject matter, and subject matter information, of Continuous Assurance can take many forms, such as (IFAC, 2004):

- financial performance or conditions (for example, historical or prospective financial position, financial performance and cash flows) for which the subject matter information may be the recognition, measurement, presentation and disclosure represented in financial statements;
- non-financial performance or conditions (for example, performance of an entity) for which the subject matter information may be a key indicator of efficiency and effectiveness;
- physical characteristics (for example, capacity of a facility) for which the subject matter information may be a specifications document;
- systems and processes (for example, an entity's internal control or IT system) for which the subject matter information may be an assertion about effectiveness;
- behaviour (for example, corporate governance, compliance with regulation, human resources practices) for which the subject matter information may be a statement of compliance or a statement of effectiveness.

Continuous Assurance is a form of auditing by exception, in other words, operating systems are considered functionally correct until a failure occurs and an alarm is triggered (Vasarhelyi et al., 2004).

When continuous assurance services are running in real time (Vasarhelyi et al., 2004) they provide the opportunity to manage processes and transactions simultaneously with its execution or after a particular event, and even in some cases, the ability to interfere with the completion of the transaction, correcting it. In addition, organisational processes and transactions have their own life cycles, they can be online or with frequency of hourly, daily, monthly or other. Each of them has a different rhythm for their controlling and monitoring (Vasarhelyi et al., 2004). When some service of Continuous Assurance points a wrong transaction, and this is corrected by the auditor, it can be said that the system becomes a proactive player in the processing of organisational information (Vasarhelyi et al., 2004).

The terms Continuous Assurance, Continuous Auditing and Continuous Monitoring are used sometimes indiscriminately in literature. Therefore, it is crucial to understand what characterises and distinguishes them, but mostly to understand how they can relate to, complementing each other (Figure 1).

As previously mentioned, Continuous Assurance can be described as a warranty on the state of affairs. It is often regarded as services closely related to audit of financial nature, but actually other organisational areas can also enjoy the benefits of Continuous Assurance (Coderre, 2005).

Continuous Assurance is a statement on the adequacy and effectiveness of controls and integrity of information. Continuous monitoring of controls is at the centre of Continuous Assurance strategies; however, the audit activity ensures that management activities are appropriate and effective so that organisations have a greater level of certainty about the effective operation of controls, about risk management and about the integrity of information used for decision making (Alles et al., 2003; Coderre, 2005; Kuhn & Sutton, 2006; Verver, 2008).

To introduce the concepts of Continuous Auditing and Continuous Monitoring, it can be said that Continuous Auditing refers to activities undertaken to provide warranty and credibility to operations, and besides, giving a more timely character to issues of control and management risk. Continuous Monitoring has the responsibility for constantly monitoring and evaluating business transactions and their related controls, allowing a real time view on effectiveness of controls and on integrity of transactions. However, there is a basic difference, which is related to the ownership of the process. Although both concepts are similar and tend to produce similar results, Continuous Auditing - as its name implies - is property of the audit function and includes any audit process which is repeated regularly, whereas Continuous Monitoring is a management process, management that is responsible for the maintenance of control systems and for ensuring their effectiveness, allowing to obtain timely information about transactions, including information resulting from errors, frauds or abuses. (Minnaar, Littley, & Farineau, 2008; Verver, 2008).

Continuous Monitoring refers to methodologies which ensure that policies, procedures and business processes are working effectively, and it has the

responsibility for managing and evaluating the adequacy and effectiveness of controls. The Continuous Monitoring principles are simple and include the following (Caldwell & Proctor, 2009; Coderre, 2005; Kuhn & Sutton, 2006):

- define the control points within a business process, according to the COSO framework, if possible;
- identify the control objectives and ensure that they are met at each control point;
- establish a series of automated tests which indicate whether a specific transaction failed to meet control objectives;
- investigate all transactions which appear to have failed a test control;
- if necessary, correct a transaction;
- if necessary, correct the weaknesses of controls.

A Continuous Monitoring benefit for the organisations is that instances of fraud and errors are significantly reduced, operational efficiency is enhanced, and final results are improved through a combination of cost reduction and a reduction in loss of revenue (Kuhn & Sutton, 2006).

In areas where the organisation has not implemented Continuous Monitoring, auditors should apply detailed tests through techniques of Continuous Auditing. In some cases, organisations also may play a proactive role in the establishment of procedures to evaluate controls and risk management. When an organisation has implemented Continuous Monitoring in various business areas, the internal audit activity no longer needs to perform the same detailed techniques which would be applied in Continuous Auditing. Instead, auditors should perform other procedures to determine whether they can trust in the process of Continuous Monitoring. In general, these procedures are similar to quality control tests performed during normal audit process to ensure that CAAT techniques were applied correctly (Caldwell & Proctor, 2010; Coderre, 2005).

These procedures include:

- review of detected anomalies and their interventions;

- analysis and testing of controls in the process of Continuous Monitoring, such as:
 - processing logs;
 - controlling of reconciliations;
 - changing system test parameters.

The Institute of Internal Auditors has defined internal auditing as an independent activity of objective assessment and of consulting designed to add value and improve operations of organisations in achieving their objectives through a systematic and disciplined approach in the evaluation of processes effectiveness of risk management, of control and governance. This modification was based on a paradigm shift which left out the traditional function of financial and accounting control of auditing, and its action changed its focus to the identification of all the risks involved in the various activities of the organisation, intending, this way, that its objectives are met as efficiently and effectively as possible (Alles et al., 2008; Alles, Tostes, et al., 2006; Morais, 2008).

In this sense, Continuous Auditing is a tool to support top management and to help organisations achieve their objectives. The main objective of the activity of internal auditing is to be as a "strategic partner of management" to allow it to be as an advisor and consultant, identifying risks and proposing possible strategies to enable the organisation the best performance within the economic sector (Alles et al., 2008; Morais, 2008).

In other words, Continuous Auditing is a process of collecting and evaluating data in order to determine and ensure efficiency and effectiveness of accounting systems in real time, to safeguard assets, maintaining data integrity and producing reliable financial information (Murcia et al., 2008).

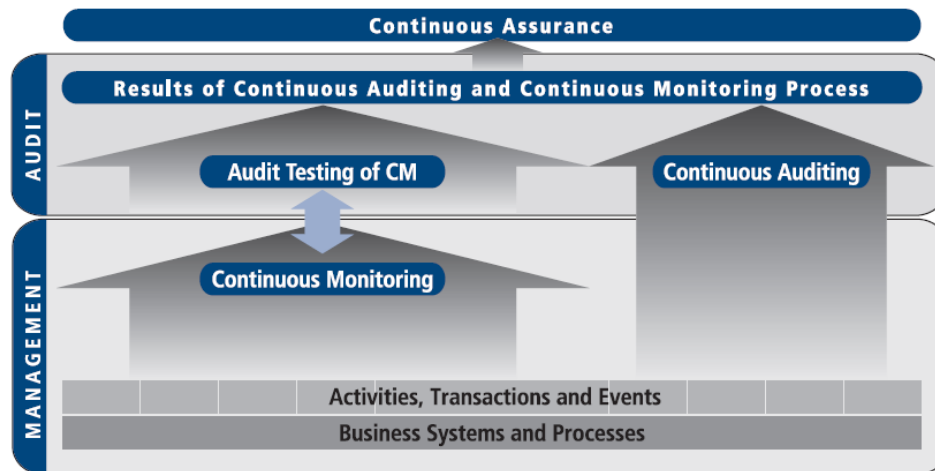


Figure 1 - Continuous Monitoring, Auditing and Assurance (conceptual model) (adapted from Coderre, (2005))

The Continuous Auditing offers several advantages comparatively to traditional approaches of auditing. More importantly, it can provide audit services to more critical organisational areas and more frequently, in spite of forcing the implementation of a specific infrastructure, bringing new concerns to the level of security, management and maintenance of infrastructure in addition to the cost of all that entails. However, the benefits are clear: it reduces risks; diminishes losses and fraud attempts; facilitates the objectives of internal control; allows timely access to information; allows drill-down of data, transactions and processes; integrates internal and external stakeholders; helps external auditing and improves operational transactions and processes, ensuring their compliance; allows timely adjustments by conducting operational testing and data analysis; relieves the auditors of the routine tasks, allowing them to concentrate on other tasks; and increases confidence in transactions and operational processes, in decision making and in financial statements (Cantu, Liu, & Zhou, 2008; Singleton & Singleton, 2005).

Despite their differences, confusion between the concepts is frequent, and sometimes they are used mistakenly as synonyms. The term Continuous Auditing is now over 20 years, and it has increasingly seen implementations of Continuous Monitoring being applied to their activities. Auditors refer to Continuous Monitoring to testing and controlling of transactions using technology. Only in recent years an

effort has been made to understand their differences and distinguish between both concepts (Verver, 2008).

Evaluating the combined results of Continuous Monitoring and audit procedures, auditors are able to provide Continuous Assurance (on the effectiveness of internal controls (Coderre, 2005).

2.1.3 Objectives

The objectives of Continuous Assurance, making it really advantageous, are divided into four levels. These four levels are difficult to define in a mutually exclusive form, but they serve to illustrate the functional dependence of Continuous Assurance on the auditing (Vasarhelyi et al., 2004).

Level 1 – Evaluation of Organisational Transactions

At this level, it is intended to evaluate organisational transactions, and analyse and verify the atomic actions of transactions execution (for example, movement of money or information to the level of data that compose it).

With the use of corporate systems, like ERP systems, there is the possibility to analyse, aggregate and evaluate data in order to classify and monitor organisational transactions.

At this level, input data should be tested in order to verify whether they are valid, and, furthermore, verify whether procedures in execution of transaction are consistent with the sequence of established operations. For example, to check whether a certain movement in the stock corresponds to a sale, to a certain bill, and whether it is in accordance with the order received. Contrary to traditional auditing, with Continuous Assurance it is possible to do this check in real time due to automation and integration of audit procedures. This transaction control can use the formal specification of workflow of processes defined in the ERP systems as a standard behaviour of transaction. Thus, it is possible to verify whether transactions have been executed in compliance with all provided steps, to foresee in some degree, the flow of transactions and whether these are missing or have experienced failures.

Security technologies such as encryption and digital signatures can be incorporated in Continuous Assurance as prevention or detection of fraud of organisational transactions. In addition, certain types of fraudulent activities have different patterns and can be detected by comparison with standard models.

Level 2 - Compliance of the Performed Operations

At this level it is intended to ensure that procedures applied in the execution of organisational transactions are appropriate (for example, are consistent with the rules, norms, or standards set by the organisation or by external regulatory entities).

There are problems with verification automation of such rules and regulations in services for Continuous Assurance because, although automated rules are strictly formal, existing standards have a significant amount of imprecision in their formulations. This automation has been increasingly resorting to the use of artificial intelligence and expert systems and its viability has been proven, for example in formalisation of accounting standards and their benefits (Fisher, 2003).

The procedures of this level use comparison with standards in order to verify the application of these rules and standards, and in case any inconsistency is found, the situation will be forwarded to the auditors or other responsible person for their consideration. Although in this latter case, the resolution of the problem is not guaranteed in real time, this selectivity will allow greater efficiency in auditors' tasks.

Level 3 - Quality of Estimates and the Consistency of Aggregate Data

In some businesses, estimates and forecasts are often used because the measurement or direct determination of some information is difficult and expensive to obtain. For example, the percentage of completion of a work is not always easy to measure, and therefore, must be estimated. However, ERP systems along with cost accounting techniques allow in many cases the precise measurement of the percentage of completion.

Another reason for the use of estimates is the impossibility of knowing the future. Sometimes, not all bills or obligations are paid and only a human can intuitively estimate this bad debt. Intuition and the capabilities of human experts can be captured

and formalised in a model which uses internal parameters (such as past experience with the collection of receivable accounts) and external parameters (such as market interest rates, unemployment levels, several indicators of economic growth, etc.) and be incorporated into ERP systems and as a service of Continuous Assurance.

Even if an organisation does not automatically generate an estimate, continuous assurance services can use their own formal models to ensure in real time that the estimate used by the organisation is acceptable. Obviously, the creation of a formal model of an accounting estimate is not a simple proposition and can add significant costs to the development of Continuous Assurance. A simple and economical alternative is to use a formal model to automatically get an estimate, then the auditor's task will be reduced only to verifying the acceptability of this model, which has to be done only once, and can be done off-line, based on knowing whether the used parameter values in model are reasonable.

This level of Continuous Assurance includes automation of analytical procedures based on internal and external parameters. The use of analytical procedures in an automated system of Continuous Assurance increases efficiency significantly and also effectiveness of auditing.

Level 4: Evaluation of Organisational Decisions

The organisational auditing carried out by using ERP systems and advanced financial instruments must incorporate complex and high level assessments which are especially important for decision making. Such judgments may have to deal, for example with the relevance of contingencies, the extent of related-party transactions, the boundaries of corporate systems, and the nature of the relationships across the value chain. Continuous Assurance and the current analytic technology allow for extensive gathering of exogenous evidence which provides crucial input into these judgments. Continuous Assurance may use, for example data warehousing and data mining as tools that facilitate automation, partial or total, of some of these decisions, contributing to significantly improve the quality of high-level decisions, which in turn will result in a significant reduction of audit risk.

2.1.4 Constitution

Continuous Assurance is divided into three distinct components (Figure 2), but complementary (M. Vasarhelyi et al., 2010):

- Continuous Controls Monitoring (CCM) which consists of a set of procedures to monitor the operation of internal control mechanisms;
- Continuous Data Assurance (CDA) which verifies the integrity of the data circulating in organisational information systems;
- Continuous Risk Monitoring and Assessment (CRMA) which is used to measure the risk dynamically and allow to sustain an audit plan.

Continuous Controls Monitoring

CCM is a set of emerging technologies which monitors controls in ERP systems and other applications in order to improve business governance, to monitor and verify access and transactional rules, and to automate audit processes. CCM assists the business in reducing business losses from fraud or failure to follow rules or procedures governing transactions and improving performance through Continuous Monitoring and reducing the cost of auditing through Continuous Auditing of the automated controls in ERP systems or other financial applications (Caldwell & Proctor, 2010).



Figure 2 - Continuous Assurance (adapted from Coderre (2005))

Caldwell and Proctor (2010) have identified many important CCM functionalities, namely controls monitoring functions (for example, apply a set of pre-audit analysis of the data imported from applications to identify exceptions), exception and remediation management (for example, track the response to identified control failures

and other deficiencies, along with the process of addressing exceptions), reporting and analytics (trending and audit analysis, audit trails), and workflow (notifications, alerts, reviews, approvals). With these functionalities, CCM adds value in an organisation to risk management and for the compliance initiatives that are:

- lowering compliance costs - a CCM solution can reduce the cost of auditing by eliminating some manual sampling and minimising the time that it takes to gather documentation;
- improving financial governance - CCM can increase the reliability of transactional controls, improve auditor trust and increase the effectiveness of antifraud controls;
- improving operational performance - CCM controls, such as those which monitor duplicate payments, incorrect discounts or misapplied warranties, go beyond what most people consider compliance.

In addition, the same authors have identified four technologies that make up CCM: CCM-SOD (Continuous Controls Monitoring for Segregation of Duties); CCM-T (Continuous Controls Monitoring for Transactions); CCM-MD (Continuous Controls Monitoring for Master Data); and CCM-AC (Continuous Controls Monitoring for Application Configuration).

CCM-SOD is used to control and manage the accesses to the applications, particularly the conflicts in these accesses. CCM-T is used to continuously monitor ERP and other application transaction information to improve governance and automate audit processes. CCM-T is an emerging governance, risk and compliance technology which ensures that business rules and policies are effective, reduce compliance and audit costs, support risk management and identify failures of internal control mechanisms. In turn, CCM-MD is an element of many data quality products because it automates controls related to ERP systems and financial application data. It is an element of many data quality products. CCM-AC is always used with each of the other CMM technologies because it is used to monitor the presence, appropriate configuration and modification of built-in application controls (Caldwell & Proctor, 2009, 2010).

Despite these developments, “*the CCM market is relatively small and immature*” (Caldwell & Proctor, 2010, p. 4). More particularly, the market penetration for CCM for segregation of duties is estimated to be 25% and less than 10% for CCM for transactions. And according to CCM vendors, the market is approximately 70% North America, 20% Europe and 10% elsewhere. For the adoption of CCM, the market has been driven by the need for regulatory compliance, risk management and performance of business processes.

Continuous Data Assurance

CDA has been a powerful tool in organisations, in particular in financial and accounting areas, to extract data from organisational databases and applications in order to make analyses at the transactional level and to provide more detailed assurance (M. Vasarhelyi et al., 2010).

CDA has the main objective to change the traditional vision of data auditing in which reports were prepared and audited only once a year, sampling was used rather than examining the entire population; data were analysed at the trial balance level using ratios; these aspects aggregated data across time and space in order to reduce the data and analysis needs of the accountant.

This aggregation and analysis at a higher level than the transactional level has been a cost and capability-based limitation rather than the ideal process for assurance. Thus, CDA can continuously and automatically monitor organisational transactions, comparing their generic characteristics to observed/expected behaviours, thus identifying anomalous situations. When significant discrepancies occur, alarms will be triggered and routed to the appropriate stakeholders (M. Vasarhelyi et al., 2010).

To implement transaction verification it is necessary to specify data validity, consistency and referential integrity rules which are then used to filter data. These rules aim to detect and remove two types of data errors: data integrity violations (for example, invalid purchase quantities, receiving quantities and bank check numbers) and referential integrity violations which are largely caused by many unmatched records among different business processes (for example a payment which was made for a non-existent purchase order).

“The power of CDA comes from a variety of sources: the possibility of running automated tests closer to the event data; the ability of the auditor to access the population of data and to choose the level of aggregation for analytic procedures as opposed to being forced to accept constrained, highly aggregate and sample data; and the use of benchmarks for analytic procedure tests that model the business processes of the entity.” (M. Vasarhelyi et al., 2010, p. 42)

Continuous Risk Monitoring and Assessment

A PricewaterhouseCoopers’s study about the future of auditing has concluded that organisations are now viewing risk management as fundamental to their business operations and it is no longer seen as the technical domains solely of internal auditing. If today’s typical internal auditing model is based on controls of assurance on risk internal audit plan, the tomorrow’s model will also be risk-centric based on the assurance on the effectiveness of risk management (PricewaterhouseCoopers, 2007).

Among multiple possible strategic initiatives, auditors should focus on embracing risk assurance as a primary objective, to expand assurance activities to cover overlooked areas of risk and coordinate with other risk and control functions to ensure that risks are appropriately controlled and managed (PricewaterhouseCoopers, 2007).

CRMA is the process by which organisations address the risks attaching to their activities in pursuit of organisational objectives and across the set of all their activities. Besides, CRMA involves: measuring risk factors continuously, integrating different risk scenarios into some quantitative framework and providing inputs for audit planning. In other words, it engages risk assessment, risk evaluation, risk treatment and risk reporting. The organisational risk management approach is intended to align risk management with business strategy and embed a risk management culture into business transactions (Collier, Berry, & Burke, 2007; M. Vasarhelyi et al., 2010).

2.2 CONCEPTUAL MODEL OF TRANSACTION

This section has the intention to present a conceptual model which characterises organisational transactions and supports the way how transactions are addressed and worked on the development of this thesis.

As in the previous section, a survey of scientific publications using a variety of bibliographic databases of scientific works was made to study and develop this topic. In this survey, many publications which showed, from its title and keywords, content about conceptual models of organisational transactions were collected. The search term in bibliographic databases was "organizational transaction" or "organisational transaction", resulting in the collection of a total of 28 scientific works (in their various categories).

This survey made accounts of the number of publications by the principal author and the number of citations that was possible to determine for this set of works. The result is shown in Table 2.

Table 2 - Authors of publications on Conceptual Model of Organisational Transactions

| Author | Number of Publications | Number of Citations |
|--|-------------------------------|----------------------------|
| Dietz JLG | 6 | 340 |
| BF van Dongen | 1 | 256 |
| Dayal U | 1 | 190 |
| Muller R | 1 | 163 |
| Hepp M | 1 | 114 |
| Albani A | 4 | 39 |
| Papazoglou M | 1 | 25 |
| Wang T | 1 | 21 |
| GropengiBer F | 2 | 11 |
| Other authors with only a collected work | 10 | 10 |

From reading the surveyed publications, the ontology proposed by Dietz, in *Enterprise Ontology - Theory and Methodology* (Dietz, 2006b), has shown evidences that it may be a model capable to represent organisational transactions, supporting the

development of this thesis, because it focuses on formal representation of the various essential aspects of transactions in a concise, objective, microscopic and detailed way. Furthermore, with this model, transactions are seen as part of larger processes and in their organisational context, as will be possible to verify with the analysis of this section.

Interestingly, six other surveyed authors present their work also supported by this ontology. From Table 2, Albani is one of those authors.

2.2.1 Introduction

The use of a conceptual model to represent an organisation is important and necessary to meet the current and future challenges, since this model is coherent, comprehensive, consistent and concise, because only then it can convey the essence of the organisation. By consistent, it is understood that all specific aspects constitute a whole fully logical and true. By comprehensive, it is understood that all relevant aspects are considered and covered. By consistent, it is understood that the model in its entirety is free of contradictions and irregularities. In brief, it is understood that the model does not contain superfluous aspects, everything in it is compact, accurate and succinct. The most important property of this model is, however, the fact that it is fundamental, because it shows the essence of the organisation and its structure (Albani & Dietz, 2011; Dietz, 2006b).

Relatively to the philosophical stance, the notion of Enterprise Ontology, as it is presented by Dietz (2006b), is mainly functionalist in nature, because one of the objectives of this model is to ensure that everything in the system (in this case the organisation) is working correctly in order to promote efficiency, adaptation and survival. However, there are several aspects (for example, the fact that an enterprise is considered a social entity, the autonomy of the various actors as social individuals, etc.) which reflect an interpretive perspective, because this is a model which also aims to understand the actions and the interactions of various actors in collaborative activities, intending to give meaning to such cooperation.

“*Enterprise Ontology*” is considered an ontology because it obeys the fundamental properties of the notion of ontology (defined by Gruber (1995)), that is an explicit and formal specification of a shared conceptualisation.

A notion of ontology presented by Dietz (2006b) is the notion of system ontology in order to understand the essence of the construction and operation of complete systems, specifically enterprises. So the main objective of Dietz, in proposing this ontology, is to provide a new understanding of any systems, and enterprises in particular, so that you can look through the appearance of a sometimes confusing business, and be able to examine the organisational and functional structure of the enterprise in a transparent manner. From the standpoint of the user of the system, this view allows you to become increasingly capable and efficient in your operations, and the designer's point of view, the proposed ontology allows you to design systems so that the resulting project, including the interfaces and cooperation between users, reflect the essence of the system.

The methodology adopted to develop the ontology of an enterprise, in a systematic way, is the DEMO (Design & Engineering Methodology for Organisations) methodology (Institute, 2011). Dietz, with over 15 years of practical experience in applying this methodology, ensures that its applicability extends to all types of organisations and all kinds of purposes. Several testimonies (especially those associated with the part of management and business administration) mention that this methodology provides a coherent, comprehensive, consistent and concise image which is the essence of the functioning of their company (Albani & Dietz, 2011; Dietz, 2006b).

This section results from the need to show people with transparency the functioning of the systems they work daily with, either at home or at the organisational level of large enterprises.

In summary, this section introduces the notion of Enterprise Ontology, and demonstrates its practical use, using a case as an example where the DEMO methodology is applied.

The Enterprise Ontology has been used in many applications, being referenced and used as an essential support tool in significant research and business works. However,

in this work only the main research fields that have benefited from the ontology, the main type of applications and the most relevant works on this topic are pointed out.

One of the main applications of this ontology is concerned with (re)designing and re(engineering) enterprises (Dietz & Hoogervorst, 2008), sometimes used together with approaches of modelling the architecture of enterprises (Ettema & Dietz, 2009) in order to improve them. In addition, it is a valuable instrument for transformation governance propelled by some complex transformations executed by enterprises, such as mergers and splits; chain redesign; sharing and sourcing; and the rationalisation of products, processes and applications (Op't Land & Dietz, 2012).

Information Systems is another field which has benefited from Enterprise Ontology. For example, Albani and Dietz (2011) demonstrate an information system development methodology based on the notions of enterprise ontology, and explain it within a conceptual and generic system development process, allowing the reduction of complexity in the information systems development process. On the other hand, Barjis (2011) demonstrates the importance of business process modelling to capture the rich reality of business systems as enacted in the users' behaviour and interactions, providing verifiable insight into underlying business processes, and thus allowing the design of complex software systems such as Enterprise Information Systems. Another relevant contribution to the information systems field is given by Van Kervel (2012), who presents the DEMO processor, mentioned below.

The identification of business components is another crucial issue that should use Enterprise Ontology for the improvement of the interoperability of enterprises (Albani & Dietz, 2006; Van der Horst, 2010) or to analyse the consistency of business process models (Caetano, Assis, & Tribolet, 2012).

Furthermore, there are works that have contributed to the development of the Enterprise Ontology and its application, as it is briefly presented above.

Aveiro's work (2010) by using Enterprise Ontology, intended to mitigate the problem of organisations wasting time in the handling of unexpected exceptions and the consequent dysfunctions and the problem of the lack of concepts and methods in organisational engineering to timely update the organisational models, which needed to be led with the natural and continuous changing of organisations. The author

contributed with a presentation and specification of G.O.D. (Generation, Operationalisation & Discontinuation) and Control (sub) organisations. G.O.D. is a DEMO-based approach for continuous real-time management of organisational change caused by exceptions which aims to act in the ontological models with generation, operation and discontinuation of parts of the Enterprise Ontology and then to include the ability to react to imposed changes in organisations. This research contributed to explicit the accountability capacity in the Enterprise Ontology, which was far from being implicit within the actors, and consequently in the design of the control of organisations.

Van Kervel (2012) was motivated by the apparent functional mismatch or lack of business-IT alignment; by the complex process of translation of high-level specifications into executable code in software programming processes; and by the growing costs of software modifications over time, which hindered the support of the agile enterprise. The author proposed the DEMO processor, which has been an important contribution to Enterprise Engineering and to Enterprise Information Systems. The DEMO processor eliminates the exhaustive programming within the domain of the ontology, because a DEMO model can be entered directly into the DEMO processor without any programming (translation to lower level primitives and constructs). The DEMO processor is the software engine that executes models, both for simulation and validation purposes and for full production as an Enterprise Information System. Thus, there is no more deterioration of software, because the information systems can be very quickly redesigned and implemented, supporting the agile enterprise. In addition, the possibility of applying DEMO models directly for early simulation and validation mitigates the problem of functional mismatch of information systems.

Guerreiro (2012) contributes with an innovative and ontological solution for the Enterprise Engineering, which is the conceptualisation of the enterprise dynamic systems control with a focus on the run-time business transactions. The work includes a fully validated ontological specification on control embedded between the business transaction models and operations. Moreover, a full constructional ontological solution to control the operation of the run-time business transactions, using DEMO

ontology, has also been developed and validated. Additionally, this solution is compatible with any DEMO business transaction, because it is integrated with the concepts used when a business modeller represent their organisational business transaction in DEMO. However, this solution can be fully used only when organisational transactions are modelled in DEMO.

The Ψ -theory which fundamentals this methodology is succinctly explained in a pedagogical way in section 2.2.2, presenting wherever possible some enlightening examples.

2.2.2 Ψ -THEORY

There are two different notions of system: a teleological (oriented to function) and ontological (oriented to construction) (Dietz, 2006b). Each of them has its own value, purpose and model.

The teleological notion of system treats the function and the external behaviour of the system, based on the black-box model. This model intends to establish a transfer function, namely to find a (mathematic) relation between a set of input variables and a set of output variables, so that the behaviour of the system can be controlled by manipulating the input variables (Dietz, 2006a).

The ontological notion of the system covers the construction and operation of the system, based on the white-box model, whose definition is presented below. The relationship between function and behaviour is that behaviour is anticipated, and hence explained, by the construction and operation of the system; the system function is understood by this demonstration of behaviour. The ontological definition of system is based on Bunge (1979) and consists in what is set out below. A “thing” is a system if and only if it has the following properties (Albani & Dietz, 2009, 2011):

- **Composition:** a set of elements of some category (physical, biological, social, chemical etc.).
- **Environment:** a set of elements of the same category. The composition and the environment are disjoint.

- Production: the elements in the composition produce things (products or services) that are delivered to the elements in the environment.
- Structure: a set of interaction bonds among the elements in the composition and between these and the elements in the environment.

The teleological notion of system is adequate for the purpose of using or controlling a system, often used, for example, in social sciences, including organisational sciences. However, for the purpose of development or changing a system, one needs to adopt the ontological notion of system, dominant in all the engineering sciences (Dietz, 2006a).

The ontological definition of organisation aims characterising it as a social system. This means that its elements are social individuals that are human beings in their ability to enter into and comply with commitments about the things that are produced in collaboration. The *Ψ-Theory* explains the construction and operation of organisations, regardless of their kind or branch (like industry or government, or manufacturing or service). This theory is based on several axioms, from which the relevant ones for this section are presented hereafter (Dietz, 2006a).

The Operation Axiom

An organisation is composed of actors (human beings with a certain profile and functions) who perform two kinds of acts (Dietz, 2006a, 2006b):

- production act (P-act for short) which may be material (for example, a manufacturing or transportation act) or immaterial (for example deciding, judging or diagnosing);
- coordination act (C-acts for short), in which actors enter into and comply with commitments, initiating and coordinating the execution of production acts.

The role of an actor is defined according to the authority and responsibility needed to perform a certain production act. The result of executing a P-act is a production fact (P-fact), also called the result of production. C-acts are, for example, an order or promise of a P-fact. The result of performing a C-act is a coordination fact or C-fact.

Thus, just as it is possible to distinguish P-acts and C-acts, it is also possible to differentiate the two worlds in which these types of acts have effect: the production world (P-world) and the coordination world (C-world), respectively (see Figure 3). At any time, the C-world and P-world are in a given state, defined as a set of C-facts or P-facts, respectively, performed so far. When active, actors take the current state of the P-world and the C-world into account (indicated by the dotted arrows in Figure 3). C-facts serve as agenda for actors, which they constantly try to deal with, i.e. actors interact by means of creating and dealing with C-facts.

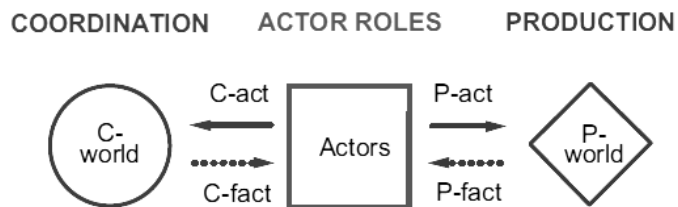


Figure 3 - White-box model of an organisation (adapted from Dietz (2006a))

The Transaction Axiom

An organisational transaction consists of two kinds of acts (P-acts and C-acts) and occurs when they interact co-ordinately. The concept of transaction is composed of three distinct phases (Dietz, 2006a, 2006b; Dietz & Habing, 2004; Dietz & Hoogervorst, 2008): the order phase (O-phase), the execution phase (E-phase), and the results phase (R-phase). A transaction always involves two types of actor profiles, the initiator and executor, sometimes also called customer and producer, as shown in Figure 4.

Figure 5 illustrates the standard pattern of an organisational transaction. In this scheme the white boxes represent the C-acts, the white circles represent the facts of the C-fact type, the box and grey diamonds represent the P-acts and its respective result (P-fact), that is, the transaction execution. The initial act and the final fact are also outlined in bold. It is also possible to identify three phases of a transaction and areas of responsibility assigned to each actor.

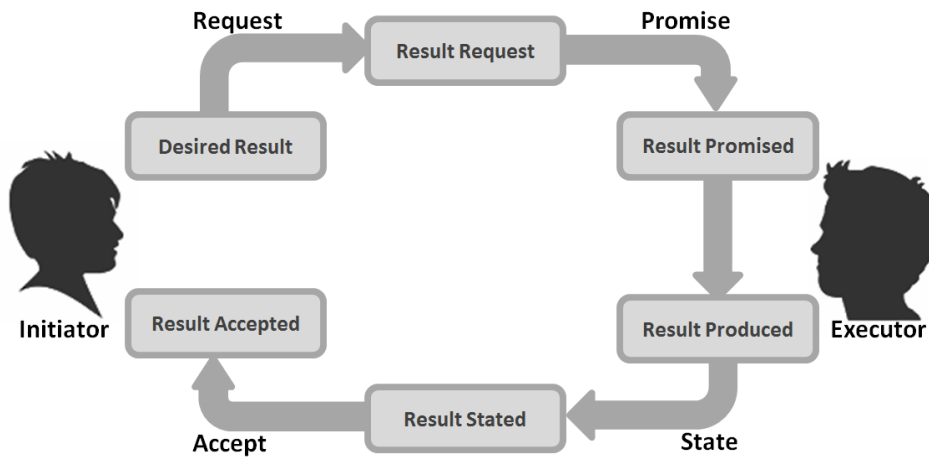


Figure 4 - Basic pattern of an organisational transaction (adapted from Dietz (2006b))

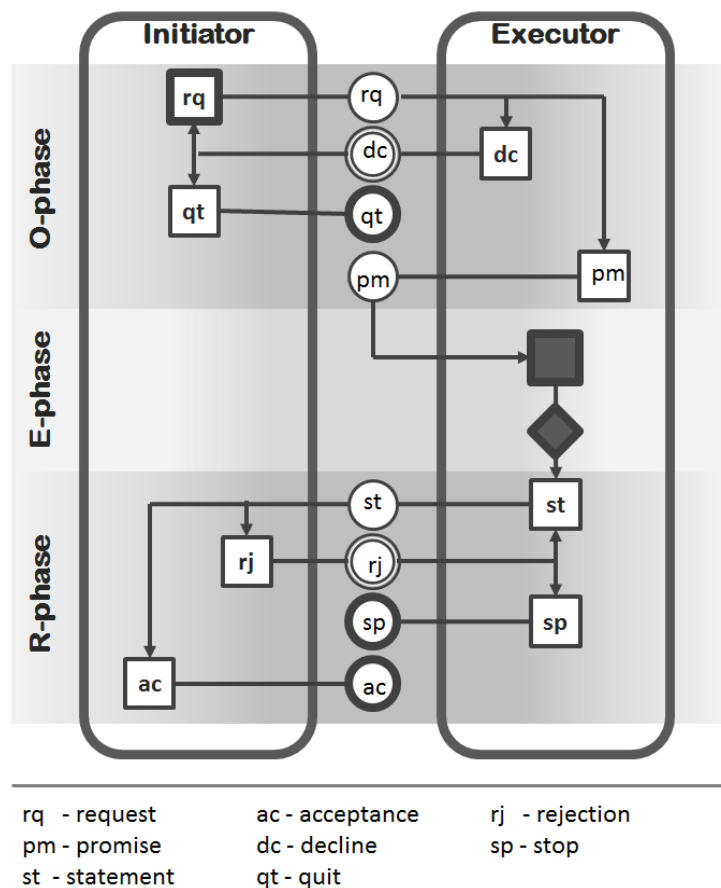


Figure 5 - Standard pattern of an organisational transaction (adapted from Dietz (2006b))

In order phase (O-phase), the initiator and executor negotiate to reach a consensus on the fact that the executor will produce. The main C-Acts in O-phase are a request

(rq) and a promise (pm). In the execution phase, the P-fact is performed by the executor. In the result phase, the initiator and executor negotiate to reach a consensus on the P-fact that was actually produced (that may be different from what was requested). The main C-acts in R-phase are a statement (st) and an acceptance (ac) of the result.

But, considering that after a request there may be a decline (dc) instead of commitment of promise (pm), and instead of accepting (ac) the result produced, there may be a statement of rejection (rj) cease to be dealing with a transaction with a desired result, but an aborted transaction (qt, in the first situation, and sp in the second).

The Distinction Axiom

Three human abilities play a significant role in performing C-Acts (Dietz, 2003):

- “Forma” concerns being able to produce and perceive sentences;
- “Informa” concerns being able to formulate thoughts (it may be a fact, a wish, an emotion etc.) into sentences and to interpret sentences;
- “Performa” concerns being able to engage into commitments, either as performer or as addressee of a coordination act. This ability may be considered as the essential human ability for doing business (of any kind).

Looked upon from the production side, the distinction levels are used to observe and analyse an organisation (see Figure 6). Looking through the ontological perspective, one observes the business actors (B-actors), who perform P-acts that result in original (non-derivable) facts, and who directly contribute to the enterprise’s function. Thus, an ontological act is an act in which new original things are brought about (deciding and judging are typical ontological production acts). Ontological production acts and facts are collectively called B-things. (Dietz, 2006a).

Looking through *infological*¹ point of view, one observes intellectual actors (I-actors), who execute *infological* acts like deriving and computing knowledge about business facts. An *infological* production act is an act in which one is not concerned about the form but, instead, about the content of information only (for example, calculating, and reasoning is considered to be an *infological* act). *Infological* production acts and facts are collectively called I-things (Dietz, 2006a).

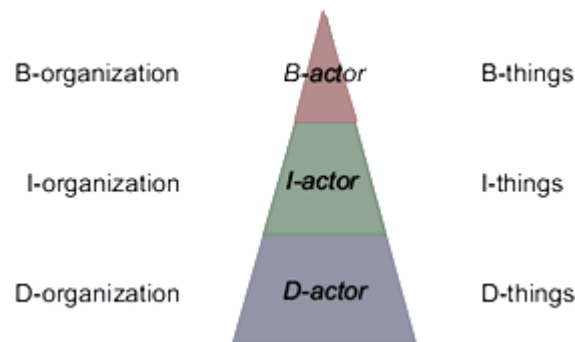


Figure 6 - Representation of the Distinction Axiom (adapted from Dietz (2006b))

Looking through the *datalogical*² point of view, one observes *datalogical* actors (D-actors), who execute *datalogical* acts like gathering, distributing, storing, and copying documents containing the knowledge mentioned above. So, a *datalogical* production act is an act in which one manipulates the form of information, commonly referred as data, without being concerned about its content. *Datalogical* production acts and facts are collectively called D-things. Thus, for example, an actor can simultaneously perform the functions of B-actor, I-actor and D-actor.

The distinction levels as illustrated in Figure 6 are an example of a layered nesting of systems, in which each layer supports the system in the next higher layer and conversely, the system in some layer uses the system in the next lower layer. So, the B-organisation uses the I-organisation and the I-organisation uses the D-organisation.

¹ The terms "infological" and "datalogical" are based, and have the same meaning as indicated by Langefors (1977)

² The terms "infological" and "datalogical" are based, and have the same meaning as indicated by Langefors (1977)

Conversely, D-organisation supports I-organisation and I-organisation supports B-organisation. If a system X supports a system Y, it means that the function of system X is expressed in terms of the construction and operation of system Y. For example, the actor in the B-system needs to know specific information. This information can by definition only be asked for in the I-organisation. In order to get the information, the person who fulfils the B-actor role has to take the role of I-actor and initiate a (*infological*) transaction, making use of the needed knowledge by the executor of this transaction (the I-actor who is the proprietor of this piece of knowledge). In turn, this I-actor may not have the requested knowledge and thus has to initiate, in the role of D-actor, a (*datalogical*) transaction of which the executor is a D-actor who keeps record of the requested knowledge. A copy of the record (a document) is sent to the initiator who, in the role of I-actor, is able to interpret the document and lastly, in the role of B-actor, is able to take the appropriate action based on the acquired knowledge (Dietz, 2006a).

The pyramid constitutes an intrinsically solid integration of the three aspect organisations in the (complete) organisation of an enterprise because it is built on the inseparability of the human being, who simultaneously possesses the *forma*, the *informa*, and the *performa* ability (Dietz, 2006a).

To get to the ontological model of a certain process it is necessary to focus exclusively on the ontological production acts and coordination activities identified in its transactions. In other words, we consider only the top triangle in Figure 6, the B-organisation, with B-actors and B-things. The ontological model of an enterprise is the model of its B-organisation.

The DEMO methodology consists of four models, as depicted in Figure 7 (Dietz, 2006b). The Construction Model (CM) is the most concise, and the Action Model (AM) is the most detailed, because it contains the rules and operational guidelines of the organisation. The State Model (SM) specifies the state space and transition space of the P-world, while the Process Model (PM) specifies the state space and transition space of the C-world. Each of them has a part of the Construction Model (Albani & Dietz, 2011).

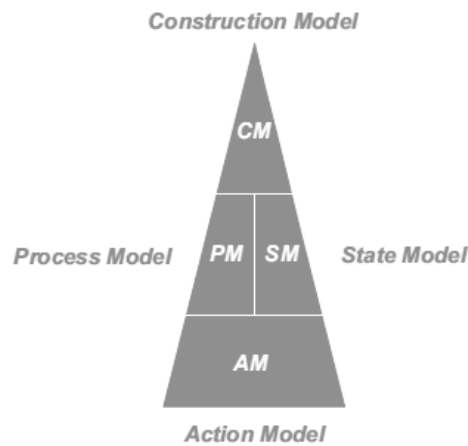


Figure 7 - Ontological models (adapted from Dietz (2006b))

The aforementioned Process Model specifies the state space and the transition space of the C-world and thus the set of lawful or allowed sequences of states in the coordination world. Considering that every transaction in the C-world consists of the creation of a C-fact and that there is a one-to-one relationship between this C-fact and the causing C-act, these C-acts are also contained in the Process Model. The Process Model is also based on the data defined on the Construction Model particularly on the actor roles that perform the C-acts. The called responsibility area of each actor role encompasses all coordination acts carried out by that actor role.

Figure 8 exemplifies a Process Model based in a case proposed by Dietz (2006a) made up of two transactions, T01 and T02, and shows the basic steps in both transactions, as well as their relationships T01/rq, T01/pm, T01/ex, T01/st, and T01/ac respectively stand for the request and the promise of T01, the execution of T01 (that is, performing the P-act), and the statement and acceptance of T01. A similar way of thinking holds for transaction T02. A C-act (small box) and its resulting C-fact (represented by a small disk) are put together in one combined symbol. The P-act (represented by a small grey box) and the P-result (represented by a small grey diamond) are combined, as well. A solid arrow is a causal link. For example, the requested by T01 causes the promise of T01, not as an inevitable cause-effect sequence, but as a possible action of actor role A01 in dealing with what is being requested. In dealing with T01/pm, two acts are performed: the execution of T01 and

the request of T02. Nevertheless, the actual performing of the execution of T01 has to wait for T02 to be accepted; this is the meaning of the dashed arrow from T02/ac to the execution symbol of T01. Thus, the two transactions are connected, that is T02 is enclosed in T01. Because of the causal and conditional (waiting) relationships between T01 and T02, together they constitute a business process.

Figure 8 shows the process structure of the business processes. The actual sequence of steps in a successful instance of this process is T01/rq, T01/pm, T02/rq, T02/pm, T02/ex, T02/st, T02/ac, T01/ex, T01/st, T01/ac. T01/rq followed by T01/dc (decline) are the only unsuccessful kind of instance.

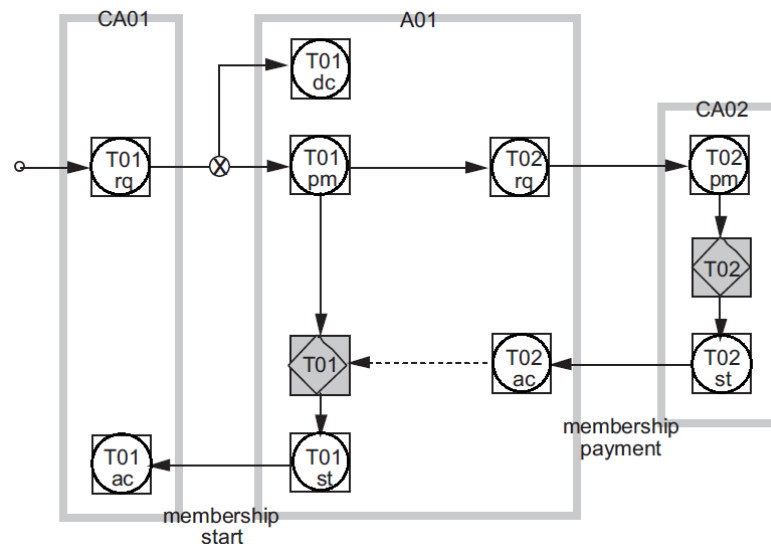


Figure 8 – Example of a Process Model (adapted from (Dietz, 2006a))

There are three different actors' roles in this case, called A01, CA01 and CA02. The large grey-lined rectangles enclose the acts each actor is authorised and responsible for. Thus, for example, the actor fulfilling the CA01 role is responsible for T01/rq and T01/ac.

For each coordination step (represented by a circle and a square), there is an action rule which guides how the actor must respond to the reached status. Below, we present all the rules of action for the player with the profile A01. The set of action rules of an organisation is called Action Model. The action model is another organisational

ontological model, together with the Process Model (discussed above), the State Model, and the Construction Model (the latter two to be discussed below).

The Action Model is the most comprehensive model and integrates the concepts defined on the models (PM, SM, and CM). Therefore, the other models may be derived from the AM. This model describes the rules of execution of every transaction. Figure 9 depicts an example of this model. Each action rule is enclosed by a pair on-no. The on clause specifies the C-fact which is being dealt with. Conditional responses (choices) are represented by an if clause (enclosed by a pair if-fi). If there is more than one choice, the second and following ones are preceded by the symbol "→." Each choice consists of the condition, which turns out to be true, followed by the symbol "→" followed by the action to take.

```

on request T01 (M) with member (new M) = P
  if age(P) < minimal_age or #members (Volley) = maximum_number(current_year)
    → decline T01 (M)
  else if age(P) >= minimal_age and #members (Volley) < maximum_number
(current_year)
    → promise T01 (M)
  fi
no

```

Figure 9 – Example of an Action Model (adapted from (Dietz, 2006a))

The State Model (SM) is the specification of the state space of the P-world. It consists of specifying the object classes, the fact types, and the result types, as well as the existential laws that hold. The technique for developing this diagram is based on ORM (Object-Role Modelling) (Halpin, 2001). The facts are pure mathematical functions and they are not included in the diagram, but listed as properties below the diagram. Figure 10 exemplifies a State Model and should be interpreted as follows: in this context there is an object class MEMBERSHIP and an object class PERSON; it states that a particular person is the member in a particular membership; there are two production fact types or result types of transactions, namely, PF01 and PF02; producing a PF01 for a particular membership means that the membership then starts to exist; producing a PF02 means that the first fee for the membership has been paid;

the list of properties is displayed immediately below in the diagram for every domain of the represented context. And the asterisk (*) next to some of them means that they are derived fact types.

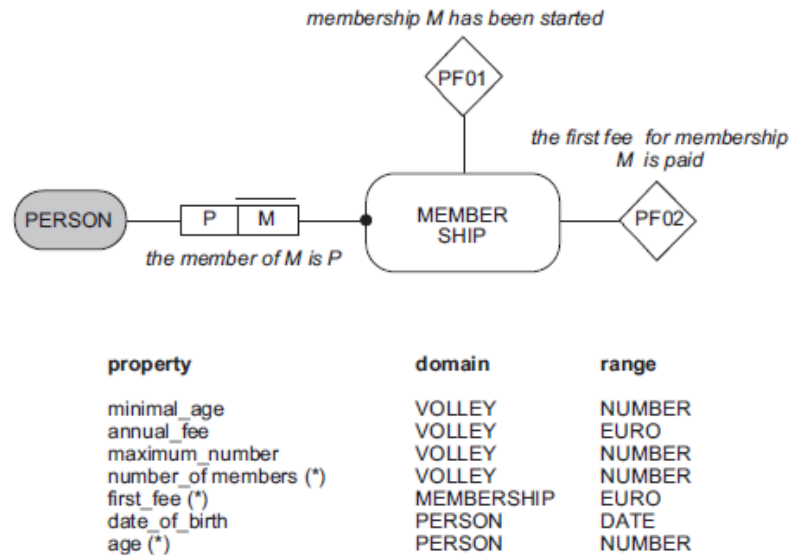


Figure 10 - Example of a State Model (adapted from (Dietz, 2006a))

Finally, the most comprehensive model is the Construction Model (Figure 11). This model specifies the composition, environment, and structure of the context we are modelling. The composition and the environment are a set of actor roles performed by humans (individually or collectively). The interaction structure therefore consists of the transaction types in which the identified actor roles take part as initiator or executor. The Actor Transaction Diagram (ATD) is used to construct this model. Transactions are now represented by only one symbol: a circle with a diamond. The actor's profile involved is represented by a square. The producer has, in addition, a small black square on the junction of this line and the square of the actor's profile. The largest grey-lined rectangle represents the boundary of the organisation under consideration. By convention, all environmental elements are grey, and their codes begin with a C for "composite".

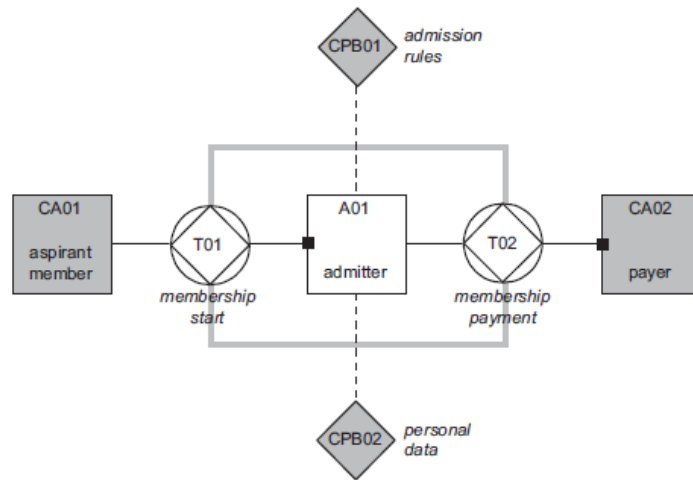


Figure 11 – Example of a Construction Model (adapted from Dietz (2006a))

There is only one internal actor role, namely, A01, that is coloured white because it is an elementary actor role, which is it is an atomic amount of authority and responsibility. It is executor of exactly one transaction type, and customer of zero, one, or more transaction types. In this case, A01 is the producer of T01 and the customer of T02. The transaction symbol has two interpretations, because, in addition to representing a transaction type of which instances are carried out in the enterprise, it is the combination of a coordination bank (the disk) and a production bank (the diamond). A coordination bank contains all coordination facts created allowing one to monitor the progress of all transaction instances. There are two composite production banks (CPB01 and CPB02). They contain facts that are needed by A01 but that are produced outside the enterprise under consideration. The dashed lines indicate that actor role A01 (the only internal actor role) has access to the contents of these banks.

3

CHARACTERISTICS OF CONTINUOUS ASSURANCE

This chapter intends to determine the essential and the most important characteristics of an information system with continuous assurance services. These characteristics were surveyed and deducted from the literature and validated by a panel of experts.

Thus, this chapter presents the methods which were implemented in order to contribute with the set of the characteristics. These methods are based on the Delphi method which aims to achieve consensus among the members of the panel of experts on a topic of study.

3.1 INTRODUCTION

The information systems with Continuous Assurance support mainly implement CCM and CDA components. Despite trying to integrate the maximum possible features, the truth is that vendors still address only in CDA, because the implementation of CCM is time-consuming and expensive due to the diversity of business processes (Coderre, 2005). But this thesis, as explained in section 1.2, intends to offer features of Continuous Assurance which cover the components and meet the majority of objectives, providing the benefits of Continuous Assurance (Alles et al., 2003, 2004).

Thus, it is apparent the need of an evaluation model to evaluate and understand whether the system is indeed an information system with continuous assurance services. And that is done confirming if the system meets the main objectives of Continuous Assurance and covers the features of its components. Table 3 summarises the objectives and components of Continuous Assurance, which were already detailed in section 2.1.

Table 3 - Objectives and components of Continuous Assurance

| | | |
|-------------------|---|---|
| Objectives | Level 1 (transaction evaluation) | At this level the main goals are: monitor and analyse the operations which constitute the execution of an organisational transaction; identify an irregular operation as soon as it occurs; verify whether, for each transaction, the operations have been correctly processed in all previous steps as required; detect lack of operations, and analyse the continuity and completeness of transactions. |
| | Level 2 (measurement rule assurance) | At this level the main objective is the system being able to: verify the transactions which are being executed, or are already completely executed; verify fulfilment of requirements, rules, conditions or sequences previously defined for each of the monitored transactions. |
| | Level 3 (estimate assurance and consistency of aggregate measures) | At this level the main objective is to: estimate which will be the result of the execution of a transaction based on the data set we have at present. |
| | Level 4 (judgment assurance) | At this level it is considered as objective the system being able to allow extensive gathering of evidence, which provides crucial input into users' judgments. |
| Components | Continuous Controls Monitoring (CCM) | It consists of a set of procedures to monitor the operation of internal control mechanisms and verify whether they are consistent with the predefined rules. Besides the controls monitoring, it produces reports and performs analyses; aims to reduce business losses from fraud or failure to follow rules on procedures governing transactions, and improves organisational performance. |
| | Continuous Data Assurance (CDA) | It verifies the integrity of the data circulating in organisational information systems, comparing it with the expected behaviours and patterns, thus identifying anomalous situations and triggering alarms when they occur. |
| | Continuous Risk Monitoring and Assessment (CRMA) | It is used to dynamically identify, assess and report the risk and allow to sustain an audit plan. |

Analysing the previous information, Continuous Assurance can be evaluated through the following dimensions: Monitoring, Compliance, Estimation and through the requirement Reporting. These dimensions and requirement comprise all aspects mentioned in the objectives as well as in the components of a system with continuous assurance services. Based on the nature of the several objectives and components of Continuous Assurance, already presented and detailed in section 2.1, the dimension Monitoring was conceptualised to encompass the objectives level 1 and the component CCM of Continuous Assurance, while the objectives level 2 and the component CDA are included in the dimension Compliance, and the objectives level 3 and the component CRMA are encompassed in the Dimension Estimation; Reporting comprises all objectives and components of Continuous Assurance (Figure 12).

Note that the objectives level 4 of Continuous Assurance have not been considered for this model, because their nature falls out the scope of this work, since this level of objectives includes exogenous functions to the organisations, for example the gathering of external evidences to provide judgments or high-level information for top strategies or decisions on top management, or the use of data warehouse and data mining. It means that these objectives are not so related with operational data but with aggregates.

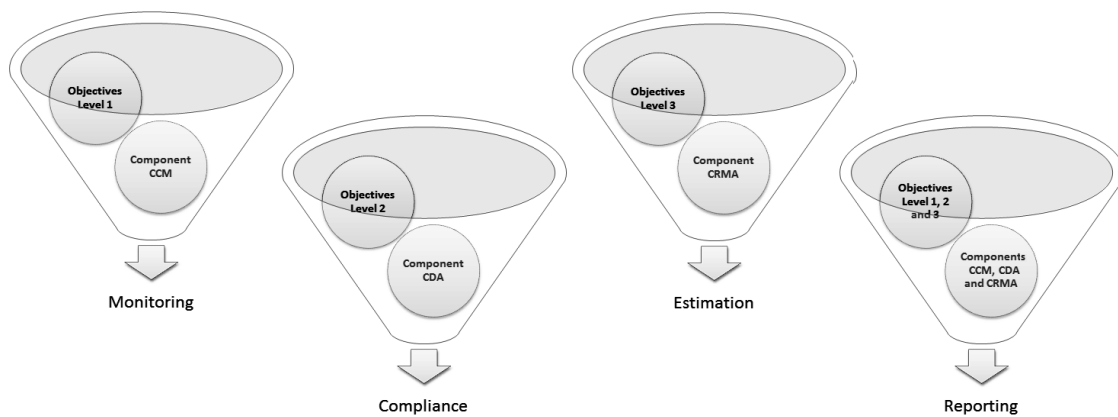


Figure 12 - Relationship between the proposed dimensions and CA

Thus, if we embrace these dimensions with the outcomes and benefits of a system with continuous assurance services (as shown in Figure 13) we will have conceived a model able to be used to guide evaluation of a system with this kind of services, because the principal characteristics of Continuous Assurance are asserted through the model dimensions.

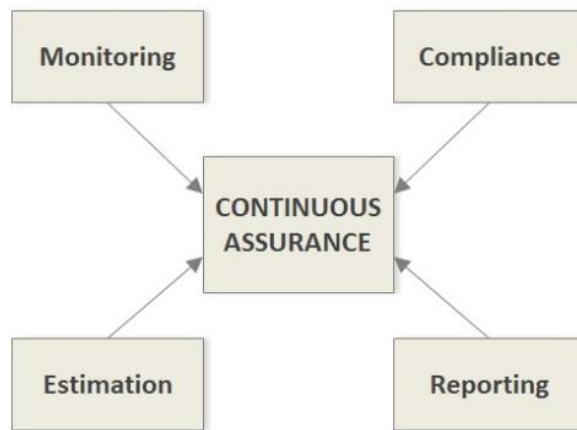


Figure 13 - Dimensions of the evaluation model

The value of a system is delivered through two outcomes: provide the essential functionality to enable users to effectively perform their duties; and provide meaningful information and reports that will empower management and help the decision making. Therefore, in theory, when building a system, the functionality and reporting need to be considered as equally important. For this reason, the requirement Reporting is not presented as a dimension in this model, like the other aspects, but as an essential requirement. The dimensions of the model refer to the functional requirements of the system.

3.2 DIMENSIONS AND REQUIREMENT OF THE EVALUATION MODEL

As explained above, the evaluation model proposed in this paper is composed of three dimensions and one requirement. This section aims to explain the existence of each one and present some metrics which can be used to assess the dimensions and consequently support evaluation of information systems with Continuous Assurance.

Monitoring (dimension)

This dimension relates with the objectives of level 1, i.e. organisational transactions evaluation. It is also connected with the component CCM. Thus, analysing the data allied with those objectives and that component, we can identify some metrics which allow to evaluate this dimension.

Hence, these metrics must assess whether the system is able to:

- monitor the various operations (which have controls embedded) of an organisational transaction as soon as they occur (IFAC, 2004; Kuhn & Sutton, 2006; Singleton & Singleton, 2005; Soltani, 2007);
- identify an irregular operation (unforeseen or inconsistent with the predefined rules) as soon as it occurs (Coderre, 2005; Soltani, 2007);
- verify whether, for each transaction, the operations were processed at all the previous steps, as required (Coderre, 2005; Kuhn & Sutton, 2006; Soltani, 2007);
- detect lack of operations (Coderre, 2005; Kuhn & Sutton, 2006; Singleton & Singleton, 2005);
- assess the continuity and completeness of transactions (Coderre, 2005; Singleton & Singleton, 2005).

Compliance (dimension)

This dimension has included the features of the component CDA and the objectives of level 2. After analysing those objectives and that component, some metrics are given as examples of how to evaluate this dimension.

These metrics assess the system on whether it is able to:

- recognise which known execution pattern was or has been followed by each organisational transaction monitored (Coderre, 2005; Singleton & Singleton, 2005);
- ascertain which rules, conditions and procedures were fulfilled and unfulfilled in the organisational transaction monitored (Coderre, 2005; IFAC, 2004; Soltani, 2007);
- detect potential errors (Coderre, 2005; Singleton & Singleton, 2005);
- inhibit inappropriate events or behaviours (Coderre, 2005; Singleton & Singleton, 2005);
- help compliance with existing laws, policies, norms and procedures (Coderre, 2005; IFAC, 2004; Soltani, 2007).

Estimation (dimension)

This dimension includes and covers the objectives of level 3 and the functions of the CRMA component. After analysing data and the characteristics of that component and those objectives, we propose a set of metrics to evaluate this dimension.

Thus, these metrics assess whether the system is able to:

- estimate, given the current situation, what the possible results of the organisational transaction execution will be (Coderre, 2005; Singleton & Singleton, 2005; Soltani, 2007);
- determine the execution pattern, or a set of execution patterns, which will be possible to be followed by the organisational transactions monitored, according with the current status of execution (Coderre, 2005; Singleton & Singleton, 2005; Soltani, 2007).

Reporting (requirement)

For Reporting requirement we propose the following set of metrics which will enable to evaluate it. These metrics must assess whether the system is able to:

- report the results of the monitoring of transactions (Coderre, 2005; IFAC, 2004; Singleton & Singleton, 2005; Soltani, 2007);
- notify the results of the verification of compliance (Coderre, 2005; IFAC, 2004; Singleton & Singleton, 2005; Soltani, 2007);
- inform the results of estimation (Coderre, 2005; Singleton & Singleton, 2005);
- alert users of irregular situations in monitoring, compliance verification and estimation of negative results (Coderre, 2005; IFAC, 2004; Singleton & Singleton, 2005; Soltani, 2007);
- allow the gathering of evidence, which provides crucial input for users' judgments (Coderre, 2005; Singleton & Singleton, 2005).

Therefore, it is patent that the features of all continuous assurance components and the objectives of all levels are included and covered by this dimension.

Continuous Assurance (outcomes)

Finally, this aspect intends to evaluate the benefits of Continuous Assurance for organisations, assessing whether the system:

- improves the accuracy of corporate information processes (Coderre, 2005; Singleton & Singleton, 2005; Soltani, 2007; Vasarhelyi, 2002);
- supports timely and accurate management and audit of processes and transactions (Bodoni, 2014; Coderre, 2005; IFAC, 2004);
- improves the accuracy of operational transactions and processes, ensuring their compliance (Morais, 2008; M. Vasarhelyi et al., 2010);
- increases confidence in transactions and operational processes execution (Coderre, 2005; IFAC, 2004);
- supports the decision making (Alles et al., 2002; Coderre, 2005; Singleton & Singleton, 2005).

The proposal of the metrics has been based on related works on this topic. Thus, for every analysed work, we looked for evidences, clues or issues which were related to objectives, components and outcomes of Continuous Assurance. For every proposed

metric in each dimension, the respective authors and works are cited in order to explicit the origin of this model proposal. Figure 14 concisely summarises its dimensions/requirement and the respective proposed metrics (R. P. Marques, H. Santos, & C. Santos, 2013a). The metrics we propose are those which are able to be quantitatively measured. Thus, this is the reason that justifies the non-inclusion of the dimension related to the outcomes of Continuous Assurance because of their qualitative and subjective nature.

Characteristics of Continuous Assurance

| | <i>Metrics</i> | <i>Suggested by...</i> |
|-------------------|--|---|
| MONITORING | Real-time monitoring of operations | <ul style="list-style-type: none"> ✓ IFAC, 2004 ✓ J. Randel Kuhn & Sutton, 2006 ✓ Singleton & Singleton, 2005 ✓ Soltani, 2007 |
| | Real-time identification of irregular operations | <ul style="list-style-type: none"> ✓ Coderre, 2005 ✓ Soltani, 2007 |
| | Verification of the processing of required operations at all previous steps | <ul style="list-style-type: none"> ✓ Coderre, 2005 ✓ J. Randel Kuhn & Sutton, 2006 ✓ Soltani, 2007 |
| | Detection of lack of operations | <ul style="list-style-type: none"> ✓ Coderre, 2005 ✓ J. Randel Kuhn & Sutton, 2006 ✓ Singleton & Singleton, 2005 |
| COMPLIANCE | Recognition of execution patterns | <ul style="list-style-type: none"> ✓ Coderre, 2005 ✓ Singleton & Singleton, 2005 |
| | Ascertaining of fulfilling of rules | <ul style="list-style-type: none"> ✓ Coderre, 2005 ✓ IFAC, 2004 ✓ Soltani, 2007 |
| | Detection of potential errors | <ul style="list-style-type: none"> ✓ Coderre, 2005 ✓ Singleton & Singleton, 2005 |
| | Verification of compliance of existing policies | <ul style="list-style-type: none"> ✓ Coderre, 2005 ✓ IFAC, 2004 ✓ Soltani, 2007 |
| ESTIMATION | Estimation of possible risks | <ul style="list-style-type: none"> ✓ Coderre, 2005 ✓ Singleton & Singleton, 2005 ✓ Soltani, 2007 |
| | Determination of possible execution patterns | <ul style="list-style-type: none"> ✓ Coderre, 2005 ✓ Singleton & Singleton, 2005 ✓ Soltani, 2007 |
| REPORTING | Real-time presentation of the executed operations which were monitored | <ul style="list-style-type: none"> ✓ Coderre, 2005 ✓ IFAC, 2004 ✓ Singleton & Singleton, 2005 ✓ Soltani, 2007 |
| | Real-time presentation of execution patterns which are being followed or are likely to be followed | <ul style="list-style-type: none"> ✓ Coderre, 2005 ✓ IFAC, 2004 ✓ Singleton & Singleton, 2005 ✓ Soltani, 2007 |
| | Presentation of the compliance verification in transactions executions | <ul style="list-style-type: none"> ✓ Coderre, 2005 ✓ IFAC, 2004 ✓ Singleton & Singleton, 2005 ✓ Soltani, 2007 |
| | Real-time presentation of the risk estimated on determining possible execution patterns | <ul style="list-style-type: none"> ✓ Coderre, 2005 ✓ Singleton & Singleton, 2005 |
| | Real-time alert for irregular situations in monitoring, compliance verification and estimation of negative results | <ul style="list-style-type: none"> ✓ Coderre, 2005 ✓ IFAC, 2004 ✓ Singleton & Singleton, 2005 ✓ Soltani, 2007 |

Figure 14 - Dimensions and requirement of the model and their metrics

3.3 MODEL VALIDATION

To validate the previous model the Delphi method was used in order to collect the opinions of a group of experts in areas directly related to the topic of study. With the opinion of experts we were able to validate a set of statements when consensus was obtained within the responses of the panel of experts. Details about this model validation process, concerning Information Systems with continuous assurance services, can be found in the publication of Marques, Santos and Santos (in press).

3.3.1 The Delphi Method

The Delphi method originated in a series of studies conducted by RAND Corporation in the 1950's in order to develop a technique to obtain a reliable consensus among a group of experts (Dalkey & Helmer, 1963).

This method consists in a structured process which uses a questionnaire in multiple iterations answered by a panel of experts in order to collect information. The process continues until there is consensus in the panel (Barbara, Melanie, David, & Anne, 2002; Keeney, Hasson, & McKenna, 2001). It is especially used to obtain consensus of opinion, judgment or choice, especially to determine, predict and explore group's attitudes, needs and priorities (L. D. d. Santos & Amaral, 2004).

Linstone and Turoff (1975) defined Delphi as a method for structuring a group communication process so that the process is effective in allowing a group of individuals, as a whole, to deal with a complex problem. To accomplish this structured communication it is provided: some feedback of individual contributions; some assessment of group judgment; some opportunity for individuals to revise views; and anonymity for individual responses (Linstone & Turoff, 1975).

The study by Okoli and Pawlowski (2004) concluded that the Delphi method is used in various fields of knowledge and very popular in research in Information Systems. The studies of Santos and Amaral (2004) and of Skulmosku, Hartman and Krahn (2007) allow to come to similar conclusions about the applicability of this method in the Information Systems field. Furthermore, the extensive literature review of a study performed by Okoli and Pawlowski (2004) shows that the main applications

of the method are: Forecasting and Issue Identification/Prioritisation; and Concept/Framework Development. The majority of the Delphi efforts during the first decade were for forecasting although concept/framework development is the most current type of application of the Delphi method, which typically involves a two-step process beginning with identification/elaboration of a set of concepts followed by classification/taxonomy development.

The Delphi method is distinguished by the ability of developing issues in a rigorous way, because the respondents correspond to experts in the field under analysis, conferring greater rigor to the study and results with a higher level of deepening (Garrod & Fyall, 2005).

The Delphi method has four essential and required characteristics (Garrod & Fyall, 2005; Keeney et al., 2001; Linstone & Turoff, 1975; Okoli & Pawlowski, 2004): the anonymity, the iterative process, the controlled feedback and the appropriateness of a variety of statistical analysis techniques to interpret the responses of the panel.

Anonymity is one of the principal advantages of the Delphi technique, because it reduces the risk of respondents to feel pressured or be influenced by other experts having an impact on their exact opinion (Garrod & Fyall, 2005).

In contrast to other techniques, the collection and analysis of data from the Delphi method is characterised by applying an iterative process consisting of several iterations of questionnaires to reach the aforementioned consensus in the panel of experts (Li-Ling Hsu, 2008).

The controlled feedback consists of informing the respondents, in each iteration, about the results of the panel's responses in the previous iteration, allowing and encouraging the reassessment of their decisions on the information provided in previous iterations (Li-Ling Hsu, 2008; Linstone & Turoff, 1975).

The iterative nature of the Delphi method, in which respondents have the opportunity to make again their judgments based on the aggregate results of the previous iteration, reduces the likelihood of respondents making judgments or decisions under pressure, contributing to increase the accuracy of the results of the study and make them more reliable (Garrod & Fyall, 2005). The statistical aggregation of responses provides the overall result of each of the iterations in a simplified manner

mostly through measures of central tendency (mean, median and mode) and measures of dispersion (standard deviation and interquartile range) (Garrod & Fyall, 2005; Miller, 2001; Sandford & Hsu, 2007). There are two conditions in which the Delphi method is based: the first implies that, in applying multiple iterations, the amplitude of responses converges to the mean value of the distribution, whereas the second condition states that the overall response of the panel successively tends to move towards providing the correct answer, the real or the most likely. (Kaynak, Bloom, & Leibold, 1994). Interestingly, all studies have at least one iteration, providing feedback to experts about responses of the previous iteration. One of the main arguments of the use of the Delphi method is that the consensus increases over the iterations (Graham, Regehr, & Wright, 2003; Sant'Ana, 2005).

In addition to the classic Delphi, Zolingen and Klaassen (2003) describe three other models of this method: Policy Delphi, Decision Delphi and Group Delphi.

The Classic Delphi is characterised by the collection of data in a certain number of iterations and in each iteration the results of previous steps are provided until the procedure offers a certain stability in the answers, which usually results in an increase of consensus (Figure 15).

The variant of the method called Policy Delphi is more applied in social issues, and whose main differences between this and the classic method is that in this method data is collected from the experts singly throughout iterations, and the purpose of the controlled feedback is not to achieve stability of responses on a particular issue, but generate alternatives for the theme using a structured dialogue, in other words, experts respond to the questionnaires individually, and different views are compiled and provided to the panel prior to the next iteration.

The variant called Decision Delphi differs from the classic, because anonymity is partial - in other words, the experts that make up the panel are introduced but their responses are kept anonymous. This procedure aims to motivate experts to respond themselves, not leaving to assistants or others.

The Group Delphi is characterised for not having anonymity because the study is conducted in person with a panel of experts to discuss the topic under study, interacting directly with each other.

Therefore, according to Zolingen e Klaassen (2003), there are four basic models of Delphi, that despite their apparent rigidity, allow some modifications that occur quite frequently due to the large range of applications of this method (Sant'Ana, 2005). For example the first iteration in the classic model is intended for brainstorming, which begins with a questionnaire composed of open-ended questions in order to collect specific information about the subject under study to underpin the questionnaires applied in the following iterations.

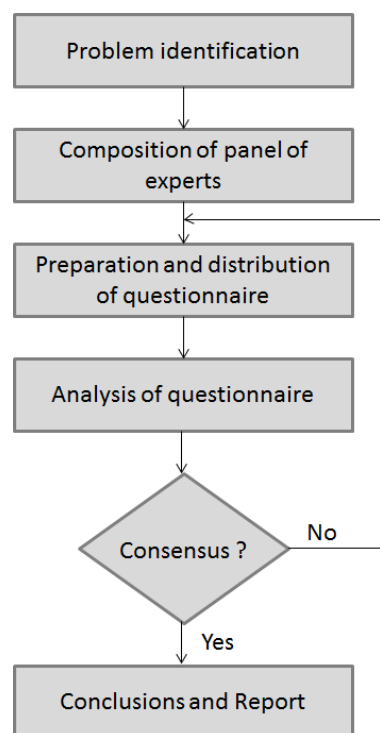


Figure 15 - Flowchart of classic process of Delphi method (adapted from Sant'Ana (2005))

However, when the collection of background information for the study is possible through an extensive literature review, the open questionnaire in the first iteration should be discarded and the deployment of the Delphi method should be begun by a questionnaire composed of closed questions targeted directly to the defined goals (Miller, 2001; Sandford & Hsu, 2007). The use of the first iteration for the collection of background information is also criticised for its inability to produce the same level of information that a careful literature review can generate (Keeney et al., 2001; L. D. Santos & Amaral, 2004; Wheeler, Hart, & Whysall, 1990). The number of

iterations required to achieve the defined objectives varies from study to study (Clemente, 2011). However, several authors state that three iterations are, in most cases, sufficient to collect the necessary information and reach a consensus, indicating also the fact that the greater the number of iterations, the greater is the likelihood of response rate being low (Clemente, 2011; Sandford & Hsu, 2007). Other authors (Kaynak et al., 1994; Keeney et al., 2001) present examples of studies where the application of two iterations was enough to achieve the intended goals.

Consensus is a fundamental element of the Delphi studies (Helmer, 1967; Rowe & Wright, 1999). However, no guidelines on setting levels of agreement in Delphi procedures could be traced in the literature (Randall, Vrijhoef, & Wilson, 2002) and few researchers have clearly defined consensus in statistical terms since the definition is often arbitrary and in many studies the decision to stop is motivated by the lack of time, human resources, budget, the sharp decrease in the response rate between iteration, among other factors (Sant'Ana, 2005; L. D. d. Santos & Amaral, 2004). Failure to offer an interpretation of the meaning of consensus is an important omission in many examples of Delphi studies (Powell, 2003).

There seems to be no firm rules for establishing when consensus is reached, although the final iteration usually shows convergence of opinion (Linstone & Turoff, 1975), with the dispersion of participants' views lessening with each iteration. Thus, it is necessary to define a priori statistical measures to assess the consensus among the panel members (L. D. d. Santos & Amaral, 2004). Mechanisms for the aggregation of scores may be open to arbitrary judgment (Murphy et al., 1998; Powell, 2003).

Powel (2003) reviewed a series of Delphi studies and concluded that consensus has been defined and achieved in a variety of ways. Setting a percentage level for inclusion of items appears to be a common interpretation (Nogueira, Azeredo, & Santos, 2012; Powell, 2003; L. D. d. Santos & Amaral, 2004). There are also researchers who choose to characterise the convergence of responses through mode, mean, standard deviation, variance or by the IQD (interquartile distance) (Clemente, 2011; Fonseca, 2012; Pereira, 2008; Rayens & Hahn, 2000; Sant'Ana, 2005). Kendall's *W* coefficient of concordance (Kendall & Smith, 1939) is also recognised as an effective coefficient to measure concordance when respondents have a list of items

to order in the questionnaire (O'Neill, Scott, & Conboy, 2010; Okoli & Pawlowski, 2004; L. D. d. Santos & Amaral, 2004; Skulmoski et al., 2007; Stevens et al., 2006). Other researchers have used Cronbach's alpha to determine the consistency and reliability of responses of the panel of experts (Graham et al., 2003; Nogueira et al., 2012; Sant'Ana, 2005).

Despite some initial controversy, currently several studies show that the method results are trustworthy and credible (Keeney et al., 2001). The Delphi method is thus considered as a reliable and valid research technique (Landeta, 2006). However, the validity of the study is only guaranteed if the member of the panel is representative of the group or area of expertise (Fish & Busby, 1996; Powell, 2003). Furthermore, the Delphi method is clearly dependent on the experiential knowledge of its panel of experts (Powell, 2003). Therefore, the scientific merit of the findings may reflect the following assertion: an empirical generalisation or communication is judged objective, true or factual if there is sufficient widespread agreement among a group of experts (Linstone & Turoff, 1975).

The number of participants that should compose the panel is a value that varies widely from study to study. It is clear that there is wide variation in the number of participants. Several studies point to consider panels with at least ten participants. However the numbers of participants varies according to the scope of the problem and the available resources but may be less than ten elements (Hasson, Keeney, & McKenna, 2000). But the more participants the better, suggesting that as the number of judges grows, the reliability of a composite judgment increases (Murphy et al., 1998). Nevertheless, the validity and reliability of the Delphi method does not increase significantly with panels which have more than thirty members (Adams, 2001). A review of Delphi studies published in Information Systems also concludes that most of these studies have panels which have between ten and thirty expert participants (Worrell, Di Gangi, & Bush, 2012). However, an expert panel as small as four is appropriate, if panellists demonstrate deep understanding of the subject matter or the focal topic requires a unique set of conditions where only few panellists are capable of contributing towards a solution (Linstone & Turoff, 1975; Worrell et al., 2012). In effect, panel size is dependent on the requirements identified in the panel

composition process as well as the characteristics of the individual panel members (Worrell et al., 2012).

In the form of a summary, the most important strengths and weaknesses of the Delphi method are hereby presented (Garrod & Fyall, 2005; Gupta & Clarke, 1996; Linstone & Turoff, 1975; Yousuf, 2007):

- The method is flexible enough to be applied to a variety of situations and in a wide range of complex problems, for which many times there is no other suitable means of analysis.
- The iterative approach allows the respondents to reconsider their decisions in the light of feedback from other members of the panel.
- The Delphi method allows participants to have more time to think about the issues presented, leading to a better quality of responses.
- Anonymity allows respondents to express their opinions freely without being subject to pressure from the other panel members. The potential influence of more significant individuals is also thereby removed.
- The issues that tend to be irrelevant to the debate can be controlled by the researcher.
- The method generates a registry of the group's thought, which can be revised as necessary.
- The method can be used to assess either the dissemination of opinion or the points of consensus.
- It prevents possible clashes at face-to-face confrontations, and also individual dominance.
- This method is indicated when there is interest in dealing with creative aspects for solving a given problem, as it motivates the independent thinking of participants.
- This method is particularly suitable when there is no historical data or when conflicting issues on ethics, society, economy and technology are observed.
- It is a relatively inexpensive method to be organised and implemented.

- It is a prospecting technique widely used and broadly tested with scientific validity and merit.
- The Delphi method may be extremely sensitive: (i) the level of knowledge of respondents, (ii) the composition of the panel of experts (iii) the clarity of questions, (iv) the way the authors of the study justify the outliers and (v) the manner of implementation of the questionnaires.
- It is assumed that respondents are willing to allow their judgments to be reformulated according to the opinion of others.
- The expert panel is vulnerable to friction situations due to boredom with the subject, disappointment with the process or lack of time to complete the questionnaire before the start of the next iteration.
- Some researchers use monetary payments or moral suasion to encourage respondents to remain in the process. These situations can lead to skewed results.
- Sometimes there is a risk of forming an illusory consensus, in which participants tend to respond according to the results of the previous iteration for dispatching the survey (or because they have little time to think properly about the issues).
- When the goal is to achieve consensus there are the issues of determining what actually constitutes the consensus because the consensus is something that is not well defined; when the iteration process should stop and when the final results should be reported.
- The Delphi method often requires a substantial period of time to be completed, which may represent an increased cost in terms of time for the researcher.
- There is the possibility of participants inadvertently or deliberately promoting undesirable outcomes. The perception of this trend should be used by the researcher as criteria to conclude the study.
- Distinguishing an expert from a layman is not always easy. Furthermore, there are the problems involved in the proof of the level of expertise of respondents

Characteristics of Continuous Assurance

besides the need to segregate the responses of these different levels of expertise.

3.3.2 Evaluation Instrument

Instrument Design

This study follows the classic process of the Delphi method (Zolingen & Klaassen, 2003) because its goal is to achieve stability of responses, or increase consensus on the answers of the experts, while maintaining their anonymity.

The implementation of the Delphi method in this study includes a variant in the first iteration of the questionnaire, namely the elimination of the first iteration of open-ended questions intended for the brainstorming, to collect specific information about the subject under study to underpin the following iterations. Thus, in this study, the Delphi method begins with a questionnaire composed of closed questions, oriented directly to defined goals. This option arises from the fact that an extensive literature review was already made (sections 2.1 and 1.2.1), one which collected the background information needed to the study.

Considering the research questions set out in section 1.2, it is necessary that the questionnaire has two essential parts:

- Part I – Evaluation of the inclusion or non-inclusion of dimensions / requirements and respective metrics in an information system which intends to offer continuous assurance services on organisational transactions.
- Part II – Evaluation of the importance of the dimensions / requirements and respective metrics in an information system which intends to offer continuous assurance services on organisational transactions. The main purpose of including this part of the questionnaire is to obtain information to assess whether there are metrics with more or less importance in the evaluation of information systems services of Continuous Assurance when compared with the other.

In addition to these two parts another initial one for characterisation of experts will be added in order to confirm and validate the basic requirements of selection of experts.

Based on the research questions of this thesis and the metrics outlined in the model presented earlier in this chapter, we selected the statements shown in Table 4 to be included in the questionnaire in order to validate the relevance of their inclusion in an evaluation model of information systems with services of Continuous Assurance. Only the metrics which are possible to quantify were considered.

Table 4 - Metrics included in the first version of the questionnaire

| Part | Metrics |
|---------------|--|
| Part I | 1. Regarding a model for implementing continuous assurance services in information systems, the inclusion of dimensions is essential for evaluating: Dimension "monitoring" - the ability of the system to monitor transactions which are intended to be audited. |
| | 2. Regarding a model for implementing continuous assurance services in information systems, the inclusion of dimensions is essential for evaluating: Dimension "compliance" – the ability of the system to verify conformity and integrity with which transactions are executed. |
| | 3. Regarding a model for implementing continuous assurance services in information systems, the inclusion of dimensions is essential for evaluating: Dimension "estimation" – the ability of the system to estimate assurance, coherence and consistency of transactions which are being executed. |
| | 4. Regarding a model for implementing continuous assurance services in information systems, the inclusion of the requirement "reporting" is essential so that the results of "monitoring", "compliance" and "estimation" functions can be presented and reported to the users of the system. |
| | 5. Dimension "monitoring" may include the following metrics to evaluate the system: Real-time monitoring of operations. |
| | 6. Dimension "monitoring" may include the following metrics to evaluate the system: Real-time identification of irregular operations. |
| | 7. Dimension "monitoring" may include the following metrics to evaluate the system: Verification of the processing of required operations at all previous steps. |
| | 8. Dimension "monitoring" may include the following metrics to evaluate the system: Detection of lack of operations. |

| | | |
|--|--|---|
| | 9. Dimension "compliance" may include the following metrics to evaluate the system: Recognition of execution patterns. | |
| | 10. Dimension "compliance" may include the following metrics to evaluate the system: Ascertaining of fulfilling of rules. | |
| | 11. Dimension "compliance" may include the following metrics to evaluate the system: Detection of potential errors. | |
| | 12. Dimension "compliance" may include the following metrics to evaluate the system: Verification of compliance of existing policies. | |
| | 13. Dimension "estimation" may include the following metrics to evaluate the system: Estimation of possible risks. | |
| | 14. Dimension "estimation" may include the following metrics to evaluate the system: Determination of possible execution patterns. | |
| | 15. The requirement "reporting" may include the following specificities: Real-time presentation of the executed operations which were monitored. | |
| | 16. The requirement "reporting" may include the following specificities: Real-time presentation of execution patterns which are being followed or are likely to be followed. | |
| | 17. The requirement "reporting" may include the following specificities: Presentation of the compliance verification in transactions executions. | |
| | 18. The requirement "reporting" may include the following specificities: Real-time presentation of the risk estimated on determining possible execution patterns. | |
| | 19. The requirement "reporting" may include the following specificities: Real-time alert for irregular situations in monitoring, compliance verification and estimation of negative results. | |
| | Part II | 20. Degree of importance of the metrics of dimension "monitoring": Real-time monitoring of operations. |
| | | 21. Degree of importance of the metrics of dimension "monitoring": Real-time identification of irregular operations. |
| | | 22. Degree of importance of the metrics of dimension "monitoring": Verification of the processing of required operations at all previous steps. |
| | | 23. Degree of importance of the metrics of dimension "monitoring": Detection of lack of operations |

| | |
|--|--|
| | 24. Degree of importance of the metrics of dimension "compliance": Recognition of execution patterns. |
| | 25. Degree of importance of the metrics of dimension "compliance": Ascertaining of fulfilling of rules. |
| | 26. Degree of importance of the metrics of dimension "compliance": Detection of potential errors. |
| | 27. Degree of importance of the metrics of dimension "compliance": Verification of compliance of existing policies. |
| | 28. Degree of importance of the metrics of dimension "estimation": Estimation of possible risks. |
| | 29. Degree of importance of the metrics of dimension "estimation": Determination of possible execution patterns. |
| | 30. Degree of importance of the specificities of the requirement "report": Real-time presentation of the executed operations which were monitored. |
| | 31. Degree of importance of the specificities of the requirement "report": Real-time presentation of execution patterns which are being followed or are likely to be followed. |
| | 32. Degree of importance of the specificities of the requirement "report": Presentation of the compliance verification in transactions executions. |
| | 33. Degree of importance of the specificities of the requirement "report": Real-time presentation of the risk estimated on determining possible execution patterns. |
| | 34. Degree of importance of the specificities of the requirement "report": Real-time alert for irregular situations in monitoring, compliance verification and estimation of negative results. |

Thus, the questionnaire is structured, as disclosed in Appendix A, in four pages: the first includes the presentation of the questionnaire and the fulfilment directions; and the following three pages comprise each constituent parts of the previously described questionnaire.

This version of the questionnaire was used to carry out the pre-tests. To this end, the questionnaire was implemented and placed online by the services provided by the University of Aveiro, namely by the area of user support of Information and

Communication Technologies Services (sTIC), having the application LimeSurvey (<https://www.limesurvey.org/>) been used.

Pre-tests

Before the disclosure of the questionnaire, pre-tests were carried out in order to ascertain which aspects of the questionnaire could be improved, and also provide appropriate solutions to improve the aspects identified. To this end, the questionnaire was tested with a small group of participants, and subsequently the data resulting from these participations were analysed to detect aspects in which improvement becomes relevant.

The method used to conduct the pre-test was based on the procedures used by Batista (2012), consisting in completing a questionnaire by the participants, followed immediately by an unstructured interview in which each participant is asked to provide their impressions of the questionnaire. The topics that are sought comments from interviews are (Batista, 2012):

- Contents - aspects on the content of the questionnaire and its questions or statements, including content that should be included, changed, or removed.
- Duration - time it may take to complete the questionnaire or its dimension.
- Scale - aspects on the scales which are used in the questionnaire, such as their suitability or the elements that constitute them.
- Structure - aspects about the structure of the questionnaire.
- Interpretation - matters which affect the interpretation of questions or statements (e.g. clarity or difficulty of interpretation).
- Completeness - the questionnaire was or not fully completed.
- Other.

Pre-tests consisted of the following set of steps (Batista, 2012):

1. Orally request the collaboration of participants to test the questionnaire. Explain the objectives of the study, the need to perform tests to validate the questionnaire and wait for eventual assent.

2. Inform that participation is anonymous.
3. In case of assent, inform the participant that there are two phases in their participation:
 - a. completing the questionnaire and registering notes by participant;
 - b. stating impressions about the questionnaire to the researcher.
4. The process of completing the questionnaire is as follows:
 - a. find a quite suitable place for completing the questionnaire;
 - b. give the following information to the participants before they start filling it in:
 - i. the researcher is present but neither interferes nor answers questions asked by the participant;
 - ii. the participant may register notes about the questionnaire: doubts about its completion; inquiries about the meaning of questions or statements; suggestions they might give to the researcher; etc;
 - iii. the researcher registers notes about completing the questionnaire.
For example, if the participant is very thoughtful on some issues, the researcher should note it and endeavour to enlighten it in the next phase;
 - c. register some data that characterise the participant;
 - d. provide the questionnaire to the participant;
 - e. the participant completes the questionnaire;
 - f. register the time taken to complete the questionnaire.
5. The participants must indicate their impressions about the questionnaire to the researcher after completing the questionnaire.
 - a. Request permission to record the impressions, emphasising the anonymity. If the participant does not want the interview to be recorded, pre-test should continue with the researcher taking notes.
 - b. Essentially, the participants should say whatever they think it is relevant, any aspects they noted.

- c. The researcher intervenes the least possible, and should especially encourage the participant in their speech.
 - d. The researcher can also use the notes taken during completion to clarify some particular aspect with the participant.
6. Finally the researcher thanks the participant.

Conduct of Pre-Tests

Five participants were requested to collaborate in pre-tests. They are professionals of the same scientific areas, or related, of the ones that experts respondents of the questionnaire are. A record sheet was prepared for each participant to conduct the pre-tests, in which some notes about participation in the pre-test and comments made by the participants were registered.

The five record sheets for each of the participants are in Appendix B in which the principal reviews about the questionnaire and some notes on the conditions of realisation of the pre-test can be read. From these sheets we conclude that the participants are distributed over four scientific areas: Management Information Systems, Management, Accounting and Auditing (as shown in Figure 16). Two of these participants indicated that they are professionals for two or more years and less than ten years, and the remaining three reported having ten or more years of experience (as shown in Figure 17). Moreover, only one participant has no scientific publications (as shown in Figure 18) and only one of the participants disagreed with the recording of the interview after the completion of the questionnaire.

The analyses of results of pre-tests are available in Appendix B. These analyses are structured in order to group the comments per topic (content, duration, structure, interpretation, scale and completeness). For each topic, the positive and negative comments are summed up, followed by their analyses to facilitate the conclusions about the changes which are needed to be made.

Characteristics of Continuous Assurance

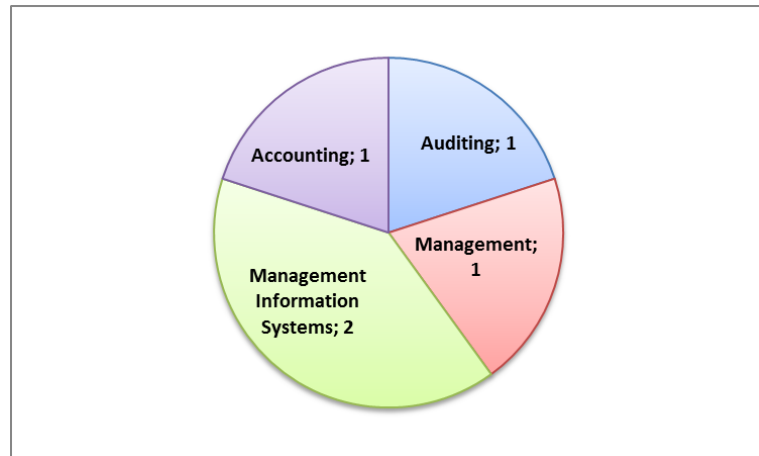


Figure 16 - Participants of pre-test by area

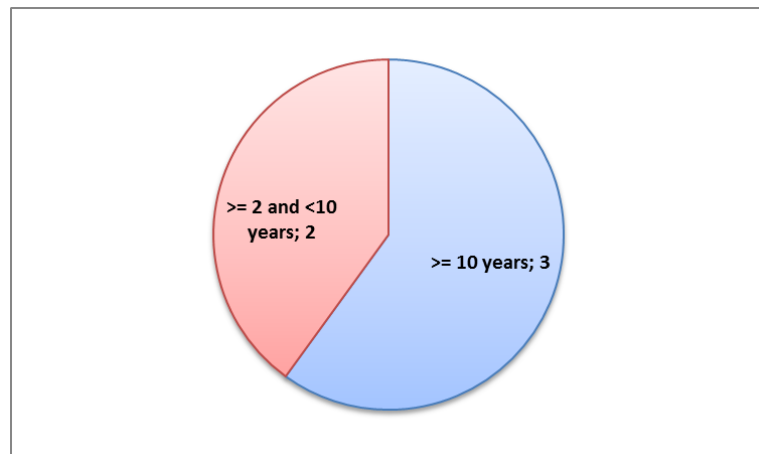


Figure 17 - Experience of participants of pre-test

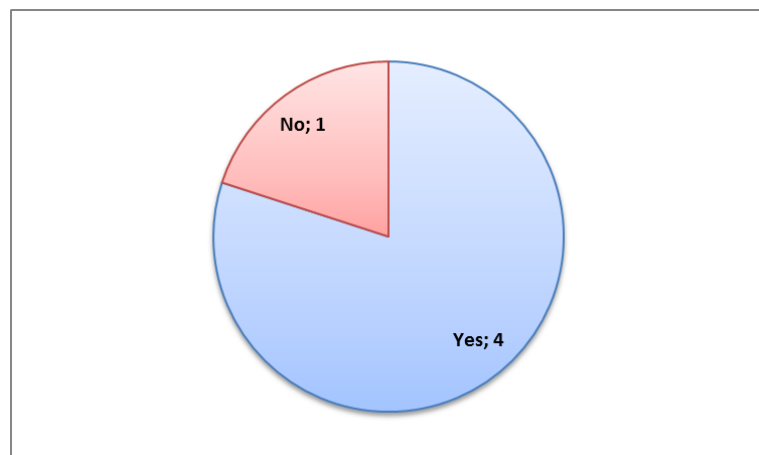


Figure 18 - Scientific publications of participants of pre-test

The final section of Appendix B presents the conclusions of the pre-tests indicating the changes that must be made to the questionnaire. According to these conclusions,

slight modifications were made to the questionnaire in three of topics: content, structure and interpretation. Every modification related to the duration, scale and completeness of the topics was made.

Appendix A shows the final questionnaire which was disclosed to the panel of experts for completion. This version of the questionnaire is similar to the original one but contemplates all the changes proposed by the findings of the pre-tests.

The pre-test also made it possible to draw conclusions about the mean time for completing the questionnaire. The average duration of completion was 10 minutes, ranging between 7 and 13 minutes. This data make it possible to inform the panel of experts about the time expected to complete the questionnaire.

Finally, Table 5 presents the statements which we intend to validate with the Delphi method.

Table 5 - Metrics included in the final version of the questionnaire

| Part | Metrics |
|---------------|--|
| Part I | 1. Regarding a model for implementing continuous assurance services in information systems, the inclusion of dimensions is essential for evaluating: The ability of the system to monitor transactions which are intended to be audited (Dimension “monitoring”). |
| | 2. Regarding a model for implementing continuous assurance services in information systems, the inclusion of dimensions is essential for evaluating: The ability of the system to verify conformity and integrity with which transactions are executed (Dimension “compliance”). |
| | 3. Regarding a model for implementing continuous assurance services in information systems, the inclusion of dimensions is essential for evaluating: The ability of the system to estimate assurance, coherence and consistency of transactions which are being executed (Dimension “estimation”). |
| | 4. Dimension "monitoring" may include the following metrics to evaluate the system: Real-time monitoring of operations. |
| | 5. Dimension "monitoring" may include the following metrics to evaluate the system: Real-time identification of irregular operations (e.g. poorly executed operations, incongruities, etc). |

Characteristics of Continuous Assurance

| | |
|--|--|
| | 6. Dimension "monitoring" may include the following metrics to evaluate the system: Real-time verification of the processing of required operations at all previous steps. |
| | 7. Dimension "monitoring" may include the following metrics to evaluate the system: Real-time detection of lack of operations. |
| | 8. Dimension "compliance" may include the following metrics to evaluate the system: Recognition of execution patterns. |
| | 9. Dimension "compliance" may include the following metrics to evaluate the system: Ascertaining of fulfilling of rules. |
| | 10. Dimension "compliance" may include the following metrics to evaluate the system: Detection of potential errors. |
| | 11. Dimension "compliance" may include the following metrics to evaluate the system: Verification of compliance of existing policies. |
| | 12. Dimension "estimation" may include the following metrics to evaluate the system: Estimation of possible risks. |
| | 13. Dimension "estimation" may include the following metrics to evaluate the system: Determination of possible execution patterns which are likely to be followed. |
| | 14. Regarding a model for implementing continuous assurance services in information systems, the inclusion of the requirement "reporting" is essential. |
| | 15. The requirement "reporting" may include the following specificities: Real-time presentation of the executed operations which were monitored. |
| | 16. The requirement "reporting" may include the following specificities: Real-time presentation of execution patterns which are being followed or are likely to be followed. |
| | 17. The requirement "reporting" may include the following specificities: Real-time presentation of the compliance verification in transactions executions. |
| | 18. The requirement "reporting" may include the following specificities: Real-time presentation of the risk estimated on determining possible execution patterns. |
| | 19. The requirement "reporting" may include the following specificities: Real-time alert for irregular situations in monitoring, compliance verification and estimation of negative results. |

| | |
|--|--|
| Part II | 20. Degree of importance of the metrics of dimension "monitoring": Real-time monitoring of operations. |
| | 21. Degree of importance of the metrics of dimension "monitoring": Real-time identification of irregular operations (e.g. poorly executed operations, incongruities, etc). |
| | 22. Degree of importance of the metrics of dimension "monitoring": Real-time verification of the processing of required operations at all previous steps. |
| | 23. Degree of importance of the metrics of dimension "monitoring": Real-time detection of lack of operations |
| | 24. Degree of importance of the metrics of dimension "compliance": Recognition of execution patterns. |
| | 25. Degree of importance of the metrics of dimension "compliance": Ascertaining of fulfilling of rules. |
| | 26. Degree of importance of the metrics of dimension "compliance": Detection of potential errors. |
| | 27. Degree of importance of the metrics of dimension "compliance": Verification of compliance of existing policies. |
| | 28. Degree of importance of the metrics of dimension "estimation": Estimation of possible risks. |
| | 29. Degree of importance of the metrics of dimension "estimation": Determination of possible execution patterns which are likely to be followed. |
| | 30. Degree of importance of the specificities of the requirement "report": Real-time presentation of the executed operations which were monitored. |
| | 31. Degree of importance of the specificities of the requirement "report": Real-time presentation of execution patterns which are being followed or are likely to be followed. |
| | 32. Degree of importance of the specificities of the requirement "report": Real-time presentation of the compliance verification in transactions executions. |
| | 33. Degree of importance of the specificities of the requirement "report": Real-time presentation of the risk estimated on determining possible execution patterns. |
| 34. Degree of importance of the specificities of the requirement "report": Real-time alert for irregular situations in monitoring, compliance verification and estimation of negative results. | |

Panel of Experts

As previously mentioned, the choice of experts to constitute the panel is one of the sensitive aspects of the Delphi method, because a suitable expert panel is essential to assure the validity of the findings.

The panel design was begun by the identification of relevant disciplines to the topic of study. Thus, three areas were chosen:

- Auditing;
- Management;
- Management Information Systems.

The choice of the discipline Auditing is due to the fact that the subject of study focuses on the implementation of continuous assurance services, which is strongly related to auditing and continuous monitoring. However, it was decided to call it Auditing, because most experts who have studied and worked in Continuous Assurance have mentioned Auditing as their area of interest. Then, for a better understanding, this area was designated as Auditing.

The discipline Management was chosen by the impact that the implementation of Continuous Assurance services have on organisational management, particularly in support of decision making and in strategic management of organisations, as evidenced in section 2.1.

Because the study focuses on the implementation of Continuous Assurance services in information systems, it is inevitable to include experts of the discipline Management Information Systems, due to their knowledge and expertise on information systems within organisations and their overriding role in functional, decision-making and strategic support in organisations.

Subsequently, some elements of the consultation were surveyed, namely the identification of:

- relevant literature related to the topic of study;
- national and international organisations and entities (public or private) tied to the topic of interest;

- social networks and other electronic communities with relevant expertise to the current study.

From these elements of consultation, we collected names and contacts of experts who, through their curricula vitae, demonstrate expertise in the subject of study, as follows:

- expert of Auditing area directly related to either Continuous Assurance, Continuous Auditing or Continuous Monitoring;
- expert of Management area directly related to strategic management and process management;
- expert of Management Information System area directly related to information systems oriented to decision support or related to internal control, continuous auditing or monitoring.

The relation between the specialists and the topic of study was measured by the following aspects:

- qualifications;
- professional experience;
- scientific publications.

A more refined selection was made from the list of identified experts, taking into consideration the following requirements:

- Qualifications - If the expert is an academic or researcher, having a PhD degree is an essential requirement to be considered or at least, a master's degree if the expert is a practitioner.
- Professional experience – It is essential requirement that the expert has ten or more years of experience. Experts with less than 10 years of experience were also considered if their experience was greater than or equal to two years and was directly related to the area of Continuous Assurance.

For the Auditing area, we considered researchers and academics affiliated to Portuguese or international institutions of higher education and research units;

independent professionals or belonging to national or international organisations that provide auditing services to companies.

In the Management area, we considered academics and researchers affiliated to Portuguese or international institutions of higher education and research units; top-level managers of public and private Portuguese or international organisations.

In the Management Information Systems area, we considered researchers and academics affiliated to Portuguese or international institutions of higher education and research units; independent professionals or belonging to national or international organisations that provide consulting services in the Information Systems Management area.

- Publications – Only experts with scientific publications in their area were considered.

After the first contact, some of the selected experts suggested other experts whose profile is consistent with the topic of study. Thus, we selected 23 experts distributed for the three areas, as follows:

- Auditing: 9 experts
- Management: 5 experts
- Management Information Systems: 9 experts

For the constitution of the panel an e-mail was sent (Appendix C) for the initially selected 23 experts requesting collaboration in this study, for participating as a respondent in the panel of experts. Besides the request for collaboration, the e-mail informed, in a brief way, the topic of study and the conditions of their participation in the study.

This e-mail obtained 14 responses, 10 of which informed about the acceptance of collaboration. Table 6 and Figure 19 show the status of response and non-response to this first e-mail.

Table 6 – Status of answers of request for collaboration by area

| | Sent | Accepted | Not accepted | No Answer |
|---------------------------------------|-----------|-----------|--------------|-----------|
| Auditing | 9 | 3 | 1 | 5 |
| Management | 5 | 3 | 1 | 1 |
| Management Information Systems | 9 | 4 | 2 | 3 |
| Total | 23 | 10 | 4 | 9 |

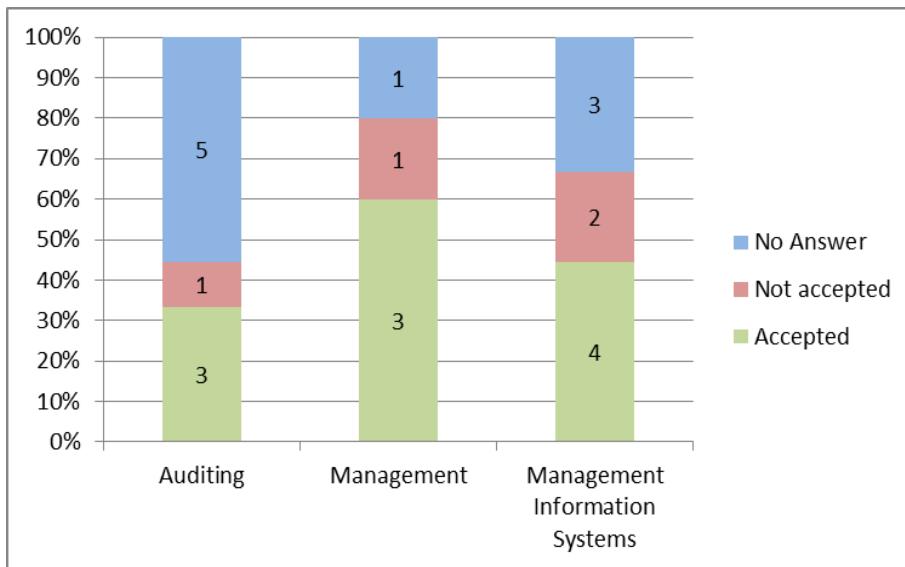


Figure 19 - Status of answers of request for collaboration by area

Then, the panel constituted by 10 elements: 3 of the Auditing area; 3 of the Management area and 4 of the Management Information Systems area.

Some aspects about the selection of experts, namely organisations which experts are affiliated to or literature which was consulted were not detailed so that this information would not compromise the anonymity of the participants who constitute the panel.

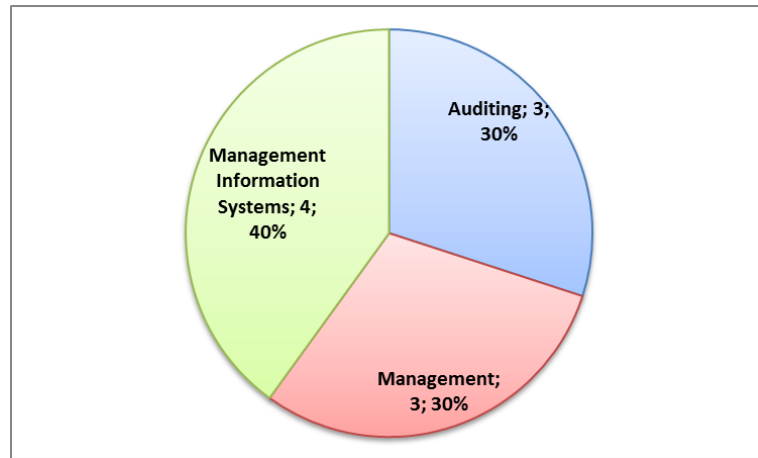


Figure 20 - Composition of the Panel of Experts by Area

Consensus

As mentioned in the section of presentation of the Delphi method, the concept of consensus is not widely defined and, therefore, it is left to the judgment of each researcher to determine the statistical measures for assessment of consensus in each study before its beginning. Thus, consensus among the members of the panel of experts is also necessary to be statistically defined in this study.

Setting a percentage level for inclusion of items appears to be a common interpretation. Thus, this was also the option to define consensus in this work. Since the response scales in the questionnaire are scales of agreement (with five options, in which 1 means totally disagree and 5 means totally agree) and importance (also with five options, in which 1 means unimportant and 5 very important) the definition of consensus is based on studies with similar design (Feitosa & Nascimento, 2003; Goossen, 2000; Nogueira et al., 2012; Sousa, MHLBC, & Mendonça, 2005). Hence, in this study, consensus of inclusion or importance is set as shown in Table 7. In addition, the consensus is also defined according to three levels: excellent, high and moderate, as shown in Table 8.

Table 7 - Consensus definition (using a 5 score scale)

| Consensus | Definition |
|---------------------------|--|
| Inclusion Criteria | 75% of responses should be scored 4 or 5 |
| Exclusion Criteria | 75% of responses should be scored 1 or 2 |
| No Consensus | Other cases |

Table 8 - Criteria for classification of the level of consensus

| | | |
|---------------------------|------------------|--------------------------------|
| Inclusion Criteria | Excellent | Percentile 25 = 5 Mode = 5 |
| | High | Percentile 25 < 5 Mode = 5 |
| | Moderate | Percentile 25 >= 4 Mode = 4 |
| Exclusion Criteria | Excellent | Percentile 75 = 1 Mode = 1 |
| | High | Percentile 75 > 1 Mode = 1 |
| | Moderate | Percentile 75 <= 2 Mode = 2 |
| No Consensus | | Other cases |

The study comes to an end when the third iteration is completed or high or excellent consensus is obtained in all statements of the questionnaire in the previous iteration.

3.3.3 Application of Delphi Method

First Iteration

For the first iteration of the Delphi method an e-mail was sent (Appendix C) to thank for the acceptance of the collaboration request and informing the questionnaire URL. Furthermore, the e-mail intended to reinforce the importance of the questionnaire response to the feasibility of the study and to remember that the anonymity and confidentiality participation in the study was guaranteed. Moreover, this e-mail informed the experts that the mean time to complete the questionnaire was about ten minutes and asked that the answer was given within seven days.

Seven days after another e-mail (Appendix C) was sent asking that those who had not yet had opportunity to complete the questionnaire did so within 2 days to make the study possible to be continued. This e-mail was sent because the number of responses was still less than the number of experts who constitute the panel. After this e-mail, all responses were obtained.

Results of First Iteration

Regarding the characterisation of the expert panel, the following results were obtained:

- Area of expertise – responses were consistent with the profile initially outlined in the process of choice of experts, i.e. the distribution of the experts by area is exactly the same: four experts of Management Information Systems area, three of Auditing area and three of Management area (Figure 21).
- Experience – responses confirmed the criteria used to select the experts. Thus the panel was constituted by a majority of experts with experience greater than or equal to ten years and the remaining with experience greater than or equal to two years (Figure 22).
- Scientific publications – responses confirmed the criteria used to select the experts because all experts confirmed having publications in their area of expertise.

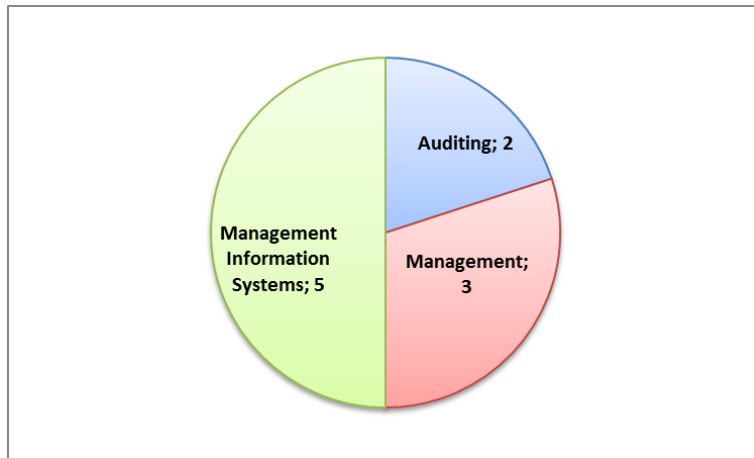


Figure 21 - Composition of the panel of experts by area (answers by experts)

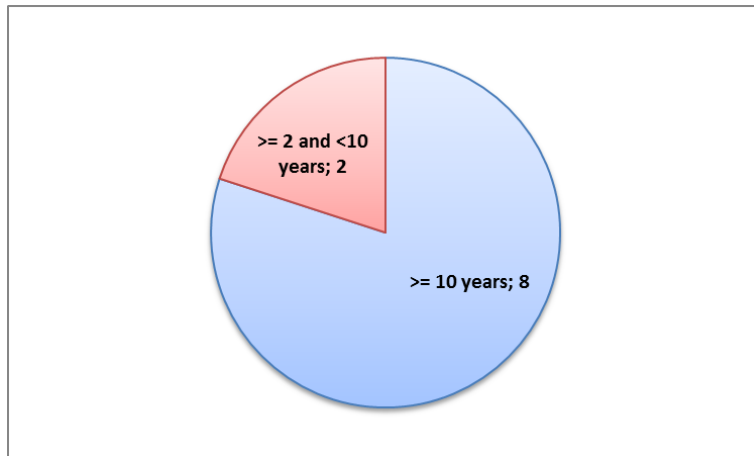


Figure 22 - Experience of experts (answers by experts)

With regard to responses to statements of Parts I and II of the questionnaire, Table 23 (Appendix D) shows the distribution of responses by the five response options which were available in Part I of the questionnaire and Table 24 (Appendix D) shows the distribution of responses by the five response options in Part II of the questionnaire. The distribution of responses by each statement is shown in Appendix VI (available in the CD which supports this thesis).

According to the criteria of inclusion and exclusion of consensus definition presented in Table 7 and the data presented in Table 23 (Appendix D) and Table 24 (Appendix D), we conclude that:

1. There is consensus in the panel of experts with regard to the inclusion of statements of Part I, because all statements have 75% or more of their responses located in the options "agree" (score 4) and "strongly agree" (score 5).
2. There is consensus in the panel of experts with regard to the inclusion of statements of Part II, because all statements have 75% or more of their responses located in the options "important" (score 4) and "very important" (score 5).

Taking into consideration Table 8, which defines the level of consensus of responses of the expert panel and Table 27 (Appendix D) and Table 28 (Appendix D), which show the statistical data required to determine this level of consensus, namely the mode and some percentiles of responses to each statement, we observed that:

3. There is moderate consensus in 6 statements (3 in each part) out of a total of 34 statements included in the questionnaire.
4. There is high consensus in 21 statements (13 in Part I and 8 in Part II) out of a total of 34 statements included in the questionnaire.
5. There is excellent consensus in 7 statements (3 in Part I and 4 in Part II) out of a total of 34 statements included in the questionnaire.

Moreover, the value of Cronbach's alpha for the results of this iteration is 0.965. The Cronbach's alpha is a coefficient frequently used to evaluate the extent of agreement among participants with respect to the ranking of subjects – in other words, it allows to quantify the reliability of a summation of entities, in this case, panellists. This coefficient is expressed as a number between 0 and 1 and a low value of alpha could be due to a low number of questions, poor interrelatedness between items or heterogeneous constructs. Furthermore, a value greater than 0.70 is considered as good reliability and internal consistency of responses (Bland & Altman, 1997; Tavakol & Dennick, 2011). Thus, our alpha means that our results for this iteration are reliable.

The above observations allow us to conclude that the first iteration is not conclusive regarding the consensus which was reached and that a second iteration of the questionnaire is necessary. This conclusion was based on the condition previously established, which determines that the Delphi method is concluded after the third iteration or before the third iteration if consensus is reached with high or excellent level in all statements of the questionnaire. Since this is the first iteration and there was no consensus of high or excellent level in all statements, a second iteration was required to try to increase consensus among the experts of the panel about the statements presented in the questionnaire.

Second Iteration

A second iteration was prepared because the intended consensus was not obtained in the previous iteration. Despite consensus which was obtained in all statements of the questionnaire, the method was not concluded because a high and excellent level of consensus was not obtained in all statements, as pre-established in the definition of consensus in this work.

The questionnaire of this iteration is equal to the one of the previous iterations but some statistical data on the results of the previous iteration were added, namely the distribution of responses by answer option for each statement, as shown in Appendix A.

For the second iteration of Delphi method another e-mail was sent (Appendix C) to thank for the participation in the previous iteration and to inform the questionnaire URL. This e-mail also reported that the questionnaire of this iteration was exactly equal to the first iteration. Nevertheless some statistical information about the results achieved in the first iteration is presented throughout this questionnaire. This intended that experts were able to re-evaluate their answers, if they wished so. However, the e-mail reinforced that the most important was that their answers reflected their real opinion about each of the statements. Moreover, this e-mail noted the importance of the questionnaire response to the feasibility of the study and that the anonymity and confidentiality participation in the study was guaranteed. In addition, the e-mail asked for responses within seven days.

Seven days after another e-mail (Appendix C) was sent asking that those who had not yet had opportunity to complete the questionnaire did so within 2 days to allow the study to be continued. This e-mail was sent because the number of responses was still less than the number of experts who constitute the panel. After this e-mail, all responses were obtained.

Results of Second Iteration

In this iteration only 9 responses were considered valid out of the 10 responses received. One of the responses was not considered because the respondent disagreed with a statement on the requirement Reporting, namely "Real-time presentation of execution patterns which are being followed or are likely to be followed", in Part I. However, the respondent indicated that this statement was very important in Part II of the questionnaire. Because of this inconsistency, this response was not considered for the result analysis.

As regards to responses to statements of Parts I and II of the questionnaire, Table 25 (Appendix D) shows the distribution of responses by the five response options which were available in Part I of the questionnaire and Table 26 (Appendix D) shows the distribution of responses by the five response options in Part II of the questionnaire. The distribution of responses by each statement is shown in Appendix VI (available in the CD which supports this thesis).

According to the criteria of inclusion and exclusion of consensus definition presented in Table 7 and the data presented in Table 25 (Appendix D) and Table 26 (Appendix D), we conclude that:

1. The consensus in the panel of experts with regard to the inclusion of statements of Part I remained, because all statements have 75% or more of their responses located in the options "agree" (score 4) and "strongly agree" (score 5).
2. The consensus in the panel of experts with regard to the inclusion of statements of Part II remained, because all statements have 75% or more of

their responses located in the options "important" (score 4) and "very important" (score 5).

Taking into consideration Table 8, which defines the level of consensus of responses of the expert panel and Table 29 (Appendix D) and Table 30 (Appendix D), which show the statistical data required to determine this level of consensus, namely the mode and some percentiles of responses of each statement, we observed that:

3. There is high consensus in 15 statements (8 in Part I and 7 in Part II) out of a total of 34 statements included in the questionnaire; these 15 high consensus represent 6 level rises from moderate level in the first iteration to high level in the second iteration; and 9 high consensus that remained from the first iteration.
4. There is excellent consensus in 19 statements (11 in Part I and 8 in Part II) out of a total of 34 statements included in the questionnaire; these 19 excellent consensus represent 12 level rises from high level in the first iteration to excellent level in the second iteration; and 7 high consensus that remained from the first iteration.

Moreover, the value of Cronbach's alpha for the results of this iteration is 0.814. We noted a slight decrease on this value when compared to the first iteration. The loss of one valid response for the second iteration could have influenced the value of alpha, because Cronbach's alpha is sensitive to the number of items or, in this case, panellists. The loss of one valid response would be more likely to decrease the value of this coefficient (Graham et al., 2003). The possibility to assign the decline of the value to the decrease of consensus does not make much sense since it was noted a decrease in dispersion of responses and an increase of homogeneity of responses within a few answer options. However, this value is greater than 0.7, which means that there is a very good internal consistency of responses.

From the foregoing, we concluded that the second iteration was conclusive regarding the consensus which was reached, which means that the Delphi method was completed at this iteration. This conclusion was based on the previously established

Characteristics of Continuous Assurance

condition, which determines that the Delphi method is concluded after the third iteration, or before the third iteration if consensus is reached with high or excellent level in all statements of the questionnaire. Although this was the second iteration, there was already consensus of high or excellent level in all statements. Thus, no more iteration was needed to be prepared.

3.4 CONCLUSION

The result obtained through the Delphi method to validate the proposed evaluation model was positive because it achieved the intended goal: consensus in the panel of experts. In this case, at the end of the study (after the second iteration) consensus of inclusion was reached in all statements of Part I of the questionnaire and also consensus on the importance of all statements in Part II of the questionnaire.

Furthermore, high consensus was reached in approximately 44% and excellent consensus in approximately 56% of all statements of the questionnaire. In Part I there was high consensus approximately in 42% and excellent consensus in 58% of the statements. In Part II consensus was high in approximately 47% and excellent in 53% of the statements.

The totality of experts strongly agreed with the inclusion of dimensions "monitoring" and "compliance" and the requirement "reporting". Regarding the dimension "estimation", all experts agreed with its inclusion, but only 78% strongly agreed. Hence, we conclude that the dimensions and the requirement are relevant to be included in an evaluation model of information systems with continuous assurance services.

As regards the metrics of the dimension "monitoring", all experts strongly agreed with the inclusion and considered very important the metrics: "real-time monitoring of operations", "real-time identification of irregular operations" and "real-time detection of lack of operations". Despite not being the totality of experts, an overwhelming majority of experts also strongly agreed with the inclusion, and considered the metric "real-time verification of the processing of required operations at all previous steps" very important.

With regard to the metrics of the dimension "compliance", all experts strongly agreed with the inclusion and considered the metric "detection of potential errors" very important. Also a vast majority of experts strongly agreed with the inclusion and considered the other metrics of this dimension very important. The proportion of experts who strongly agreed with the inclusion of these metrics is similar to the proportion of experts who considered them very important.

In regard to the metrics of the dimension “estimation”, 78% of experts strongly agreed with their inclusion and 67% considered them very important.

Regarding the metrics of the requirement “reporting”, all experts strongly agreed with the inclusion and considered the metric “real-time alert for irregular situations in monitoring, compliance verification and estimation of negative results” very important. Also a vast majority of experts strongly agreed with the inclusion and considered the following metrics: “real-time presentation of execution patterns which are being followed or are likely to be followed”, and “real-time presentation of the risk estimated on determining possible execution patterns” very important. The proportion of experts who strongly agreed with the inclusion of these metrics is similar to the proportion of experts who considered them very important. As regards the metrics “real-time presentation of the compliance verification in transactions executions” and “real-time presentation of the executed operations which were monitored”, all experts strongly agreed with their inclusion but a small minority considered that they are important instead of very important.

Of the foregoing, we are able to validate the proposed model. Thus, Table 9 presents the dimensions and requirements and their respective metrics (M1- M15) of the evaluation model of information systems with continuous assurance services, which were considered for evaluation with the Delphi method, with slight changes compared with those initially presented (Figure 14). These changes are not about content but the way they are presented; these changes are due to the results of pre-tests.

The consistency of the model is verified by the bibliographic survey, and later by the expert panel validation with consensus. The coherence of this model is validated by the scientific rigour with which the Delphi technique was implemented and by the contents and structure of the evaluation instrument (questionnaire) whose first part was used to allow experts to give their opinion about the inclusion of each metric, and in the second part about their importance. The fact that it has been found that all metrics proposed for inclusion in the model have also been considered important or very important in a continuous assurance system gives coherence to the list of proposed items.

The list of items is not complete because as already mentioned only those which are quantitatively measurable have been considered and included in the model, since the aim of this work is to propose an effective architecture, and then the assessment of the qualitative outcomes (net benefits) is given for future work. However, for the same reasons, the proposed model is appropriate because it is narrowly focused on the objectives of the work.

Table 9 - Dimensions and requirement of the model and their metrics after validation

| Dimensions and Requirement | Metrics |
|-----------------------------------|--|
| Monitoring (dimension) | M1. Real-time monitoring of operations M2. Real-time identification of irregular operations M3. Real-time verification of the processing of required operations at all previous steps M4. Real-time detection of lack of operations |
| Compliance (dimension) | M5. Recognition of execution patterns M6. Ascertaining the fulfilling of rules M7. Detection of potential errors M8. Verification of compliance of existing policies |
| Estimation (dimension) | M9. Estimation of possible results M10. Determination of possible execution patterns which are likely to be followed |
| Reporting (requirement) | M11. Real-time presentation of the executed operations which were monitored M12. Real-time presentation of execution patterns which are being followed or are likely to be followed M13. Real-time presentation of the compliance verification in transactions executions M14. Real-time presentation of the risk estimated on determining possible execution patterns M15. Real-time alert for irregular situations in monitoring, compliance verification and estimation of negative results |

4

SOLUTION PROPOSAL

This chapter aims to present a proposal which shows evidence of being effective in achieving the stated objectives and which enables- to obtain the needed results to meet the raised research hypotheses. In this proposal both the requirements that must be implemented and a possible conceptual architecture to meet these requirements are presented.

Moreover, this chapter describes an implementation which allowed to test the prototype in a simulated organisational environment and to collect data in order to validate the effectiveness of the proposed solution.

4.1 CONCEPTUAL DESIGN

The objective of this section is to present the requirements of the information system, which is the prototype of the solution proposal. These requirements are based on the research hypotheses. The chapter 3 also heavily contributed to the definition of these requirements, because it is strongly linked to the research hypothesis H1.1, and therefore presents a set of characteristics that any information system with continuous assurance services should possess.

Thus, the considered requirements are the following:

- Req1 - The system should be able to record the operations which compose the organisational transactions and which are performed in the operational information system.
- Req2 - The system should enable the instantiation of risk profiles associated with organisational transactions, which are intended to be monitored, controlled and audited.
- Req3 - The system should be capable of recognising risk profiles, which were followed by the already concluded organisational transactions.

- Req4 - The system should be capable of determining possible risk profiles, which are being followed or likely to be followed by organisational transactions still in progress.
- Req5 - The system should provide the presentation of the executed operations, which were monitored.
- Req6 - The system should provide the presentation of execution patterns, which are being followed or are likely to be followed.
- Req7 - The system should provide the presentation of results of the compliance verification in transactions executions.
- Req8 - The system should provide the presentation of risk estimated on determining possible execution patterns.
- Req9 - The system should be able to alert for irregular situations in monitoring, compliance verification and estimation of negative results.
- Req10 - The system should provide its functionalities in real time.

From the enumeration above, the first nine items are functional requirements and the last one (Req10) is a performance requirement. In addition to the aforementioned requirements, there are other requirements which should be considered in any system development process. These requirements are related to dynamical systems and the respective concepts of system observability and controllability (Franklin, Powell, & Emami-Naeini, 1994; Ribeiro, 2002).

In this context, observability means that the system output must be affected by every state variable, i.e. for any possible state variable, the current state can be determined in finite time by the measuring of output. If there is a state which cannot be observed from the outputs, the state is defined unobservable and thus the system is not completely observable or unobservable. A system is defined completely controllable if every state variable is able to be controlled to reach a concrete objective in finite time by some unconstrained control $u(t)$. Otherwise, it is defined as uncontrollable or not completely controllable, if there are state variables which are not dependent on the control $u(t)$, and therefore it is not possible to achieve the desired

objectives in finite time from those state variables (Franklin et al., 1994; Ribeiro, 2002).

On analysing the previously defined requirements, different areas of the system may be delineated so that desired results are achieved. Thus, the following considerations must be taken into account in the conceptualisation of the solution:

- C1. A layer of internal control mechanisms should be conceptualised in order to be incorporated (preferably non-intrusive) in the operational information system (e.g. ERP system), which supports the execution of the organisational transactions to be monitored and audited. These internal control mechanisms when embedded into operational information system must be aligned with the ontological model of Dietz, already studied, that is to say the design of these mechanisms will have to take into account the different types of events, stages and relationships that constitute the essence of each transaction. This consideration indirectly addresses the requirement Req1, because the internal control mechanisms are the artefacts responsible for the detection of operations and for the collection of the needed data for their recording and monitoring.

- C2. Internal control mechanisms embedded in the transactions, which need a component that manages and stores the results from these mechanisms. This component should be able to record, maintain and manage all the data derived from internal control mechanisms and that represents the transactional events occurring on-line. This consideration directly addresses the requirement Req1.

- C3. A key requirement of this proposal is the development of risk profiles repository specified in the statement of the research problem and in the research hypothesis H3.1. This repository should be able to maintain and manage the known negative and positive risk profiles of each organisational transaction to be monitored and audited. These profiles must be modelled according to the ontological model studied. This consideration directly addresses the requirement Req2.

C4. To meet directly the requirements Req3 and Req4, another software artefact must be conceptualised and prototyped. This module should be capable of comparing the data from the internal control mechanisms with the records maintained in the Risk Profiles Repository and then to be able to recognise the execution pattern (risk profile) of every organisational transaction execution, which is already concluded or still in progress.

Because risk profiles minutely represents and characterises the essence of organisational transactions, the ability to recognise risk profiles also enables to:

- C4.1. Determine which profile is being followed by running each transaction (both the complete and incomplete ones), because the system should recognise the risk profiles for every transaction execution regardless of their state of completeness, since its initiation. Therefore, before the completion of the transaction execution, the risk profile or risk profiles, which are being followed by the transaction execution, are already possible to be estimated; however, if the transaction execution is following none of the risk profiles defined in the Risk Profile Repository, the system should present this execution as an unknown transaction;
- C4.2. Estimate possible results, because on recognising the possible risk profile of an organisational transaction still in progress, the system should qualitatively estimate the results. If there is not a possible positive risk profile associated with the transaction execution, it means that the organisational transaction will result in a negative or unknown situation for the organisation. Furthermore, if the possible risk profiles associated with the transaction execution are positive, results without negative effects for organisations are predicted;
- C4.3. Ascertain the fulfilling of rules and policies because on recognising the risk profile, all policies and rules, which were defined in every risk profile, should be automatically checked. To be more specific, rule refers to all conditions imposed by national or international directives,

while policy refers to a set of procedures defined internally by each organisation. The concepts of rule and policy are not differentiated in this thesis because their only difference lies in their origins, and their implementation in the definition of risk profile is exactly the same. Moreover, the aim of the study is to validate the ability to audit guidelines, regardless of the fact they are rules or policies;

C4.4. Detect potential errors, because on recognising the possible risk profiles for every transaction execution, the system is assessing these possible risk profiles regarding their type (negative or positive). Thus, the system should correctly identify the type of the identified possible risk profile, as well as all transactions which follow unknown risk profiles. Thus, when the system identifies possible negative risk profiles or unknown risk profiles, it is detecting potential errors on the transaction execution;

C4.5. Identify irregular operations because when the system is able to verify the non-fulfilling of rules; to detect potential errors; and to detect the compliance of existing policies, it should identify the irregular operation, which is causing the negative situation (e.g. delay in execution, unauthorised executor or unexpected operation);

C4.6. Detect the lack of operations, because this lack should be detected during the continuous comparison with the defined risk profiles in the Risk Profiles Repository. When an operation is lacking, and this lack is safeguarded in a defined risk profile, this risk profile is automatically indicated and associated with this fault;

C4.7. Verify the processing of required operations at all previous steps, because when a risk profile is identified for an organisational transaction execution, all performed operations, which comprise it, are also checked, so that they may be validated regarding the definition of the risk profile of this transaction.

C5. The on-line results of the Transaction Comparator module should be presented to the users of the system through an interface and a report. This interface and

report should contain the history of the results of the transaction auditing and monitoring and a picture of the current situation regarding the organisational transactions still in progress. Furthermore, notifications to the users in negative situations should be provided. This consideration directly addresses the requirements Req5, Req6, Req7, Req8 and Req9.

The above considerations address the dual requirements of observability and controllability. This happens because the considerations aim that the system has a processor that considers all received inputs in order to achieve the desired and defined goals. It is intended that all events detected by the internal control mechanisms are handled by this processor, grouping them by respective transactions and business processes, and providing a qualitative evaluation on how these transactions are being executed (fourth consideration). There should not be any unprocessed events, even if it means creating a new event group (transaction) or the classification of a transaction as unknown, when no other option is possible. This addresses the requirement of controllability. In addition, any event from internal control mechanisms shall result in a change in the system output, from its inclusion in a transaction to an eventual change in the qualitative evaluation of the transaction or any alarm activation. These results are visible in the different system's outputs: the system interface, reports and alarms (fifth consideration). This addresses the requirement of observability.

The aforementioned requirements and considerations have been defined so that the final prototype can achieve the main goals and allows to support and answer the main research questions. Thus, these requirements and considerations have been conceptualised having as reference the need of all the characteristics of Continuous Assurance of being verified in the prototype outcomes. It means that every requirement and consideration is related to one or more characteristics of Continuous Assurance (M1-M15) stated in Table 9. Table 10 shows this relationship between functional requirements, development considerations and the characteristics of Continuous Assurance.

Table 10 - Relationship between functional requirements, development considerations and the considered metrics of Continuous Assurance

| Requirements <i>(pp. 106-107)</i> | Considerations <i>(pp. 108-111)</i> | Metrics of Continuous Assurance <i>(p. 105)</i> | |
|---|--|---|--|
| Req1 | C1 | M1 - Real-time monitoring of operations | |
| | C2 | | |
| Req2 | C3* | *supports consideration C4 | |
| Req3 Req4 | C4 | C4.1 | M5 - Recognition of execution patterns |
| | | C4.2 | M9 - Estimation of possible results |
| | | | M10 - Determination of possible execution patterns which are likely to be followed |
| | | C4.3 | M6 - Ascertaining the fulfilling of rules |
| | | | M8 - Verification of compliance of existing policies |
| | | C4.4 | M7 - Detection of potential errors |
| | | C4.5 | M2 - Real-time identification of irregular operations |
| | | C4.6 | M4 - Real-time detection of lack of operations |
| C4.7 | M3 - Real-time verification of the processing of required operations at all previous steps | | |
| Req5 | C5 | M11 - Real-time presentation of the executed operations which were monitored | |
| Req6 | | M12 - Real-time presentation of execution patterns which are being followed or are likely to be followed | |
| Req7 | | M13 - Real-time presentation of the compliance verification in transactions executions | |
| Req8 | | M14 - Real-time presentation of the risk estimated on determining possible risk patterns | |
| Req9 | | M15 - Real-time alert for irregular situations in monitoring, compliance, verification and estimation of negative results | |

With the aforementioned, an architecture was conceptualised in order to provide a solution to the problem addressed in this thesis (R. P. Marques, Santos, & Santos, 2012b, 2012c). Figure 23 schematically represents the conceptual architecture proposed.

From the analysis of the architecture represented in Figure 23, we perceive that the proposal (area bounded by the rectangle designated as Proposed Solution) is intended to be permanently connected to the operational information system of the organisation, e.g. ERP system. That is to say internal control mechanisms should be incorporated in the operational information system in order to monitor the status of the various phases and stages (defined by the ontological model studied) of organisational transactions according to the first specified requirement, supporting thus the proposed system, and consequently the monitoring and auditing of organisational transactions.

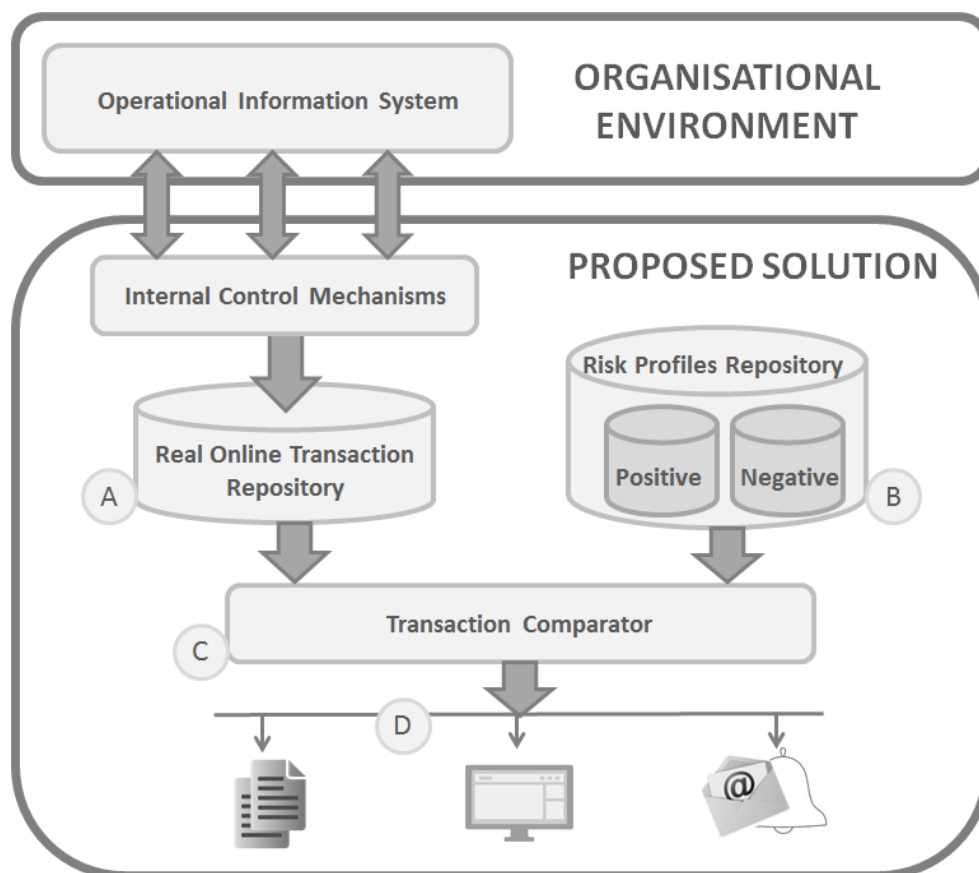


Figure 23 - Conceptual architecture of the proposed solution

These internal control mechanisms must provide data about the monitored operations to the Real Online Transaction Repository (component A of the architecture), which manages and maintains this information referring to the various states of execution of transactions, as specified in the requirement Req1 and in the second consideration (C2).

To meet the third consideration (C3) and the requirement Req2, the architecture has the component B, which illustrates the Risk Profiles Repository of the organisational transactions to be monitored and audited.

The component C is the module intended to be able to compare the various records in the Risk Profiles Repository and determine which profile is being followed by running each transaction, according to information received by component A. It meets the requirements Req3 and Req4 and the fourth consideration (C4).

For the fifth consideration (C5), and also for the requirements Req6, Req7, Req8 and Req9, the results of the organisational transactions monitoring carried out by comparison module (component C) are made available to the users of the system through different media (component D), enabling the viewing of the current and historic state of controlling of the audited transactions.

To meet the requirement about the real-time function (Req10), some aspects should be considered (R. P. Marques, H. M. D. Santos, & C. Santos, 2013c): the time and the rhythm of organisational transactions are variable and in different orders of greatness (transactions may have running times in the order of minutes, days or several months depending on the situation in question); a real-time system is one, where the correctness not only depends on the functionality but also on the timeliness of this functionality (Möller, 2002). Thus, because the purpose of the system is not to act in a direct and intrusive way on execution of organisational transactions, but rather to control, monitor, audit and then work with reporting functions, the real-time concept is defined within this work as the interval of time closer to the occurrence of an event. This interval of time may be variable but it is the time which allows the user of the system to effectively react in a corrective way, after being alerted of an anomaly. It is variable because it also depends on the pace and the rhythm of the transaction in question.

4.1.1 The role of Enterprise Ontology

The main role and objective of the ontology adopted in this work, is to provide the abstraction and semantic which are necessary to formally represent organisational transactions in a concise, objective, microscopic and detailed way. This representation intends to give adaptability and flexibility to the proposed solution making it applicable to any business context and any type of organisational transaction and process.

The Enterprise Ontology supports this work in many aspects and in many modules of this solution. This section aims to briefly explicit this support in order to make clear the situations of its application. This is thoroughly described in the next section about the solution development.

The module where ontology application is more evident is the Risk Profiles Repository, because it aims to be able to represent organisational transactions of any kind in any business area, and to be a database of patterns of execution of organisational transactions (risk profiles) used as references of how they can be carried out. Thus, the Enterprise Ontology is used to represent the essence of every risk profile defined in the repository, i.e. all events, facts and operations which make up the transactions, their relationships, and the rules and operational guidelines about how the transactions should be executed. It means that this repository meets the Action Model, Process Model and State Model. Therefore, the conceptualisation and design of this module should take into consideration the issues of these models, as it is verifiable by analysing section 4.2.3.

Another important contribution given by the ontology is the conceptualisation of the internal control mechanisms. The explanation of which internal control mechanisms are necessary to develop and implement is based on the modelled risk profiles. This modelling allows to know the essence of the transaction and then to identify what is important to control and monitor in the operational database, and therefore develop internal control mechanisms in those interest points for monitoring. Thus, the ontology provides the necessary knowledge to define the internal control mechanisms.

The sub-section “Simulated Enterprises, Organisational Transactions and Users” in section 4.3.1 exemplifies how the contributions of the ontology are made effective in the solution development. This sub-section briefly presents the modelling of a risk profile of an organisational transaction, the main related issues, and some ontological models. Furthermore, it exemplifies how the internal control mechanisms (triggers in this case) are determined based on this ontological representation.

The structure of all modules of the solution are conceptualised taking into consideration the aforementioned contributions, also including the existence of some important details to establish the relationship between modules and those with the ontology. See for example the situation depicted in Figure 30 and the related text which describes it.

Moreover, another contribution is evident in the logic layer of the Transaction Comparator module, described in section 4.2.4., because the whole algorithm comprehends the risk profiles (modelled according to the ontology, as it is already known) defined in their repository, and use them to achieve its main goals: check the status of completion of every transaction execution; audit the authorisation of the executors; audit the time in which transactions are executed; and qualitatively classify each transaction execution as negative, positive or unknown depending on the risk profiles they are following.

Thus, the Enterprise Ontology has a crucial role in achieving the objectives of the proposal, and consequently in giving conditions to implement a solution that provides continuous assurance services.

4.2 SOLUTION DEVELOPMENT

The purpose of this section is to present the aspects related to the development of the system, taking into consideration the conceptual design. Technical issues are described in a detailed way, but also at high level in order to allow an easier understanding of the system development process. More technical information will be referenced in the appendixes (available in the CD which supports this thesis).

4.2.1 Internal Control Mechanisms

Considering the set of facts presented in the survey of related works (section 1.2.1), CEP would be tendentially the choice in order to develop these control mechanisms and also for the identification in real time of the possible risk profiles for every transaction execution (R. P. Marques et al., 2013c). Such a choice would be due to the features and performance of this paradigm in the processing of large amount of events and its ability to respond in real time. However, there is a requirement of the prototype which indicates that it must work with the operational information systems of the organisations in a non-intrusive way, which puts into question, in some part, the use of CEP in the development of this component. CEP is primarily designed to work with transient data, and data processing is done in memory. The CEP employs the "inbound" approach to process the flow of events as a source of input data, enabling data to be processed as soon as they are received and then stored. In contrast, the databases take an "outbound" processing approach, requiring the storage of all data prior to processing (Oliveira, 2011; Roth et al., 2010).

The fact that the system must be non-intrusive, the functional architecture is designed so that it acts upon data resulting from the execution of transactions in operational systems. In other words, the data to be processed will be persistent. Thus, databases are an option to process persistent data, with the advantage that they do not have specified time intervals contrary to the CEP processing. Because the system acts directly in the database of the operational systems, it means that the organisational events associated with persistent data have already occurred.

Thus, the use of triggers in operational databases is a way of detection of events, since the insertion, edition or deletion of a record or a record field means the occurrence of an event of a given organisational transaction. Then, the component will render the activation of these triggers as if they were an occurrence of an event (R. P. Marques et al., 2012c; R. P. Marques et al., 2013c).

Because these mechanisms must be tailored to the needs of each organisation, i.e. for organisational transactions to be controlled, monitored and audited, this section only specifies the data that any implemented trigger must provide the system, specifically to the Real Online Transaction Repository.

Thus, the triggers which are implemented as internal control mechanisms should be automatically activated when insertion, edition or deletion occur in a relevant record and then they should be able to return data essential for this monitoring, each time they are activated, so that the monitoring of operations at the operational information system is provided (Figure 24). These data are:

- its own identification, i.e. the identifier of the trigger which has been activated and is returning the data;
- the date and time of activation of the trigger, i.e. the date and time of the detection of the transaction at the operational information system;
- the table of the information system database in which the operation has been registered;
- the identifier of the user who has performed the operation accordingly with the data in the database;
- the field values of the database which are required to univocally identify the record of the database that has been affected with the performed operation. For this, the trigger should provide the field name, its value and description for all fields which are necessary for the record identification;
- the field values of the database which are required to univocally identify the record of the preceding operation, when the operational information system recognises that succession. When this precedence exists, the trigger should

provide the field name, its value and description for all fields which are necessary for the record identification.

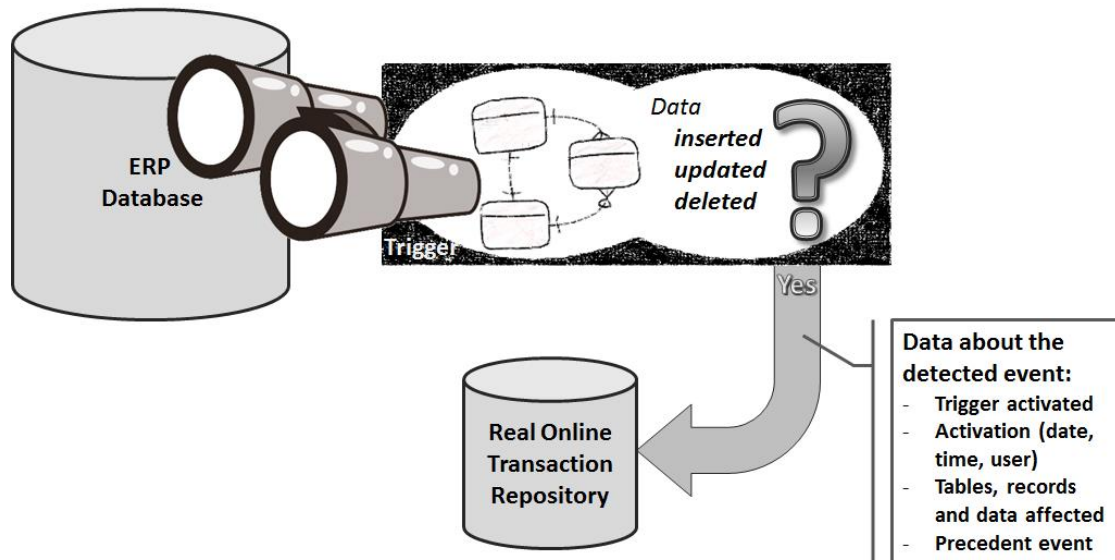


Figure 24 - High-level relationship of internal control mechanisms and the Real Online Transaction Repository

4.2.2 Real Online Transaction Repository

This module (R. P. Marques, Santos, & Santos, 2014) of the proposed architecture has the purpose to manage and maintain the data derived from internal control mechanisms and that represent the transactional operations occurring on-line in the operational information system.

The data which derive from triggers were taken into consideration for the design and development of this repository. Thus, the entities needed to represent these data in a database are the following:

- Tgr_Trigger – represents the various triggers implemented in the database of the operational information system;
- Ttp_TriggerType – represents the possible trigger types (insert, delete and update);
- Tgo_TriggerOccurrence – represents every trigger occurrence, i.e. the occurrence of an operation in the database of the operational information system. It is characterised by general data about the occurrence (besides the

identification of the respective trigger, it is also characterised by the date and time of the occurrence, the identifier of the executor user and the database table, in which the operation was executed);

- **Toi_TriggerOccurrenceInfo** – represents the data associated to each performed operation, which allow to univocally identify it. This entity is characterised by the name of the attribute which instantiate the value, and by the respective attribute value and description;
- **Tpi_TriggerParentInfo** – represents the data associated to the precedent operation (when it exists), which allow to univocally identify it. This entity is characterised by the name of the attribute which instantiate the value, and by the respective attribute value and description;
- **Usr_User** – represents the users who are executors of operations in the database of the operational information system;
- **Url_UserRole** – represents the user's roles.

To better understand how the various entities are connected, their relationship and a set of assumptions are presented in order to define the type and degree of each relationship and the setting about the mandatory participation of entities in relationships. Furthermore, Figure 25 also allows to understand these relationships through the conceptualisation of the database and its abstract description, using the ER (entity-relationship) model, which was designed based on Chen's technique (Chen, 1976).

The core entity is **Tgo_TriggerOccurrence**. Its relationship with the entity **Tgr_Trigger** is inevitable, because if we have a trigger occurrence, we must assign it to the respective trigger. Hence, all trigger occurrences are always associated with one and only one trigger. However, the same trigger may have many occurrences. In turn, the entity **Tgr_trigger** is related to the entity **Ttp_TriggerType**: every trigger is classified into only one trigger type, and different triggers may be the same type.

Furthermore, the entity **Tgo_TriggerOccurrence** is related to the entity **Toi_TriggerOccurrenceInfo**, because all trigger occurrences have data about the respective performed operation. An instance of the entity **Tgo_TriggerOccurrence** has

associated, at least, an instance of the entity `Toi_TriggerOccurrenceInfo`, but every instance of `Toi_TriggerOccurrenceInfo` is associated with only one trigger occurrence and it must be always related to a trigger occurrence.

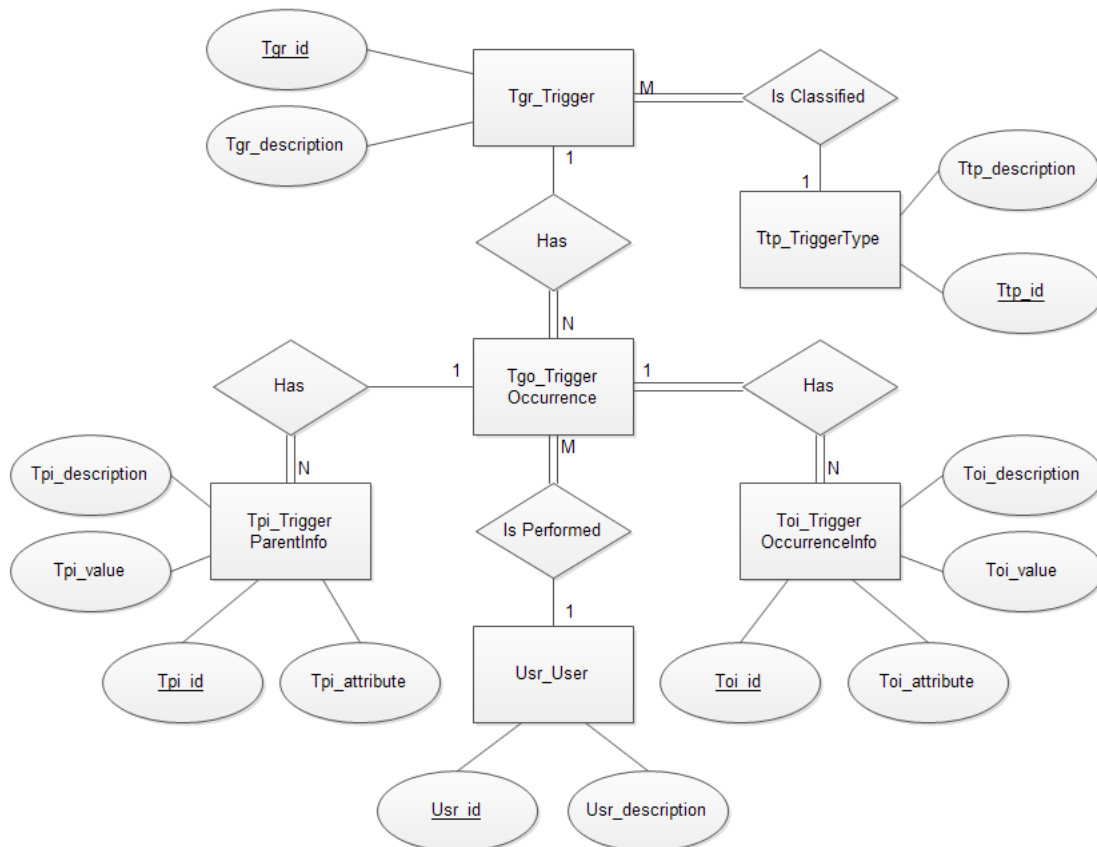


Figure 25 - Entity-relationship model of the Real Online Transaction Repository

Moreover, the entity `Tgo_TriggerOccurrence` is also related to `Tpi_TriggerParentInfo`: a trigger occurrence may have, or not, a precedent operation. Thus, an instance of `Tgo_TriggerOccurrence` may be associated with one or more instances of `Tpi_TriggerParentInfo`. However, every instance of `Tpi_TriggerParentInfo` is always associated with one, and only one, instance of `Tgo_TriggerOccurrence`.

Finally, the relationship between the entities `Tgo_TriggerOccurrence` and `Url_UserRole` is justified because it is important to know the user who has executed the operation, which has gone off the trigger occurrence. Although a user may be

associated to many trigger occurrences, it is not mandatory, however, that all trigger occurrences have one, and only one, user associated with them.

The physical model of the Real Online Transaction Repository (Figure 26) is presented in order to give a more realistic understanding about how the relationships between entities are developed in the database management system.

4.2.3 Risk Profiles Repository

This repository (R. P. Marques, H. Santos, & C. Santos, 2013b) intends to maintain and manage the known risk profiles of each organisational transaction to be monitored and audited, according to the enterprise ontology which supports this work.

From the several models of the ontology, which is studied and applied in this work, and that has been briefly presented in section 2.2, this repository intends to address the issues of the Action Model, Process Model and State Model. The Construction Model, which is the most comprehensive one, is not addressed directly in the development of this repository because the exhaustive representation of the other models makes us implicitly enclose it.

As we can perceive by the brief ontology explanation, particularly by the Process Model, an organisational transaction can have several patterns (risk profiles) depending on the actors' behaviours.

In addition, the segmentation of the risk profiles into different types, for example positive and negative, turns this database into a repository of references of patterns. Remember that negative profiles may refer to an unwanted behaviour during the execution of transactions, for example incomplete or poorly executed operations; lack of crucial procedures; non-conformities; delays; incongruities and malfeasance and positive profiles refer to all valid and appropriate events. This repository of risk profiles provides the ability to audit organisational transactions when it is used to compare operational data.

Consequently, if all risk profiles associated with an organisational transaction are represented in the database, we will start to characterise the Action Model of that organisational transaction, because we will have the execution rules of that transaction described on its risk profiles.

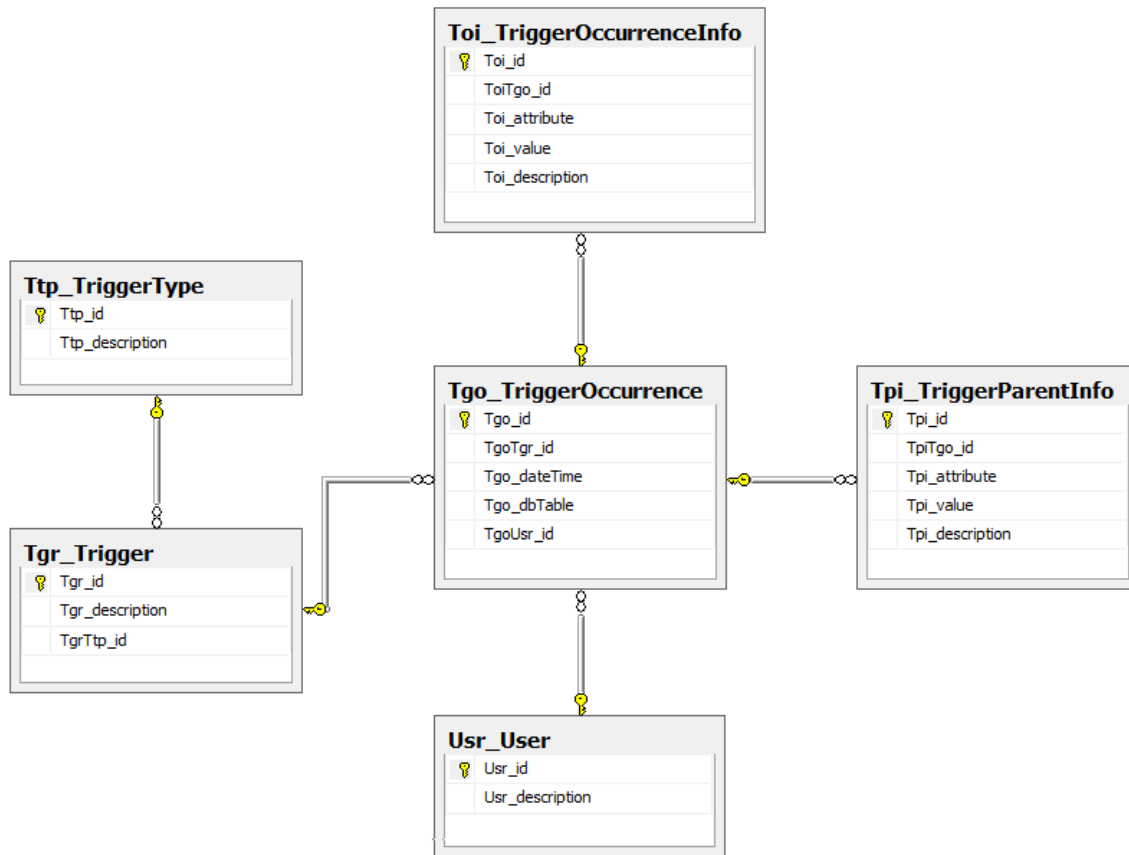


Figure 26 - Physical Model of the Real Online Transaction Repository

Furthermore, the database needs classes to represent the facts or events by type (request, promise, execution, statement, acceptance, decline, quit, reject and stop) and their relationships, which constitute the organisational transaction. Hence, we have the Process Model represented in the database.

Finally, by linking authorised users to the facts and establishing the maximum interval of time between their relationships, we complete the representation of the Action Model and consequently the State Model.

The various entities which are needed for the design of this database are stated below. The entities, and their relationships, are described in order to make their purpose and their role known in the representation of the Enterprise Ontology in this database. Thus, the entities are:

- Tst_Transaction - it represents all organisational transactions which are intended to be monitored and audited;
- Tpf_TransactionProfile – it symbolises the risk profiles, which are known for each organisational transaction;
- Ptp_ProfileType – it exemplifies the existing risk profile types in order to allow the classification of the profiles of each organisational transaction;
- Evt_TransactionEvent – it represents all the facts or events that may be considered as part of the execution of organisational transactions;
- Etp_EventType – it exemplifies the different types of events which characterise ontologically an organisational transaction (request, promise, execution, statement, acceptance, decline, quit, reject and stop);
- Url_UserRole – it represents the user's roles.

To better understand how the various entities are related, the relationships are presented grouped by how they relate directly to the two central entities of this database: Tpf_TransactionProfile and Evt_TransactionEvent. Thus, a set of assumptions are presented in order to define the type and degree of each relationship and the setting about the mandatory participation of entities in relationships. Furthermore, Figure 27 also allows to understand these relationships through the conceptualisation of the database and its abstract description, using the ER model, which was designed based on Chen's technique (Chen, 1976).

The entities which are related to the one that represents the known risk profiles for each organisational transaction are: Tst_Transaction, Ptp_ProfileType and Evt_TransactionEvent.

The relationship with the entity Tst_Transaction is inevitable, because if we have a particular risk profile defined, we will have to assign it to the respective organisational transaction. Hence, all risk profiles are always associated with one and only one transaction. However, the same transaction could be associated to one or more known risk profiles. Each risk profile must be classified as positive or negative. Thus, the entities Ptp_ProfileType and Tpf_TransactionProfile are related: all risk profiles are classified into only one type of profile, and different risk profiles may be the same

type. Finally, the two main entities of the database (Tpf_TransactionProfile and Evt_TransactionEvent) are also related. All risk profiles comprise a set of one or more events. Moreover, an event is associated with only one risk profile although it must be always related with a risk profile.

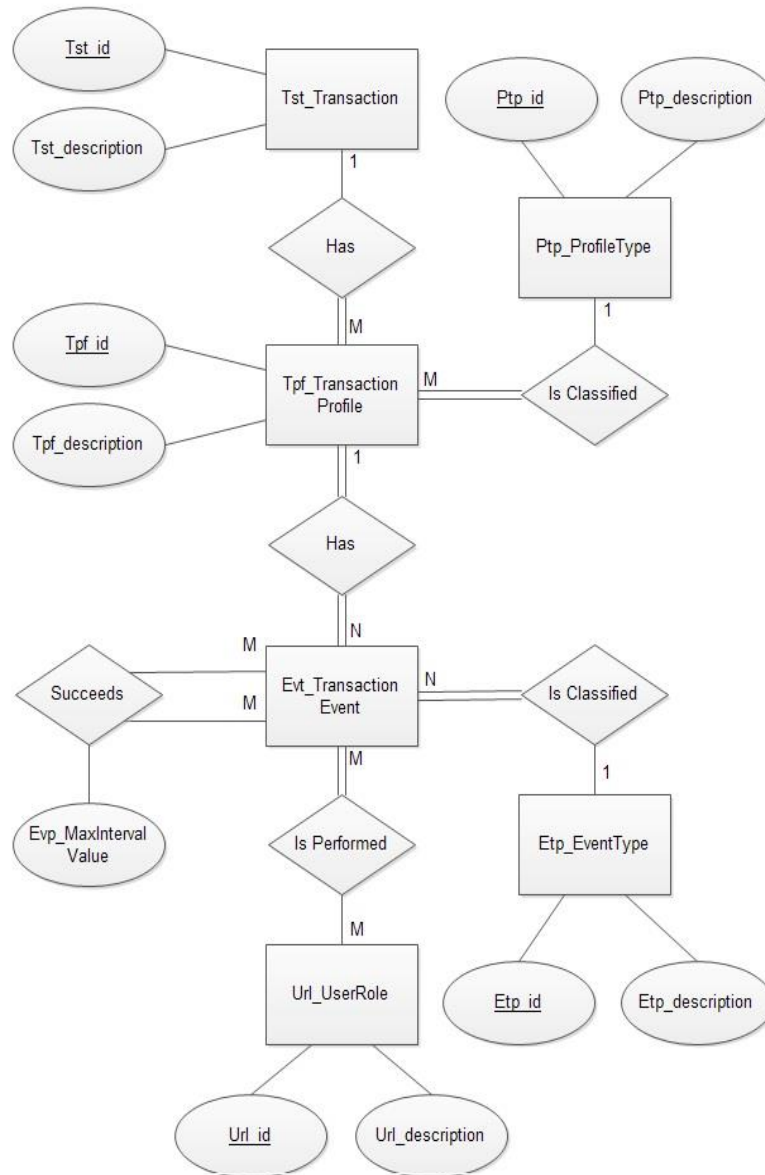


Figure 27 - Entity-relationship model of the Risk Profiles Repository

In addition to the entity Tpf_TransactionProfile, the entity Evt_TransactionEvent also relates to entities Etp_EventType, Url_UserRole and with itself. The relationship of this entity with Url_UserRole is justified because it is important to know the user

profiles that are authorised to perform/ trigger each fact or event. This is a many to many relationship since an event can be performed or triggered by a number of different user profiles, and vice versa. In addition, the authorised user profiles for each event are also necessary to know.

Furthermore, the type of event (e.g. request, promise, rejection, acceptance, etc.), in which each event is classified must also be known. This justifies the relationship with the entity Etp_EventType, because all events are classified into one of the existing types, although each type of event can be associated with several events.

Finally, the definition of the sequence of events for each organisational transaction is also needed in order to make the precedence of each known event. A risk profile of an organisational transaction will be fully defined if the sequences and precedences of facts or events, which may occur during the execution of this transaction, are completely known. Thus, the entity Evt_TransactionEvent relates with itself. An event may have, or not, one or more events that precede or succeed it. The maximum intervals of time between facts are configured in this latest relationship.

Figure 28 depicts the physical model of the Risk Profiles Repository. The physical model is given because this type of model gives a more realistic understanding about how the relationships between entities are developed in the database management system.

4.2.4 Transaction Comparator and Outputs

The Transaction Comparator module intends to be able to compare the data from the internal control mechanisms with the records maintained in the Risk Profiles Repository and then to be able to recognise the risk profiles of the execution of organisational transactions. Simultaneously, it should provide information to the users about this processing and the respective results.

The development of this module is based on a three-layer architecture, as depicted in Figure 29:

- Data access layer – This layer does not comprise data, but only the data access services, covering a business view of the access to data, and detaching the

logical layer. Therefore, only this layer has SQL (Structured Query Language) strings to access and manipulate data in the databases.

- Logic layer – This layer is responsible for implementing the business rules associated with the problem being solved. This layer is unaware of the details of data persistence, uses the services of the data access layer and returns the results to the presentation layer for dissemination.
- Presentation layer – This layer is responsible for interaction with the users of the system, having all presentation logic and mechanisms, including the provision of the results derived from the logic layer and validations, which increase the usability of these results.

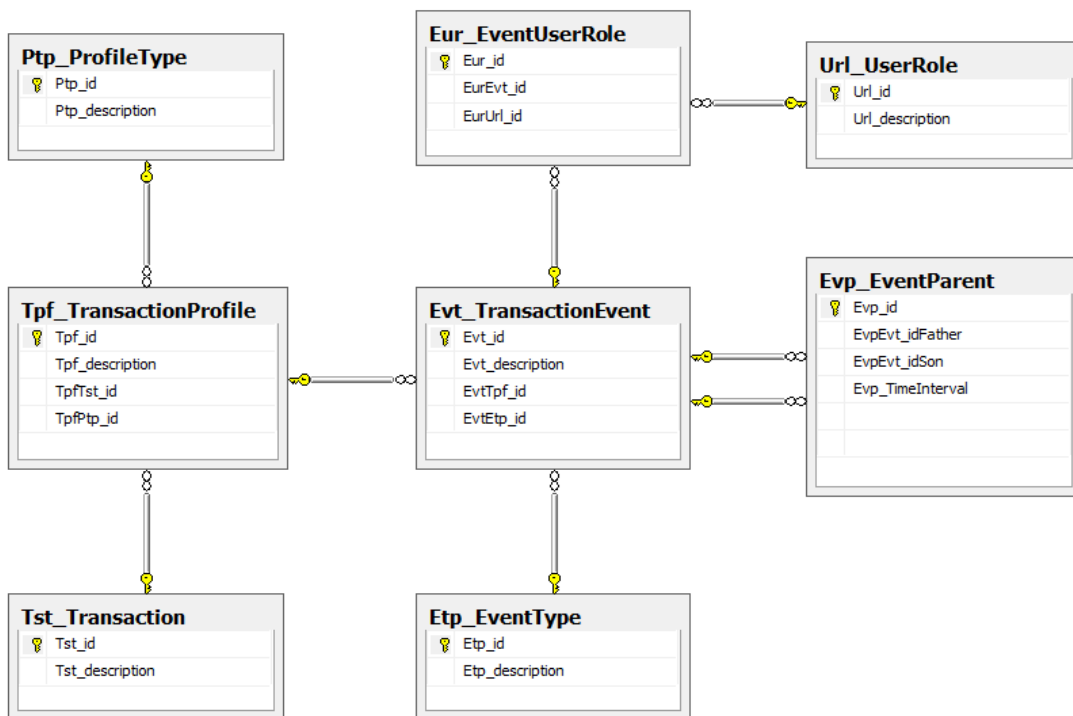


Figure 28 - Physical model of the Risk Profiles Repository

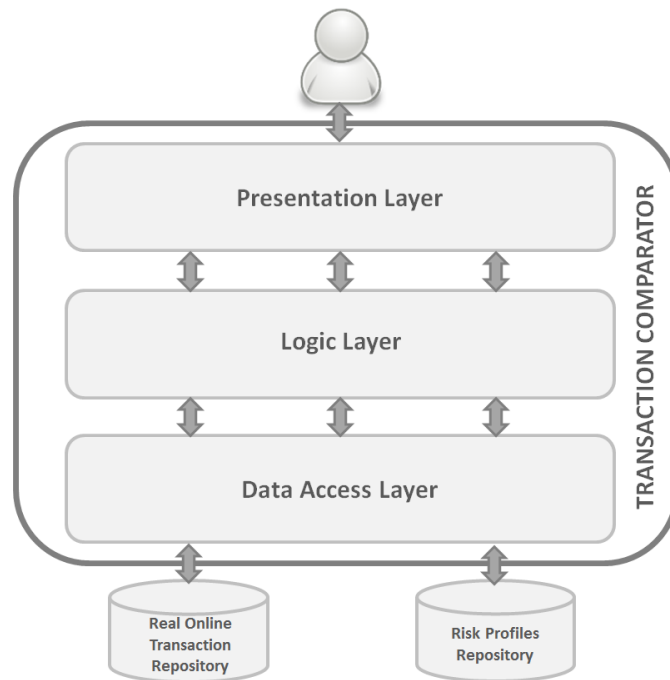


Figure 29 – Architecture of Transaction Comparator module

Before the development of this module, some adjustments in the databases of Real Online Transaction Repository and Risk Profiles Repository had to be made. Despite the fact that these modules were independently designed and developed, data of both databases are conceptually related and therefore the physical relationship of these data is also advantageous for the performance of this module. These adjustments are depicted in Figure 30:

- The relationship between the tables `Usr_User` (from database Real Online Transaction Repository) and `Url_UserRole` (from database Risk Profiles Repository). This relationship allows to assign a role to each user who is executor of operation, facilitating the auditing of organisational transactions with regard to authorisation of users as executors. This relationship is achieved by adding an attribute in table `Usr_User`, which is a copy of the primary key (foreign key) of the table `Url_UserRole` because each user always has one and only one role associated, although there may be multiple users with the same role assigned.

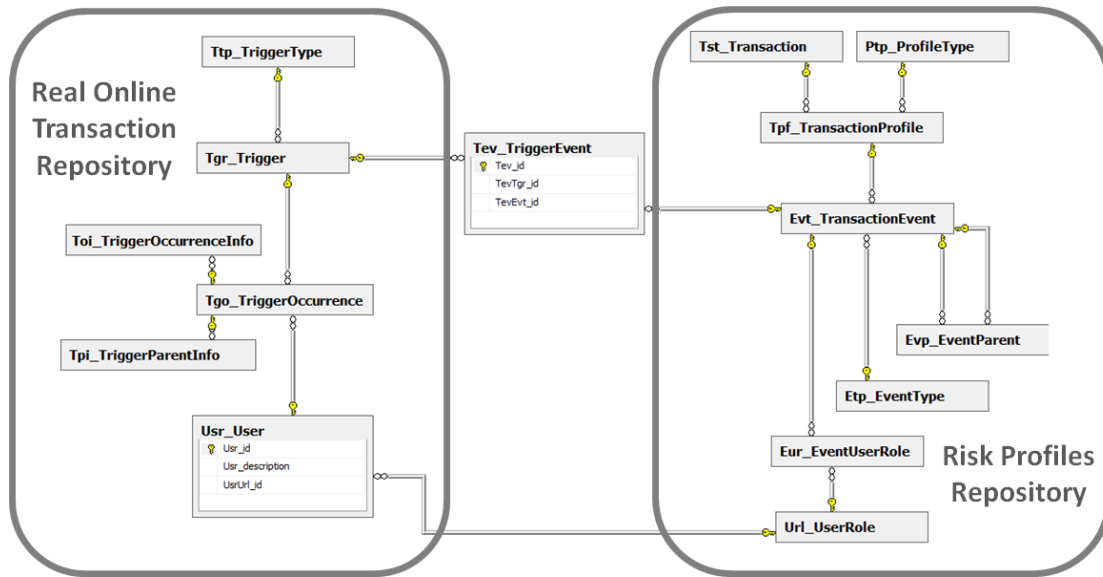


Figure 30 - Relationship between repositories

- The relationship between the tables Tgr_Trigger (from database Real Online Transaction Repository) and Evt_TransactionEvent (from database Risk Profiles Repository). This relationship is justified by the fact that there is the need to know how to associate an event (belonging to a risk profile) to a trigger. Thus, for each trigger occurrence it is possible to map it out to a certain risk profiles, enabling the identification of possible risk profiles for each transaction execution. This relationship is achieved by adding a new table Tev_TriggerEvent, which includes copies of primary keys (foreign keys) of the two tables, because we have a many-to-many relationship.

To understand in detail the design of this module and its features, the rest of this section is structured to provide high-level and detailed information of Transaction Comparator module. These details are the essential ones to understand the mechanism of the module, and are presented by layer of the architecture of this module. Technical details about the development are included in Appendix I (available in the CD which supports this thesis).

Logic Layer

The logic layer is responsible for the key features of this module, because it assesses the operations performed in the operational information system (these data are contained in Real Online Transaction Repository), comparing them with the execution patterns (risk profiles), defined in the Risk Profiles Repository.

Figure 31 illustrates, in a general way, the function of Transaction Comparator, from the perspective of the logic layer and, in its final stage, the presentation layer as well. This function is presented below in greater detail, but maintaining a high-level language. In addition, Figure 32 shows a diagram with the main classes that were considered to represent the business of Transaction Comparator. This diagram contributes to a better understanding of the processes shown in the flowchart and described immediately below.

The process Loading Risk Profiles intends to create an object that contains all risk profiles defined in the Risk Profiles Repository in order to be able to use them in the subsequent processes. This process includes the following activities:

1. create a list of all risk profiles defined in the Risk Profiles Repository. In other words, it implies the creation of a list of items in which each item is an object of the class RiskProfile;
2. associate to each item in this list:
 - a. the respective events (note that each risk profile comprises events), i.e. each of these events is an object of class RiskProfileEvent which, in turn, is associated by aggregation to the class RiskProfile;
 - b. the precedence of each event (note that the events of a risk profile follow each other in a specific order). In other words, each object of the class RiskProfileEvent has associated, by aggregation, a list of other objects belonging to the same class, representing their predecessors;

- c. the triggers which correspond to it (note that triggers conceptually represent operations), i.e. to each object of the class RiskProfileEvent is associated, by aggregation, a list of objects of the class Trigger;
- d. the list of identifiers of the user roles authorised to be executors of this event.

After obtaining the list of risk profiles, the Transaction Comparator module will continuously interact, via data access layer, with the database of Real Online Transaction Repository to determine whether operations were performed and detected by triggers in the operational information system (and recorded in Real Online Transaction repository) since the last interaction with this repository.

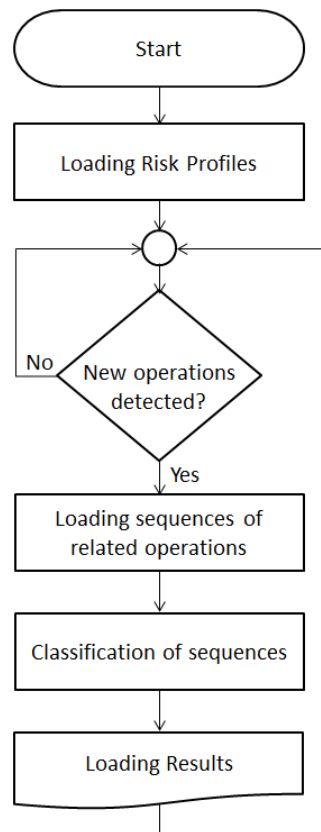


Figure 31 - Flowchart of Transaction Comparator

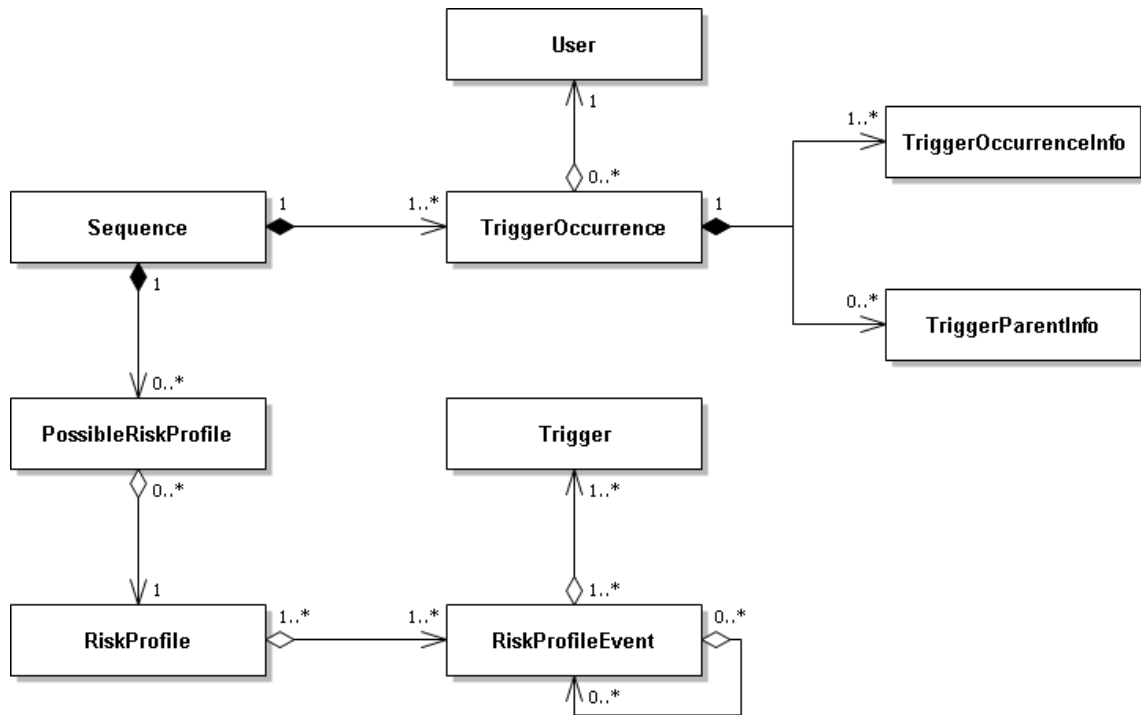


Figure 32 - Diagram of classes of the logic layer of Transaction Comparator module

When a new operation is performed and detected in the operational information system, the flowchart indicates that a process called "Loading sequences of related operations" runs. This process aims to aggregate operations which are related due to the fact they belong to the same organisational transaction execution (Figure 33). Thus, a chronological sequence of execution of operations is possible to be established in order to allow the comparison with the sequence of events defined in the risk profiles of reference. This process includes the following activities:

1. create a list of trigger occurrences, upwardly sorted by date and time of occurrence, which corresponds to the performed operations since the last interaction with Real Online Transaction Repository. Hence, the class TriggerOccurrence exists because its objects make up this list;
2. For each item in this list:
 - a. collect data which are associated to each performed operation and allow to univocally identify it, i.e. each object of the class

TriggerOccurrence is associated, by composition, to the class TriggerOccurrenceInfo;

- b. collect data which are associated to the precedent operation (when it exists) and allow to univocally identify it, i.e. each object of the class TriggerOccurrence is associated, by composition, to the class TriggerParentInfo;
- c. verify if the item is related to any existing sequence in the list of sequences. This verification is performed by searching the data of the object TriggerParentInfo of this item in the data of the object of TriggerOccurrenceInfo of every operation of the sequences in the list. If the process finds a sequence in the list with related operations, this item is added to this sequence. Otherwise, it creates a new sequence in the list with this item.

After this process another one, designated as Classification of Sequences, runs. This is the most complex process because it is responsible for identifying possible risk profiles for each sequence of operations (transactions) in the list of sequences. Besides checking the compliance in the chronological order of execution of operations, auditing the authorisation of the executors, auditing the time in which the operations are performed, it is also responsible for the correct classification of the possible risk profiles as negative, positive or unknown, allowing to qualitatively estimate the risks associated to the transactions execution.

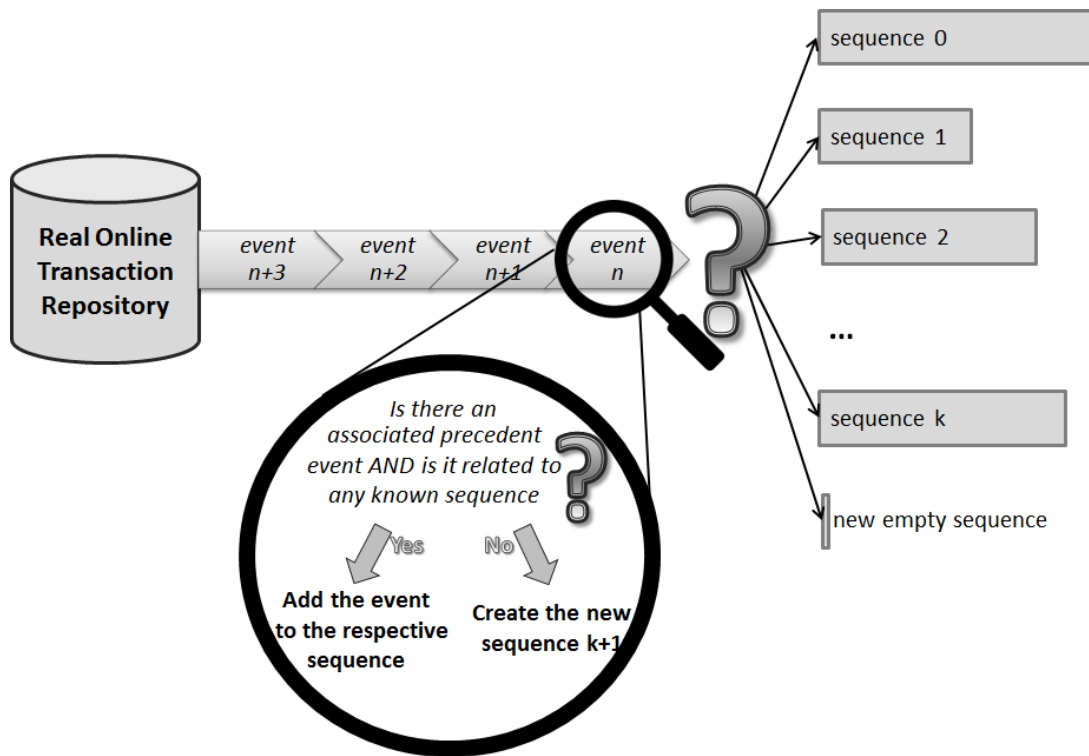


Figure 33 - High-level description on loading sequences of related operations (transactions)

These evaluation activities are carried out comparing the executed transactions (sequences of related operations mentioned immediately above) with the patterns of transactions executions (risk profiles) defined in the Risk Profiles Repository (Figure 34). This process comprises the following activities:

1. For each sequence (transaction) in the list of sequences:
 - a. creates and associates to it an empty list of possible risk profiles. Hence, it justifies the association, by composition, of the class PossibleRiskProfile with the class Sequence and with the class RiskProfile by aggregation. An object of the class PossibleRiskProfile contains information about the risk profile that has been associated to a given transaction execution, and the results of the auditing to this sequence based on the data of this risk profile (e.g. transaction completeness). Note that determining that a risk profile is a possible risk profile of a transaction execution consists

in finding concordance between the performed operations and those of the risk profiles defined in the Risk Profiles Repository;

b. analyse each of its operations:

i. If the operation is the first one in sequence, the process looks in the risk profiles for those which also begin with this operation. If they are not found, the list of possible risk profiles of this sequence continues null, but if the process finds at least one risk profile, it adds this risk profile to the list of possible risk profiles of this sequence. Then, for all objects in the list of possible risk profiles of the sequence:

- check the status of the transaction execution (complete or incomplete) based on this possible risk profile;

- audit the authorisation of the executors;

ii. if the operation is not the first in the sequence, the process looks at the list for possible risk profiles associated to this sequence, those which have this operation in their event list. The possible risk profiles which do not have this operation, are removed from the list of possible risk profiles of this sequence.

The possible risk profiles are audited regarding the precedence of this operation, i.e. it checks if the operations in the list follow the chronological order of succession provided by the risk profile. If the precedents are not validated, this possible risk profile is removed from the list of possible risk profiles of this sequence. However, if the precedents are validated, the process proceeds to the remaining audits for each possible risk profile:

- check the status of execution of the transaction (complete or incomplete) based on this possible risk profile;

- audit the authorisation of the executors;
- audit the time in which operations were executed (in time or delay), based on the time intervals between operations and which were defined in the respective risk profile.

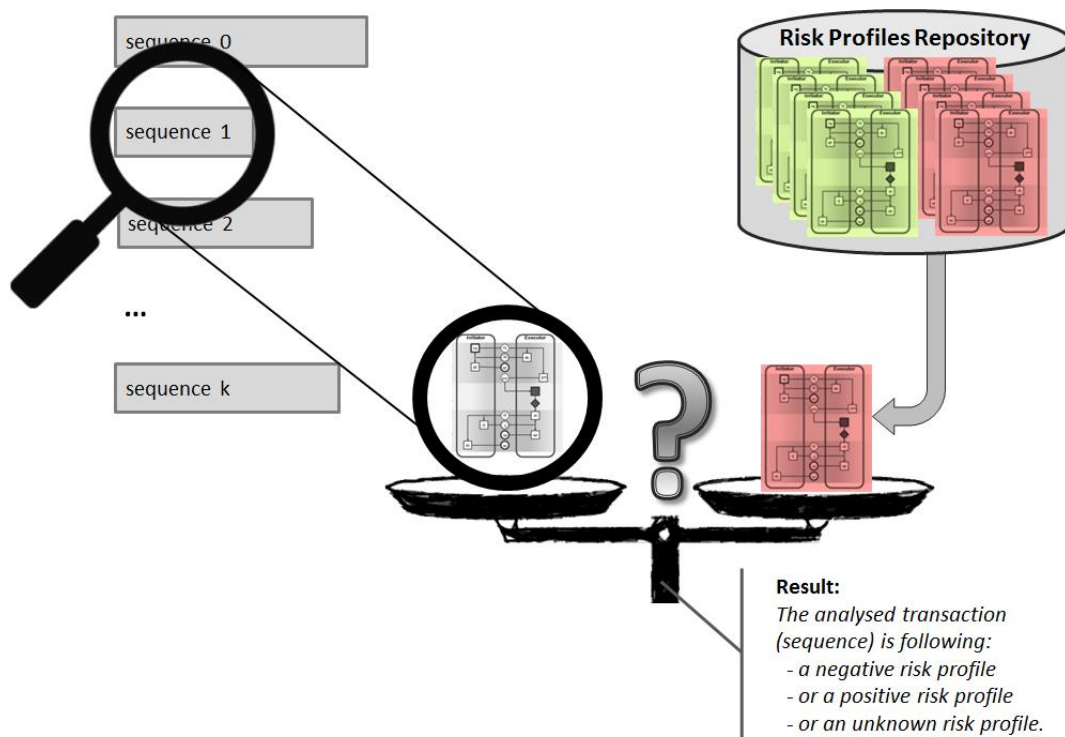


Figure 34 - High-level description of the operation of the Transaction Comparator evaluating the executed transactions

Presentation Layer

All functionalities of presentation and dissemination of the results of the logic layer belong to this layer, i.e. refer to the process Loading Results of the flowchart depicted in Figure 31.

The prototype of this solution includes three different media of disseminating results:

- interfaces so that the results of monitoring and auditing of organisational transactions can be visualised at run-time by users on a computer;

- reports in spreadsheet format to allow the users to visualise the results as well as manipulate them for other purposes, e.g. statistical objectives or to support the decision making;
- e-mail to alert users of high-risk situations, including organisational transactions which are following negative or unknown risk profiles.

Regarding the interface, more importance is given to the information which must be available to meet the requirements of the system instead of usability issues. Then, as it can be seen in Figure 35, the system should have one main window divided into two major areas:

- Area A corresponds to the presentation of the list of all organisational transactions already completed or still in progress. In this area, it is intended to have only basic information about each transaction (identifier, description, date and time of first operation and date and time of the last operation performed);
- Area B is activated as soon as a transaction (area A) is selected, and it indicates the possible risk profile which is followed by the transaction execution. This area intends to provide: the identifier of each possible risk profile; their description and type; and the results of auditing regarding completeness, executors and execution time of the respective organisational transaction compared with the risk profile settings;
- Area C is a popup window which opens with double-click in a transaction of area A. This window presents some details of the performed operations of the transaction. This area brings together all data associated with the occurrence of the operations performed in an organisational transaction, i.e. it presents all data associated with the clicked transaction, of the tables Tgo_TriggerOccurrence and Toi_TriggerOccurrenceInfo.

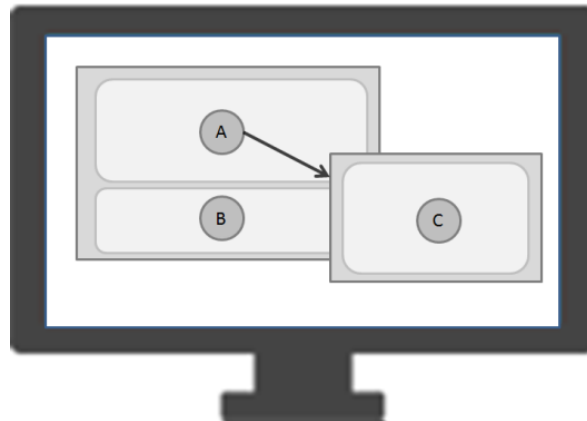


Figure 35 - Conceptualisation of the interface of the system

In the report, the most important information must be available in a spreadsheet format. Appendix III (available in the CD which supports this thesis) presents one of those reports as an example for better understanding. Thus, this report consists of a workbook composed of three worksheets:

- “Transactions” – this worksheet presents general data about executed transactions, particularly:
 - the column “#” shows the ID of the executed transactions. This ID is a sequential number and has the sole purpose of univocally identifying each execution;
 - the column “Transaction” presents the names of the executed transactions. These names are included in the Risk Profiles Repository and are associated with the risk profiles identified by the algorithms of monitoring, controlling and auditing;
 - the column “First Event” shows the date and time of the first occurred event, which was associated to each transaction execution;
 - the column “Last Event” shows the date and time of the latest occurred event associated with each transaction execution.

- “Transaction Details” – this worksheet presents data about the occurred events of each transaction execution, including:
 - the column "Trans ID" identifies the transaction execution each line refers to, i.e. the identifier of the transaction execution presented in the column "#" of the worksheet "Transactions";
 - the column "Occurrence ID" presents the identifier created by the component "Real Online Transaction Repository" for the executed and monitored operations. This ID is a sequential number and has the sole purpose of univocally identifying each monitored transaction;
 - the column “Description” shows the name of the monitored operations. This name is given by the trigger which detected the operation, and is composed of the type of operation (insert, update or delete) followed by the specification of the monitored operation;
 - the column “Date Time” presents the date and time of occurrence of the operation;
 - the column “User ID” presents the identifier of the user who executed the operation.
- “Possible Risk Profiles” – this worksheet presents data about the risk profiles which are being followed by each transaction execution, particularly:
 - the column "Trans ID" identifies the transaction execution each line refers to, i.e. the identifier of the transaction execution presented in the column "#" of the worksheet "Transactions";
 - the column "Risk Profile ID" shows the identifier of the risk profile, which is being followed by the respective transaction execution. This identifier is defined in the Risk Profiles Repository. It is a sequential number, and was created with the objective of univocally identifying the existing risk profiles in the repository;
 - the column "Risk Profile" presents the description that was given to the risk profile in the Risk Profiles Repository;
 - the column "Status" indicates the status of the transaction executions (complete or incomplete) compared with the respective risk profile;

- the column "Type" identifies the risk profile type (positive or negative);
- the column "Users" specifies whether the operations associated with the transaction executions were executed by users with role authorised by the respective risk profile. Just one operation performed by an user with unauthorised role is sufficient to change the state into "unauthorised";
- the column "Time" indicates the value "In time" or "Delay" depending on the interval time between the occurrence of operations associated with the transaction execution. Just one operation occurred after the expected time by the risk profile is sufficient to change the state into "Delay".

With regard to e-mail alerts, the users of the system must receive an e-mail per transaction, whose execution has been estimated by the system as potentially negative. In other words, if all possible risk profiles associated with a transaction execution are negative, an e-mail alert should be sent informing the users about this negative situation. Furthermore, e-mail content should have included the date and time of the last operation which brought about the situation. Moreover, if no possible risk profile was identified, users must also be alerted about the situation.

Appendixes I and II (available in the CD which supports this thesis) include the source code of the application and the script of creation of databases.

4.3 IMPLEMENTATION

This section aims to present the implementation of the proposed solution fully developed and prototyped in an organisational environment, so that results can be collected in order to ascertain compliance with the requirements of the system and subsequently contribute to the validation of the research questions and hypotheses.

Thus, this section presents the object of study, the elements involved in the implementation and the methods used during the case study.

4.3.1 Object of Study

This section aims to give a short presentation of the resources which are intended to be used for the deployment of the prototype.

To validate the prototype it will be necessary its implementation in an organisational environment, and to this end, we intend to use the course "Enterprise Simulation" of the degree in Accounting from the Higher Institute of Accounting and Administration of the University of Aveiro, because it yields a controlled environment, and also allows the application of the prototype in different organisational areas.

As described above, it is intended that the prototype will incorporate internal control mechanisms in the ERP system of organisations. For this reason, we will have to use the ERP system used by companies created in the course "Enterprise Simulation": ERP Primavera Professional 8.

In addition, organisational transactions that were used for controlling, monitoring and auditing during the implementation of the prototype are also presented and described.

Curriculum Unit “Enterprise Simulation”

The University of Aveiro has the curriculum unit "Enterprise Simulation" included in the last year of the degree in Accounting, which aims to simulate the organisational activities. The students have to create their own enterprise, develop its operations in the business during an operational period in accordance with the economic calendar

and prepare and disseminate financial statements. With this, students are able to: consolidate and integrate the knowledge which they have acquired in other courses, especially those that are most closely related to the exercise of professions for which the course enables, have a practical view of these professions integrated in the normal curricular plan of the graduation, covering the basic needs that ensure an easier approach to the working life and a better understanding of professional issues, ethics and experience in business, developed in a simulation environment of organisational reality, but sufficiently deep and striking to provide a future ethical posture (F. Silva, 2009).

Every year there are dozens of groups of students who attend this course, creating their own businesses in various organisational areas, like services, commerce, industry and public services. The university provides a well-structured simulation environment that is very close to reality. To this end, in addition to organisations run by students, a business central, a financial central and a public central of services are created (F. Silva, 2009).

The business central aims: to supply all the deficiencies that the simulated enterprise market is not able to absorb in the first instance; take over the participating enterprises in the universe market of business simulation when these seem absolutely unable to meet the needs of the development of the activity of other companies; establish itself as a competitive partner of the market of enterprise simulation, being a regulator and stimulator of its competitive nature; apply fines or other penalties when companies deliberately do not comply with the guidelines of the central or lack to fulfil their obligations in abusive way (F. Silva, 2009).

The financial central's mission is to ensure and distribute a range of financial products and services to the companies incorporated in the Enterprise Simulation, providing them with a broad range of financial transactions for financial registration, accounting and evaluation. Besides the possibility of the company to deposit its funds in a demand deposit account, the Financial Central also offers a set of products aimed at providing: solutions to finance / investment (financing products: loans, escrow account, leasing, renting, bill discount, products for the application of excess cash,

deposits, equity fund, bond fund, hedging products that address the following insurance: accident, multi-hazard, car, life, health and other services) (F. Silva, 2009).

The public central of services aims to contribute to the proper functioning of the universe of Enterprise Simulation, providing the services of various public and private organisations necessary to their legal obligations and other requirements of their respective enterprises. This centre aims to provide services related to the following organisations: Institute of Registration and Notary, Directorate General of Taxation, Bureau of Collection of VAT (Value Added Tax) Directorate General of Social Security, Directorate-General for Enterprise, the Regional Directorate of the Ministry of Economics; Authority for Labour, Chartered Accountant, private notary and others (to be provided by professional and specialised entities as may be necessary) (F. Silva, 2009).

Primavera – Professional ERP

Based on the experience acquired over the years in contact with more than 40,000 business customers of many different industries, and different dimensions in various markets, coupled with the steady bet on innovative information technologies, Primavera provides a wide range of solutions of organisational management (Primavera, 2013), including ERP Primavera Professional, which was used in the implementation of the prototype of this work.

This ERP system of business management combines the latest technological innovations to features that promote maximum productivity of organisations. Based on a cross platform, ERP Primavera includes a set of fully integrated modules that cover the major functional areas of business (e.g. financial, logistics, treasury, commercial, human resources, among others). Thanks to its high capacity for parameterisation and configuration, this ERP system provides management solutions which address the specific needs of each organisation (Primavera, 2013).

Simulated Enterprises, Organisational Transactions and Users

The organisational transactions which are most executed in the curricular unit “Enterprise Simulation” are the commercial and the accounting ones (F. Silva, 2009).

However, those with the most occurrences are related to sales and the respective accounting entries (F. Silva, 2009), and therefore, this implementation gives more emphasis to these transactions, because they are the ones which mostly contribute with data to the analysis results. Thus, commercial transactions related to a sale, were always considered in this implementation, because it is an organisational transaction which may have several risk profiles, because there are many factors that influence the number and type of operations to perform, as we shall see below.

Because this implementation occurs in a simulated environment, and a calendar year is simulated and run in just over three months, many of the national rules and directives which govern the commercial domain cannot be met in this implementation. Thus, this means that the considered risk profiles are not substantiate because the policies that govern "Enterprise Simulation" are more flexible than the directives that govern real organisations.

Hence, the risk profiles, including the rules and values that we attribute to them, do not match the rules that we used to see in the usual routine of real companies.

Risk profiles created for the commercial transaction may include combinations of various operations, including the operations of insertion, update and deletion of: budget, order; consignment note, invoice, receipt, credit note, debit note, and accounting entry. In case of operations on documents, the operations of update or deletion on the document header were differentiated from these operations on the document lines.

A representation of one of the many possible risk profiles of a commercial transaction is presented below accordingly with the ontological model adopted in this work. This possible risk profile comprises a budget, an order, an invoice and an accounting entry.

To understand this risk profile of commercial transaction, two actors are considered: the customer and the supplier. The latter can be split into elemental actors, for example, the staff that directly interact with the customer, the ERP system or other.

For this risk profile, several other basic transactions which compose it are considered: T01 - budget; T02 - order; T04 - invoice; T05 - accounting entry.

Furthermore, the transaction T02 originates another transaction: the issuance of the order proof (T03).

The interaction between customer and supplier is always performed by the elementary actor staff. Their interaction can be represented by the following interaction model (Figure 26).

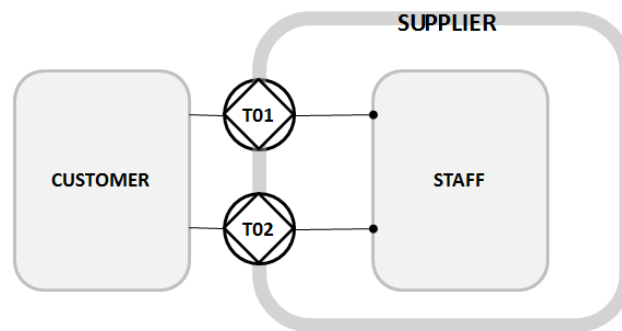


Figure 36 - Interaction Model of a possible risk profile of a commercial transaction

Note that transactions T03, T04 and T05 are not in the interaction model, because they are automatically triggered by T02, i.e. T02 will only be completed when all the others are also completed. In this interaction, the actors of the supplier appear as executor of T01 and T02.

Before presenting the process model of the risk profile of the commercial transaction, it is important to take into account the various symbols that are used in the model:

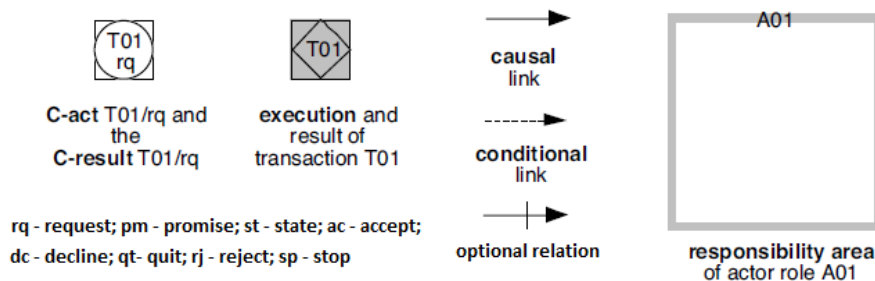


Figure 37 - Legend for interpreting the process model

For the risk profile in representation, the following context may be considered:

The customer requests an order to the staff of the supplier, providing the needed data for their execution. The staff of the company satisfies the request, executing the budget in the ERP system and returning it to the customer. The customer, in turn, accepts the budget and initiates the request of an order based on the accepted budget. The staff of the company, receiving the order, starts the issuance of an order proof which is executed in the ERP system and returned to the customer. The delivery of this document to the client initiates the execution of the order. When the order is executed and is ready to be made available to the customer, the process of issuance of invoice is started by the staff. The invoice is executed in the ERP system and returned to the client, allowing that the order is finally delivered to the customer and completed. Moreover, after the issuance of the invoice an accounting entry, related with the invoice, is started by the staff, which is also recorded in the ERP system and validated by the staff of the company.

Figure 38 depicts this risk profile (Figure 37 helps its analysis). Based on this representation, we are able to understand the situation from the ontological point of view:

The customer requests an order to the staff of the supplier, providing the needed data for their execution (T01 rq). The staff of the company satisfies the request (T01 pm) executing the budget in the ERP system (T01) and returning it to the customer (T01 st). The customer, in turn, accepts the budget (T01 ac) and initiates the request of an order based on the accepted budget (T02 rq). The staff of the company receiving the order (T02 pm) starts the issuance of an order proof (T03 rq and implicitly T03 pm), which is executed in the ERP system (T03) and returned to the customer (T03 st). The delivery of this document to the client (T03 ac) initiates the execution of the order (T02). When the order is executed and is ready to be made available to the customer (T02 st), the process of issuance of invoice is started by the staff (T04 rq and implicitly T04 pm). The invoice is executed in the ERP system (T04) and returned to the client (T04 st), allowing (T04 ac) the order to be finally delivered (T02 st) to the customer and completed (T02 ac). Moreover, after the issuance of the invoice (T04 st),

an accounting entry related with the invoice is started by the staff (T05 rq and implicitly T05 pm), and is also recorded in the ERP system (T05) and validated by the staff of the company (T05 st and implicitly T05 ac).

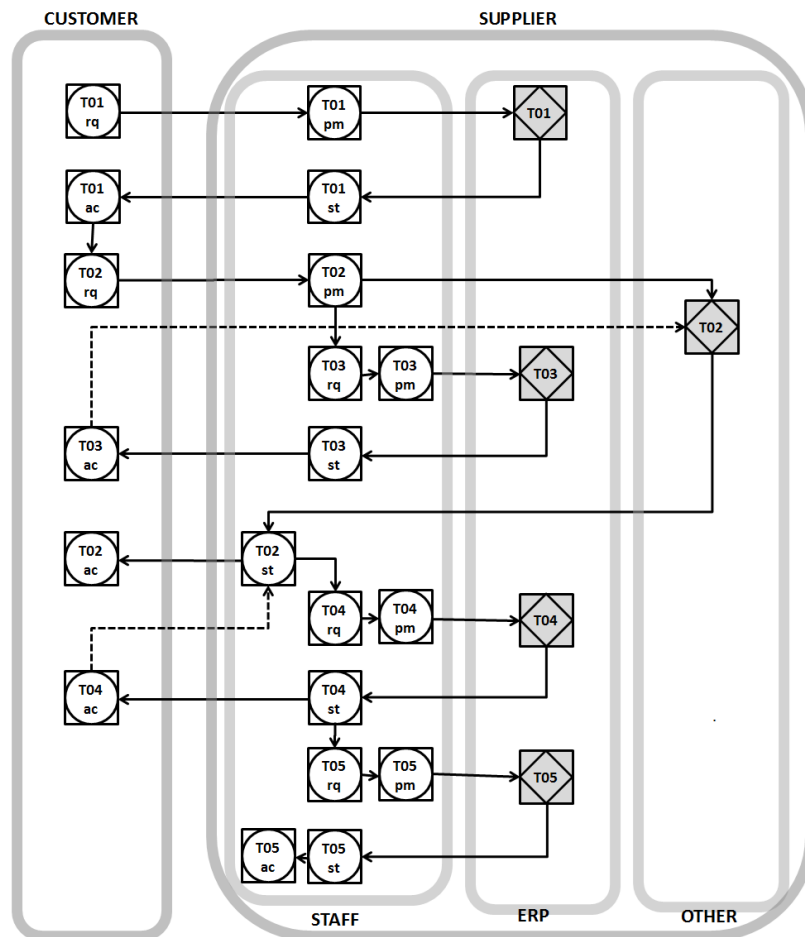


Figure 38 - Process model of a possible risk profile of a commercial transaction

Some rules in the execution of the commercial transaction (action model) may also be defined, for example, periods of validity for some documents. For instance, the order promise (T02 pm) based on a budget should only occur if the expiration date of the budget is not over.

```

on requested T02
  if budget_date (T01) + budget_period_validity (T01) >= Now → promise T02
no
    
```

Still regarding the rules, some conditions of succession may also be defined. For example, the order will only be executed after the receipt and validation of the order document by the customer.

on accepted T03
 execute T02
no

After the modelling of the various risk profiles of transactions, it is necessary to determine which of the possible events are monitored through the detection of insertion, modification or deletion of records in the ERP database. On the risk profile modelled above, only four events are possible to monitor in the database of the ERP system: executions of transactions T01, T03, T04 and T05, i.e. the issue of the budget, order and invoice documents related to the considered commercial transactions, and also the accounting entry associated with the issued invoice.

It is also necessary to determine the tables of the database which allow the detections of those events. And only then are we able to develop triggers on those tables that give monitoring data to Real Online Transaction Repository.

These triggers can be of three different types: insert (to detect insertion of records in tables); update (to detect modification of records in tables), and delete (to detect deletion of records in tables). Therefore the choice of a trigger type depends solely on the type of operation which is intended to be monitored. But regardless of the trigger type, all of them have to return the same type of information to the Real Online Transaction Repository:

- its own identification;
- the identification of the user responsible for the operation;
- the date and time of detection of the operation;
- the table on which the trigger is implemented;
- the set of attributes and their respective values and description, which univocally identify the performed operation;

- the set of attributes and their respective values and description, which univocally identify the precedent operation of the detected one.

Appendix II (available in the CD which supports this thesis) presents the triggers. In this appendix it is possible to see how they were performed in this implementation.

In addition to the risk profile presented above, which serves as an example, only more 19 risk profiles were defined in the Risk Profiles Repository, making a total of 20 risk profiles (10 positive and 10 negative). The following table (Table 11) presents, in a very simple way, the operations which are included in the risk profiles defined in the Risk Profiles Repository.

Table 11 - Risk profiles defined in the Risk Profiles Repository

| Positive Risk Profiles | | Negative Risk Profiles | |
|------------------------|---|------------------------|---|
| 1 | Invoice; Accounting Entry | 11 | Invoice; Receipt; Accounting Entry; Update of Invoice Header |
| 2 | Budget; Order; Consignment Note; Invoice; Accounting Entry | 12 | Order; Invoice; Receipt; Accounting Entry; Update of Invoice Header |
| 3 | Budget; Order; Invoice; Accounting Entry | 13 | Invoice; Update of Invoice Header |
| 4 | Order; Invoice; Accounting Entry | 14 | Invoice; Receipt; Accounting Entry; Deletion of Invoice |
| 5 | Order; Consignment Note; Invoice; Accounting Entry | 15 | Order; Invoice; Receipt; Accounting Entry; Deletion of Invoice |
| 6 | Invoice; Receipt; Accounting Entry | 16 | Invoice; Deletion of Invoice Header |
| 7 | Budget; Order; Consignment Note; Invoice; Receipt; Accounting Entry | 17 | Invoice; Update of Invoice Lines |
| 8 | Budget; Order; Invoice; Receipt; Accounting Entry | 18 | Invoice; Receipt; Accounting Entry; Update of Invoice Lines |
| 9 | Order; Invoice; Receipt; Accounting Entry | 19 | Order; Invoice; Receipt; Accounting Entry; Update of Invoice Lines |
| 10 | Order; Consignment Note; Invoice; Receipt; Accounting Entry | 20 | Invoice; Update of Invoice Lines |

As regards the maximum time intervals between operations, because of the aforementioned reasons, a set at random intervals were defined. However, it also allows to determine the effectiveness of the auditing of the time in which transactions are executed.

The prototype was made available to three enterprises of the "Enterprise Simulation": one was a provider of catering services, another was a construction company and the other one was a fuel supplier. These companies were managed by a small group of people (students responsible for each company), all of them were assigned the role of administrator to access the ERP system. In order to make it possible to evaluate the effectiveness of the capacity of the prototype to audit the authorisation of users to execute operations we created a user with unknown role, in addition to the users created for each participant of the prototype with their respective role, which was known by the prototype.

Appendix II (available in the CD which supports this thesis) presents a database script which allows to know the data that were included in the databases of Real Online Transaction Repository and Risk Profiles Repository. Additionally, the scripts of all triggers implemented in the ERP database are also available in this Appendix.

4.3.2 Methods

The implementation began on 17 April 2013 and ended on the 5 July of the same year, nearly three months of prototype testing. Some methods were defined to conduct this implementation, in order to collect data and verify the compliance with the initial requirements.

We have already seen that the system produces reports with the results of the controlling, monitoring and auditing of organisational transactions. The analysis of these reports was performed using another file, in which the researcher registered the essential indicators to subsequently have data for a more general analysis. Therefore, the analysis of these reports is still partial, which enables us to obtain a more conclusive analysis from the point of view of research hypotheses validation.

Only data related to transaction executions initiated from the latest report as well as the transaction executions which have suffered some type of change since the latest report (e.g. occurrence of new operations or simply the change of state from "in time" into "delay") were considered in each report. The font colour of the data related to transaction executions which are not to be considered for analysis is grey in the three worksheets of the report and the font colour of the data related to transaction executions which are to be considered for analysis is black or red. The data in black font colour mean that the execution followed or is following at least one known positive risk profile, and the data in red font colour mean that the execution followed or is following a negative risk profile or an unknown risk profile which is not defined in the Risk Profiles Repository. Only the data with black or red font colour in the three worksheets are subjected to examination by the researcher.

As aforementioned, the support file results from the reports analysis. It can be consulted in Appendix IV (available in the CD which supports this thesis) and aims to present some indicators for further treatment. These indicators are presented in Table 12.

Table 12 - Indicators considered in the analysis of the reports of the prototype

| | Indicator Description |
|---|---|
| 1 | Total of possible risk profiles, which are being followed |
| 2 | Number of possible positive risk profiles which are being followed out of a total of possible risk profiles |
| 3 | Number of possible negative risk profiles which are being followed out of a total of possible risk profiles |
| 4 | Total of risk profiles which were correctly identified out of a total of possible risk profiles |
| 5 | Number of positive risk profiles out of a total of possible risk profiles which were correctly identified |
| 6 | Number of negative risk profiles out of a total of possible risk profiles which were correctly identified |
| 7 | Total of risk profiles which were incorrectly identified out of a total of possible risk profiles |

Solution Proposal

| | Indicator Description |
|----|--|
| 8 | Number of positive risk profiles out of a total of possible risk profiles which were incorrectly identified |
| 9 | Number of negative risk profiles out of a total of possible risk profiles which were incorrectly identified |
| 10 | Total of possible risk profiles which were not identified out of a total of possible risk profiles |
| 11 | Number of positive risk profiles out of a total of possible risk profiles which were not identified |
| 12 | Number of negative risk profiles out of a total of possible risk profiles which were not identified |
| 13 | Number of possible risk profiles which were correctly classified on their type as negative, out of a total of possible negative risk profiles which were correctly identified |
| 14 | Number of possible risk profiles which were incorrectly classified on their type as negative, out of a total of possible negative risk profiles which were correctly identified |
| 15 | Number of possible risk profiles which were correctly classified on their type as positive, out of a total of possible positive risk profiles which were correctly identified |
| 16 | Number of possible risk profiles which were incorrectly classified on their type as positive, out of a total of possible positive risk profiles which were correctly identified |
| 17 | Number of possible risk profiles which were correctly classified on their state of execution as complete, out of a total of possible risk profiles which were correctly identified |
| 18 | Number of possible risk profiles which were incorrectly classified on their state of execution as complete, out of a total of possible risk profiles which were correctly identified |
| 19 | Number of possible risk profiles, which were correctly classified on their state of execution as incomplete, out of a total of possible risk profiles which were correctly identified |
| 20 | Number of possible risk profiles which were incorrectly classified on their state of execution as incomplete, out of a total of possible risk profiles which were correctly identified |
| 21 | Number of possible risk profiles which were correctly audited regarding the users who were executors, when they were authorised users |

| | Indicator Description |
|----|---|
| 22 | Number of possible risk profiles which were incorrectly audited regarding the users who were executors, when they were authorised users |
| 23 | Number of possible risk profiles which were correctly audited regarding the users who were executors, when they were unauthorised users |
| 24 | Number of possible risk profiles which were incorrectly audited regarding the users who were executors, when they were unauthorised users |
| 25 | Number of possible risk profiles which were correctly audited regarding the time at which each transaction was executed, when they were executed in time |
| 26 | Number of possible risk profiles which were incorrectly audited regarding the time at which each transaction was executed, when they were executed in time |
| 27 | Number of possible risk profiles which were correctly audited regarding the time at which each transaction was executed, when they were executed with delay |
| 28 | Number of possible risk profiles which were incorrectly audited regarding the time at which each transaction was executed, when they were executed with delay |
| 29 | State of alert? (0 - there is no state of alert, or the alert already went off in past occurrences; 1 - if the transaction is following an unknown risk profile; 2 - if all possible risk profiles (1 or n) are negative) |
| 30 | Identification of the state of alert (Yes or No) |
| 31 | Date and time of the occurrence responsible for the state of alert (stored in the ERP database) - only applicable if there is state of alert |
| 32 | Date and time of the occurrence responsible for the state of alert (stored in the prototype database) - only applicable if there is state of alert |
| 33 | Date and time of the alert (data retrieved from e-mail header) - only applicable if there is state of alert |
| 34 | Time interval between the occurrence of the event and the alert (33-31) |
| 35 | Time interval between the occurrence of the event and the occurrence registration in the database of the prototype (32-31) |
| 36 | Time interval between the occurrence registration in prototype database and the alert (33-32) |

Indicator 1 tells how many risk profiles are actually being followed by the transaction execution. This value is determined individually and manually by the researcher by observing the occurred operations in each transaction execution included in the report, and the risk profiles of reference defined in the Risk Profiles Repository.

Indicators 2 and 3 are also determined by the researcher by using the same method stated in the previous indicator and intend to indicate the number of positive and negative risk profiles, which are being followed by the transaction execution.

Indicators 4, 7 and 10 show, respectively, the number of risk profiles which were correctly identified by the prototype; the number of risk profiles which were incorrectly identified by the prototype and the number of risk profiles which were not identified. These indicators are intended to determine the success rate in the identification of risk profiles. Their values result from the observation of the risk profiles associated with each transaction execution (data in the reports generated by the prototype) and their comparison with the risk profiles which were actually followed by the transaction execution specified by indicator 1.

Indicators 5 and 6 present the number of risk profiles, positive and negative respectively, which were correctly identified by the prototype. These values are determined by using the same method of the previous indicators and are intended to supplement indicator 4, enabling thus to determine the rate of risk profiles which were correctly identified by type (positive and negative).

Indicators 8 and 9 present the number of risk profiles, positive and negative respectively, which were incorrectly identified by the prototype. These values are determined by means of the same method of the previous indicators and are intended to supplement indicator 7, making it possible to determine the rate of risk profiles which were incorrectly identified by type (positive and negative).

Indicators 11 and 12 present the number of risk profiles, positive and negative respectively, which were not identified by the prototype. These values are determined using the same method of the previous indicators and are intended to supplement indicator 10, enabling to determine the rate of risk profiles which were not identified by type (positive and negative).

Indicators 13 and 14 respectively show the number of risk profiles which were correctly and incorrectly classified as negative risk profiles out of a total of negative risk profiles which were identified by the prototype. These values are determined by the researcher by observing the classification assigned by the prototype and comparing it with the records of the Risk Profiles Repository.

Indicators 15 and 16 respectively present the number of risk profiles which were correctly and incorrectly classified as positive risk profiles out of a total of positive risk profiles which were identified by the prototype. These values are determined by the method cited in the previous paragraph together with indicators 13 and 14. These indicators are intended to determine the rate of false positives and false negatives as regards the classification of risk profiles which were correctly identified by type (negative or positive) by the system.

Indicators 17 and 18 show, respectively, the number of risk profiles which were correctly and incorrectly classified as complete out of a total of risk profiles which were correctly identified by the prototype. These values are determined by the researcher by observing the classification assigned by the prototype and comparing it with the records of the Risk Profiles Repository.

Indicators 19 and 20 respectively present the number of risk profiles which were correctly and incorrectly classified as incomplete out of a total of risk profiles which were correctly identified by the prototype. These values are determined by the method cited in the previous indicators. Together with indicators 17 and 18, these indicators are intended to determine the rate of false positives and false negatives as regards the evaluation of risk profiles which were correctly identified by the system concerning the completion of transaction executions (complete or incomplete).

Indicators 21 and 22 respectively present the number of risk profiles which were correctly and incorrectly audited by the prototype regarding user permission (authorised or unauthorised) in transaction executions in situations when all executors have an authorised role. These values are determined by the researcher by observing the classification assigned by the prototype and the users associated to the transaction execution as executors and by comparing them with the records of the Risk Profiles Repository.

Indicators 23 and 24 respectively present the number of risk profiles which were correctly and incorrectly audited by prototype regarding user permission (authorised or unauthorised) in transaction executions in situations when at least one executor has an unauthorised role. These values are determined by the method cited in the previous indicators. Together with indicators 21 and 22, these indicators are intended to determine the rate of false positives and false negatives as regards this auditing.

Indicators 25 and 26 respectively present the number of risk profiles which were correctly and incorrectly audited by the prototype in regard to timing (in time or delay) in transaction executions in situations when the transaction is executed in time. These values are determined by the researcher by observing the classification assigned by the prototype and the date and time of occurrence of operations associated to the transaction execution and by comparing them with the records of the Risk Profiles Repository.

Indicators 27 and 28 respectively present the number of risk profiles which were correctly and incorrectly audited by the prototype concerning the timing (in time or delay) in transaction executions in situations when the transaction is executed with delay. These values are determined by the method cited in the previous indicators. Together with indicators 25 and 26, these indicators are intended to determine the rate of false positives and false negatives as regards this auditing.

Indicator 29 is the result of observation of the operations which have occurred in every transaction execution in order to determine whether we are facing a situation of alert (consider the transactions that followed an unknown risk profile and the transactions that followed only negative risk profiles, as situations of alert).

Indicator 30 indicates whether the prototype triggered alerts for every transaction execution. This value is determined by the researcher who investigates whether an e-mail was sent for every situation of alert and it aims to determine the rate of false positive and false negative of alerts in risk situations.

Indicator 31 indicates the date and time of the occurrence responsible for the state of alert. This data is stored the ERP database and is directly collected by the researcher. However, this happens only if there is state of alert.

Indicator 32 indicates the date and time of the detection of the occurrence responsible for the state of alert. This data is stored in the Real Online Transaction Repository. However, this happens only if there is state of alert.

Indicator 33 indicates the date and time of the alert. This data is retrieved from e-mail header by the researcher. However, this happens only if there is state of alert.

Indicators 34, 35 and 36 result from arithmetic operations (as stated in Table 12) and have the objective to determine the time intervals between the occurrence and detection of events and the alert.

Besides these instruments, the participants (elements that managed the simulated enterprises) were asked to take notes on the operations which were being carried out, and their execution date and time for later analysis, and to make it possible to evaluate whether all operations were monitored.

4.4 RESULTS

The methods presented above were implemented and after their implementation we found that two reports were generated per week, in average, in each of the three enterprises included in the case study so that their data could be analysed. From the three enterprises, 45 reports were collected and analysed. Each of these reports was analysed by the researcher in order to fill in the support file with the analysed data, presented in the section above.

Taking a broader view of the results obtained, we observe that during the case study applied to the three companies, 282 organisational transactions, made up of the occurrence of 1129 operations, were executed as shown in Table 13. These transactions and operations imposed the performance of 2423 analyses supported by the reports generated by the prototype. The number of analyses corresponds to the number of possible risk profiles for the various transactions to be examined in all reports. Hence, the number of analyses is much higher than the number of transactions, because the identification of many possible risk profiles for an incomplete transaction execution may be common. Out of a total of 2423 analyses, 880 positive risk profiles, 1306 negative risk profiles and 237 unknown risk profiles have been identified (Table 14).

Furthermore, with respect to the notes that that participants took about the performed operations, all annotated operations were detected and monitored by the prototype. However, the number of operations detected was slightly higher than the amount annotated by the participants. This is due to only one reason: when a participant performs an update to one of the lines of a document, the system also automatically updates the header of that document, i.e. an update operation executed over a document means that there are more records updated in the database than those the user has perception of. This result allows us to validate that the requirement Req1 was fulfilled by the prototype.

Moreover, given the 2186 possible risk profiles (positive and negative), it has been observed that 2115 were indicated as performed by users with authorised roles and the remaining 71 were indicated as performed by users with unauthorised roles; 1231 possible risk profiles were indicated as performed in time and the remaining 955 with

delay. Only 2186 possible risk profiles, which are known and defined in the Risk Profiles Repository, were considered for this analysis, because they are the ones in which the evaluation regarding the authorisation of users and the timing in which transactions are executed are possible. These evaluations are not possible with the 237 unknown risk profiles, since there is no reference data in the Risk Profiles Repository.

Table 13 - Number of transactions, operations and analyses carried out during the case study

| | Transactions | Operations | Analyses |
|---------------------|---------------------|-------------------|-----------------|
| Enterprise 1 | 118 | 542 | 1148 |
| Enterprise 2 | 117 | 430 | 1200 |
| Enterprise 3 | 47 | 157 | 75 |
| Total | 282 | 1129 | 2423 |

Table 14 - Number of risk profiles analysed by type

| | Positive Risk Profiles | Negative Risk Profiles | Unknown Risk Profiles | Total |
|---------------------|-------------------------------|-------------------------------|------------------------------|--------------|
| Enterprise 1 | 534 | 454 | 160 | 1148 |
| Enterprise 2 | 303 | 831 | 66 | 1200 |
| Enterprise 3 | 43 | 21 | 11 | 75 |
| Total | 880 | 1306 | 237 | 2423 |

In Appendix V (available in the CD which supports this thesis) it is also possible to observe in detail other information gathered from the analysis of the reports generated by the prototype, as follows:

- how the number of occurred operations are distributed by enterprise and by operation type;
- how the number of possible risk profiles are distributed by enterprise, by type of risk profile (positive and negative) and by risk profile defined in the Risk Profiles Repository.

With regard to the support file with the indicators (Appendix IV, available in the CD which supports this thesis) resulting from the analysis of the reports, and made up of 745 situations (rows of worksheet), which correspond to 2423 analyses, some important conclusions about the performance of the prototype can be drawn:

- 1) From indicators 1-12 we can conclude that the prototype has been able to:
 - a) Correctly identify all possible risk profiles, positive and negative, for every transaction execution, regardless of their state of completion when the transaction execution followed one or more known risk profiles defined in the Risk Profiles Repository. This is because for all situations in which the researcher identified risk profiles for the transaction execution (indicators 1, 2 and 3), the prototype identified exactly the same possible risk profiles (indicators 4, 5 and 6), causing indicators 7 and 12 to be assigned value zero, in other words, the prototype did not incorrectly indicate any possible risk profile and it did indeed indicate the possible risk profiles, which should have been indicated;
 - b) Correctly identify an unknown transaction, regardless of their state of completion when its execution did not follow any of the risk profiles which are known and defined in Risk Profiles Repository. This is because for all situations when the researcher did not identify possible risk profiles of the transaction execution (indicators 1, 2 and 3), the prototype did not identify any possible risk profile either (indicators 4-6 and also indicators 7-12).

Note that a single unexpected behaviour has been observed in these results but it has been identified, defined and justified. We refer to the situation that occurred when the user repeated the same operation consecutively, and the prototype considered only one of these operations. This led to an incorrect assessment of the possible risk profiles for this transaction execution. Specifically, transactions with ID 20088, 20089, 20090, 20091, 20094 and 20095 were composed of occurrences of the operations of issuing the invoice and the respective receipt, and then the respective accounting entry. The latter occurred twice in a row by user error, i.e. those

transactions were completed with two consecutive accounting entries. In Risk Profiles Repository there is no similar risk profile and these seven transactions should thus have been identified as unknown. However, the prototype indicated the possible risk profiles as if only a single accounting entry existed, despite the fact that the alert was properly activated. This behaviour is due to a flaw in the algorithm of the component Transaction Comparator. As the reason for this failure is limited to a well identified and defined problem, these seven situations have been discarded and they have not been considered for statistical analysis of these results.

This result allows us to validate that the requirements Req3 and Req4 were fulfilled by the prototype.

- 2) From indicators 13-16 we can conclude that the prototype has been able to:
 - a) Correctly classify as positive risk profile all possible positive risk profiles identified in transaction executions;
 - b) Correctly classify as negative risk profile all possible negative risk profiles identified in transaction executions.

Note that the prototype presents no deficiencies in the classification of the possible risk profiles identified in transaction executions regarding their type. This result allows us to validate that the requirement Req8 was fulfilled by the prototype.

- 3) From indicators 17-20 we can conclude that the prototype has been able to:
 - a) Correctly classify as complete the transaction executions whose possible risk profile is also complete;
 - b) Correctly classify as incomplete the transaction executions whose possible risk profile is also incomplete.

Note that the prototype shows no deficiencies in the classification of the possible risk profiles identified in transaction executions regarding their completion. This result allows us to validate that the requirement Req7 was fulfilled by the prototype.

- 4) From indicators 21-24 we can conclude that the prototype has been able to:

- a) Correctly audit all possible risk profiles identified in transaction executions as regards the transaction executors, when they were performed only by users with authorised roles;
- b) Correctly audit all possible risk profiles identified in transaction executions as regards the transaction executors, when they were performed only by users with unauthorised roles.

Note that the prototype presents no deficiencies in the auditing of authorisation of users to perform transactions. This result allows us to validate that the requirement Req7 was fulfilled by the prototype.

- 5) From indicators 25-28 we can conclude that the prototype has been able to:
 - a) Correctly classify, as performed in time, all possible risk profiles identified in the transaction executions regarding their time of execution, when all operations were carried out without delay;
 - b) Correctly classify, as performed with delay, all possible risk profiles identified in the transaction executions regarding their time of execution, when at least one operation was carried out with delay;

Note that the prototype presents no deficiencies in the classification of the possible risk profiles identified in the transaction executions regarding their time of execution. This result allows us to validate that the requirement Req7 was fulfilled by the prototype.

- 6) From indicators 29-30 we can conclude that the prototype has been able to :
 - a) Correctly identify almost all situations that are not alert (state 0) caused by the existence of transaction executions whose risk profiles are positive or because e-mail alerts were already sent in the past in alert situations, and therefore the prototype does not send e-mail alerts (Table 15).

- b) Correctly identify almost all situations that are alert (state 1) caused by the existence of transactions executions whose risk profiles are unknown, and therefore, the prototype sends e-mail alerts (Table 16).
- c) Correctly identify all situations that are alert (state 2) caused by the occurrence of transaction executions whose risk profiles are negative, and therefore, the prototype sends e-mail alerts (Table 17).

Table 15 - Table of frequencies of State 0

| | Frequency | Percent | Cumulative Percent |
|--------------|------------------|----------------|---------------------------|
| No | 597 | 99.3 | 99.3 |
| Yes | 4 | 0.7 | 100.0 |
| Total | 601 | 100,0 | |

Table 16 - Table of frequencies of State 1

| | Frequency | Percent | Cumulative Percent |
|--------------|------------------|----------------|---------------------------|
| No | 1 | 0.8 | 0.8 |
| Yes | 122 | 99.2 | 100.0 |
| Total | 123 | 100.0 | |

Table 17 - Table of frequencies of State 2

| | Frequency | Percent | Cumulative Percent |
|--------------|------------------|----------------|---------------------------|
| Yes | 17 | 100.0 | 100.0 |
| No | 0 | 0.0 | 100.0 |
| Total | 17 | 100.0 | |

Note that these conclusions have been drawn considering only 741 out of a total of 745 cases for analysis. The remaining four situations, which have not been considered, refer to situations which occurred in the early days of the case study, in which some instability of the prototype was noted and this made it impossible to ascertain whether the e-mail alerts were sent in these four situations.

In state 0, e-mail alerts were checked in the four situations that were not alert. These four situations refer to transaction executions whose risk profile was unknown but that had already been alerted in the past immediately after the identification of the irregularity. Thus, two e-mail alerts were sent in these four transaction executions. For this case, a binomial test was made, and for the hypotheses $H_0: p=99.7\%$ vs. $H_1: p<99.7\%$, we obtained a $p\text{-value}=0.109>0.01$. Thus, there is no rejection of H_0 for significance level of 1%. Hence, we can conclude that the percentage of not being e-mailed an alert is equal to or greater than 99.7%, with a significance level of 1%.

In state 1, an e-mail alert was not checked in a situation of transaction execution whose risk profile was unknown. For this situation, the binomial test was made, and for the hypotheses $H_0: p=99.9\%$ vs. $H_1: p<99.9\%$, we obtained a $p\text{-value}=0.116>0.01$. Thus, there is no rejection of H_0 for significance level of 1%. Hence, we can conclude that the percentage of being e-mailed an alert is equal to or greater than 99.9%, with a significance level of 1%.

In state 2, e-mail alerts were sent in all situations in which they must have been sent.

These results allow us to validate that the requirement Req9 was fulfilled by the prototype.

In order to measure the time that the prototype took to detect the operations performed in the ERP and which were intended to be monitored, the researcher searched the date and time of execution of the operations, which are indicated in the respective records in the ERP database, and the date and time of detection of these operations by the prototype, which are indicated in the respective records of prototype database. The subtraction of these value determines the interval of time between the occurrence and the detection of the operations.

Regarding these intervals of time, 806 measures were performed out of a total of 1129 operations executed during the case study. The intervals of time of all 1129 operations were not possible to be determined, because there were some situations in which the measurement has not been allowed, for example: most documents were recorded in tables that had a field for the date and time of the last update, so if more than one operation was executed in the same document since the last measurement by

the researcher, only in the last operation performed in this document would be possible to get the date and time of execution; when operations of deletion were executed via ERP interface (without being scripted in the database), the respective records disappeared from the database and it became impossible to measure the interval of time because of the lack of data; and on the first days of the case study, some database triggers had been noticed as being incomplete, because they were registering only the hours and minutes, without the seconds, of the date and time of operations detection. Therefore, the measurement of the interval of time of the operations that were being monitored by this set of triggers badly scaled was not possible to be carried out.

To analyse these measured time intervals, the boxplot of Figure 39 was considered. The boxplot below represents the 806 observed values of the time interval between the occurrence of each operation and its detection by the prototype. Hence, we observe that: half of the occurrences were detected in zero seconds, and only 25% of cases had detection time greater than one second. Some outliers whose values are highlighted from most of the observations are also observed because they are quite superior, ranging between 3 and 8 seconds.

Observing the table of frequencies (Table 18), a more detailed analysis is possible to be made, allowing to conclude that 96.7% of the operations were detected by the prototype up to 1 second after their occurrence, and 74.4% of operations were detected at the very same second as their occurrence. This result allows us to validate that the requirement Req10 was fulfilled.

Regarding the time of sending the e-mail alert, we can observe from the boxplot of Figure 40 and the respective table of frequencies (Table 19) that: the overwhelming majority of e-mail alerts were sent up to 9 seconds after the detection of the operation which caused the alert situation; at least 75% of the e-mails were sent up to 6 seconds; at least half of the e-mail alerts were sent up to 5 seconds; and in only 25% of the situations the e-mails were sent up to 4 seconds, despite having been observed cases in which the alerts were sent up to 1 second. In addition, four outliers were observed, ranging between 10 and 23 (these being the maximum values). This result allows us to validate that the requirement Req9 was fulfilled.

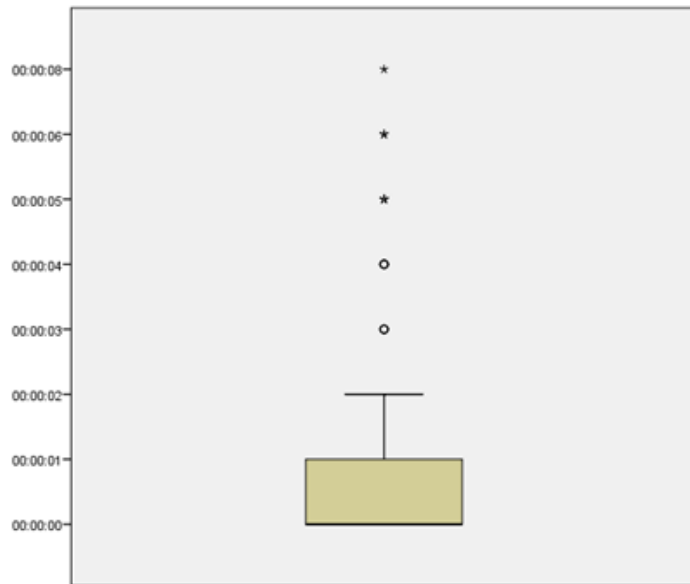


Figure 39 - Boxplot of the interval of time of operations detection

Table 18 - Table of frequencies of the interval of time of operations detection

| | Frequency | Percent | Cumulative Percent |
|----------------|------------------|----------------|-------------------------------|
| 0:00:00 | 600 | 74.4 | 74.4 |
| 0:00:01 | 179 | 22.2 | 96.7 |
| 0:00:02 | 6 | 0.7 | 97.4 |
| 0:00:03 | 5 | 0.6 | 98.0 |
| 0:00:04 | 6 | 0.7 | 98.8 |
| 0:00:05 | 6 | 0.7 | 99.5 |
| 0:00:06 | 3 | 0.4 | 99.9 |
| 0:00:08 | 1 | 0.1 | 100.0 |
| Total | 806 | 100.0 | |

Moreover, the information in the reports (an example in Appendix III, which is available in the CD that supports this thesis) and in the interface (Figure 41) of the prototype allows us to conclude that the requirements Req5, Req6, Req7 and Req8 were fulfilled.

Table 19 - Table of frequencies of the interval of time when sending an e-mail alert

| | Frequency | Percent | Cumulative Percent |
|-----------------|-----------|---------|--------------------|
| 00:00:01 | 5 | 4.7 | 4.7 |
| 00:00:02 | 7 | 6.5 | 11.2 |
| 00:00:03 | 11 | 10.3 | 21.5 |
| 00:00:04 | 25 | 23.4 | 44.9 |
| 00:00:05 | 20 | 18.7 | 63.6 |
| 00:00:06 | 16 | 15.0 | 78.5 |
| 00:00:07 | 8 | 7.5 | 86.0 |
| 00:00:08 | 7 | 6.5 | 92.5 |
| 00:00:09 | 4 | 3.7 | 96.3 |
| 00:00:10 | 1 | 0.9 | 97.2 |
| 00:00:12 | 1 | 0.9 | 98.1 |
| 00:00:16 | 1 | 0.9 | 99.1 |
| 00:00:23 | 1 | 0.9 | 100.0 |
| Total | 107 | 100.0 | |

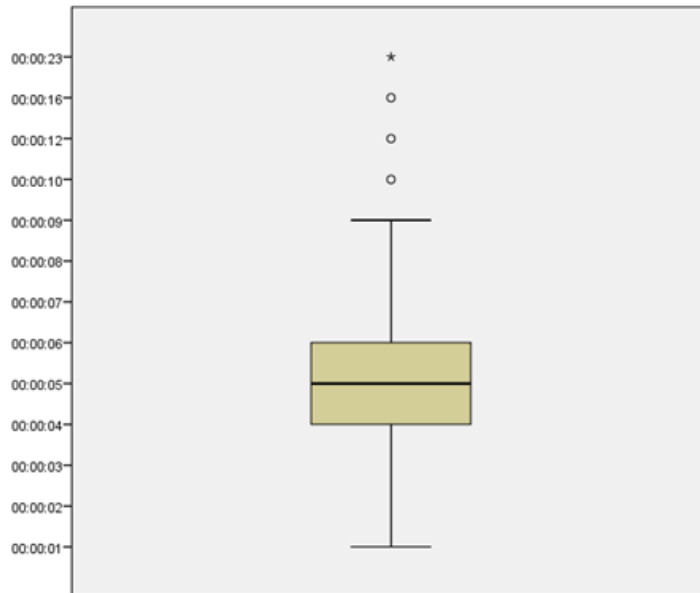


Figure 40 - Boxplot of the interval of time of sending an e-mail alert

Solution Proposal

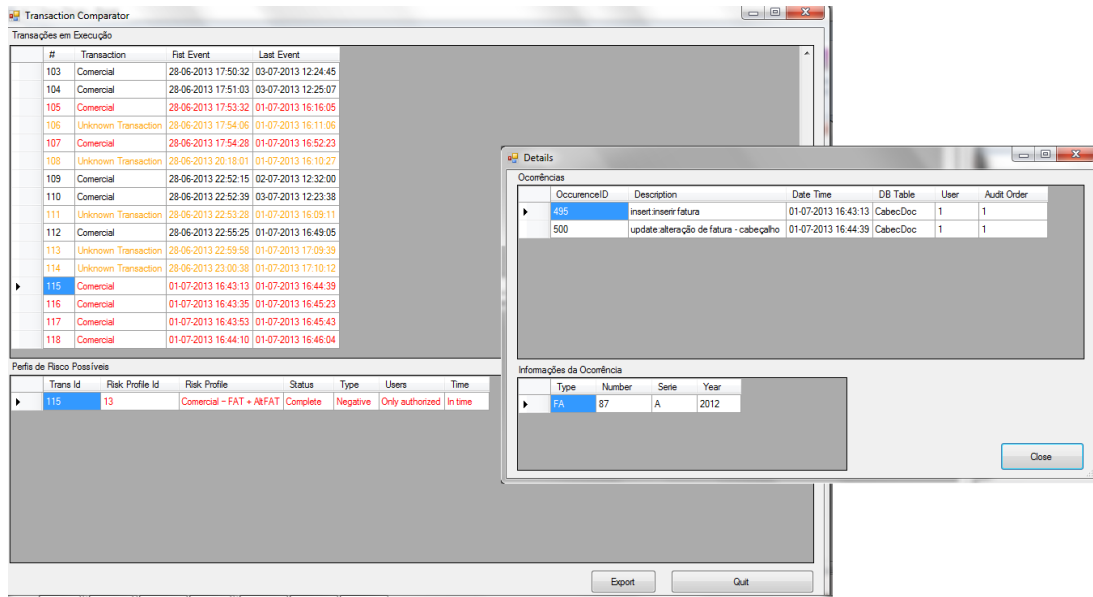


Figure 41 - Print screen of the interface of the prototype

Regarding the concepts of observability and controllability, which have also been defined as requirements, we can conclude, based on the prototype results analysed above, that the proposed system is completely observable and controllable. This conclusion is supported by the following results:

- all operations were detected and monitored by the prototype;
- the prototype presents no deficiencies in the classification of the possible risk profiles identified in transaction executions regarding their type, completion and time of execution;
- the prototype presents no deficiencies in the auditing of authorisation of users to perform transactions;
- the prototype provides an interface and reports as outputs which contain the history of the results of the transaction auditing and monitoring and a picture of the current situation regarding the organisational transactions still in progress; notifications to the users are also provided as output in all negative situations.

It means that all inputs are processed and all of them induce a certain result in finite time. There are no state variables which do not reach the intended objectives (controllability). In addition, all inputs noticeably affect the system output in a finite time, and the users are capable of knowing the current state of execution of the monitored transactions based on the outputs (observability).

All these results allow us to conclude that the initial requirements (section 4.1) have been met in full.

5

VALIDATION OF RESEARCH QUESTIONS AND HYPOTHESES

This chapter discusses the results which were obtained during the research performed within this thesis, with the purpose to address the research questions and the research hypotheses.

As stated in section 1.2 of this thesis, the research has been guided by three research questions and some research hypotheses:

Q1 - Is it feasible to develop information systems with continuous assurance services applicable to any organisational transaction represented by an ontological model and executed exclusively in digital format?

H1.1 - The proposed information system provides functionalities related to continuous assurance services.

Q2 - What are the essential and the most important characteristics of an information system with continuous assurance services?

Q3 - How to develop an information system with continuous assurance services enabling it to be applicable to any organisational transactions?

H3.1 - The development of a risk profiles repository of organisational transactions represented by an ontological model, is feasible and supports information systems with continuous assurance services.

Because the research questions Q2 and Q3 are derived from the research question Q1, these will be the first to be addressed in this chapter, and then their answers will allow a more comprehensive answer to the research question Q1.

Research Question Q2

What are the essential and the most important characteristics of an information system with continuous assurance services?

The survey methodology was followed in order to answer this research question, through the application of the Delphi method (chapter 3). This method allows to obtain the opinion of a panel of experts on the most important and essential characteristics of information systems with continuous assurance services. This study was relevant to this research because the literature survey had not enabled to obtain this information, which must be simultaneously objective and measurable through the study of an implementation of an information system with continuous assurance services and the analysis of its results.

From the literature survey, the researcher collected some relevant and summarised inputs, including objectives, components, functionalities and outcomes of other implementations of Continuous Assurance. A wide range of quantitatively measurable characteristics (metrics) were acquired from the synthesis of those inputs. In addition, the researcher has grouped these metrics into dimensions, in accordance with the nature of the functionality. Through the application of the Delphi method, these metrics were submitted to the evaluation by a panel of experts in order to be classified regarding their appropriateness for inclusion and their importance as a characteristic of an information system with continuous assurance services.

As a result, 15 metrics, which met high or excellent consensus by the panel of experts, were identified, with regard to their inclusion as a characteristic of an information system with continuous assurance services and consequently as metrics to include in a model to evaluate such type of information systems. Regarding the importance of these characteristics, all metrics were classified by the panel, with high or excellent consensus, as very important features.

In conclusion and answering to the research question Q2, the essential and the most important characteristics of an information system with continuous assurance services are grouped into three dimensions and one requirement, as follows:

- Monitoring (dimension)
 - i. Real-time monitoring of operations
 - ii. Real-time identification of irregular operations

- iii. Real-time verification of the processing of required operations at all previous steps
- iv. Real-time detection of lack of operations
- Compliance (dimension)
 - i. Recognition of execution patterns
 - ii. Ascertaining of fulfilling of rules
 - iii. Detection of potential errors
 - iv. Verification of compliance of existing policies
- Estimation (dimension)
 - i. Estimation of possible results
 - ii. Determination of possible execution patterns which are likely to be followed
- Reporting (requirement)
 - i. Real-time presentation of the executed operations which were monitored
 - ii. Real-time presentation of execution patterns which are being followed or are likely to be followed
 - iii. Real-time presentation of the compliance verification in transactions executions
 - iv. Real-time presentation of the risk estimated on determining possible execution patterns
 - v. Real-time alert for irregular situations in monitoring, compliance verification and estimation of negative results.

Research Question Q3

How to develop an information system with continuous assurance services enabling it to be applicable to any organisational transactions?

The architecture which was proposed in this thesis has revealed to be effective for the development of an information system with continuous assurance services. This conclusion is grounded on the fact that the prototype, which is the result of the implementation of this architecture, has outcomes related to the characteristics that

have been designated as essential and very important for an information system with continuous assurance services. In fact, as we can find below in the validation of the research hypothesis H1.1, all those characteristics have been validated. Therefore, the prototype, which was developed according to the proposed architecture, is presented as an information system with continuous assurance services.

Thus, according to the proposal, an information system with continuous assurance services should be modular and should comprise:

- a layer of internal control mechanisms which must be conceptualised according to the adopted ontological model and incorporated in the operational information system, which supports the execution of the organisational transactions to be monitored and audited;
- a repository which must be able to record, maintain and manage all the information is derived from internal control mechanisms and represents the transactional events occurring on-line;
- a risk profiles repository which must be able to maintain and manage the known negative and positive profiles of each organisational transaction to be monitored and audited (these profiles must be modelled according to the ontological model studied);
- a component which must be able to compare the data from the internal control mechanisms with the records maintained in the risk profiles repository and that can determine which profile is being followed by running each transaction;
- mechanisms which must be able to provide and disseminate the results of the transaction auditing and monitoring and a picture of the current situation regarding the organisational transactions still in progress. These mechanisms should work as an interface with the users of the system through queries, reports, notifications and alerts;

Research Hypothesis H3.1

The development of a risk profiles repository of organisational transactions represented by an ontological model, is feasible and supports information systems with continuous assurance services.

For the validation of this hypothesis, a database was designed, one whose entities and their relationships reflect the axioms of the adopted ontological model. This database model is presented and justified in section 4.2.3.

The validation of this database as a risk profiles repository was only possible after successful instantiation of various risk profiles. To deploy the prototype in the three organisations which were target of study, twenty risk profiles (ten positive and ten negative) were defined and instantiated. This risk profiles were instantiated without any problems. It means that the entities and their relationships are sufficient to represent all the necessary data associated with the risk profiles of organisational transactions in compliance with the adopted ontology. Moreover, it also means that the database is not overdesigned, because all data were represented, and there were no data redundancy.

The risk profiles repository, as it is designed in this work, proved to be an important element to support the proposed functional architecture, i.e. to support an information system with continuous assurance services. Thus, it presents itself as a module which allows the parameterisation of the system, including the identification of the risk profiles of organisational transactions which are intended to be monitored, controlled and audited.

Therefore, the risk profiles repository may be seen as a link between technology and organisational aspects, because it reflects the organisational knowledge about the issues to be considered and addressed in the monitoring and auditing of organisational transactions. Moreover, it represents technologically this knowledge so that it is able to interact with other technological artefacts. In this particular case, the risk profiles repository interacts with the algorithm "Transaction Comparator", providing it with the necessary references and data to evaluate the data derived from the internal control mechanisms, which are responsible for monitoring transactions.

Hence, we can state that the Risk Profiles Repository, as designed and presented in this thesis, is technologically feasible to be developed and that it supports information systems with continuous assurance services.

Research Question Q1

Is it feasible to develop information systems with continuous assurance services applicable to any organisational transaction represented by an ontological model and executed exclusively in digital format?

In order to answer this question we must consider the following aspects:

- A proposal of architecture for the development of an information system with continuous assurance services was made. This architecture was technologically developed and deployed. The respective prototype was tested in three situations in which the organisational environment was simulated;
- The validation of the research hypothesis H1.1 (see below) indicates that the prototype is an information system with continuous assurance services because all characteristics considered essential and very important for an information system of this type (contribution of the research question Q2) were checked and confirmed in the prototype;
- The use of an ontological model in the development and in the operationalisation of the proposed system gives adaptability and flexibility to the system, since any organisational transactions which are represented by the adopted ontology can be monitored and audited by the prototype, because their ontological representation is object of parameterisation of the system. In other words, to implement the system within an organisational context, you only have to select the organisational transactions which are intended to be monitored, controlled and audited. Furthermore, they are represented according to the ontology so that you can identify the operations or events which require control mechanisms and thus make it possible to define the respective risk profiles and their instantiation in the Risk Profiles Repository. Hence, we can say that any organisational transactions represented by the

adopted ontological model may be subject to the services of continuous assurance provided by the proposed system.

These aspects allow to positively answer this research question, and therefore it is possible to develop information systems with continuous assurance services applicable to any organisational transactions which are represented by an ontological model and executed exclusively in digital format.

Research Hypothesis H1.1

The proposed information system provides functionalities related to continuous assurance services.

In order to validate this research hypothesis, each of the characteristics identified in the answer of the research question Q2 were checked.

- Monitoring (dimension)

- i. Real-time monitoring of operations

The results in section 4.4 indicate that almost all operations, which were performed in the case study, were detected up to 2 seconds after their occurrence. Specifically 96.7% of the operations were detected by the prototype up to 1 second after their occurrence and 74.4% of operations were detected at the very same second as their occurrence.

To evaluate this result, consider that: real-time is defined within this work as the time interval closer to the occurrence of an event; the purpose of the system is not to act in a direct and intrusive way on the execution of organisational transactions, but rather to work with reporting functions; the time and the rhythm of organisational transactions are variable and in different orders of greatness (transactions may have running times in the order of minutes, days or several months depending on the situation in question); a real-time system is one where the correctness not only depends on the functionality but also on the timeliness of this functionality; the time in which the user of the prototype has to react in a corrective way, after

being alerted of an anomaly, is also variable, depending on the pace of the transaction in question.

With these considerations we summarise that the real-time requirement within this thesis is the ability of the prototype to detect operations in the shortest time possible, enabling the user to effectively monitor the occurrence of operations before of the execution of the next related operation, i.e. the time of detection must accompany and follow the rhythm and pace in the execution of transactions.

We can conclude that the prototype is able to monitor operations in real-time, because 74.4% of the operations were detected at the very same second as their occurrence and because the time of detection of the remaining 25.6% operations is very inferior when compared, in common sense, with the time of execution of the operations associated with organisational transactions, due to the fact that the latter depends on the capacity and speed of execution by users of operational information systems, and therefore the order of greatness of the running times of organisational transactions are much higher than the capacity of detection of the prototype.

Another reason that leads us to this validation is that all operations have been detected by the prototype, and therefore effectiveness of the monitoring of the prototype is proved.

ii. Real-time identification of irregular operations

The results evaluated in the previous item are as valid for the regular operations as for the irregular. Thus, effectiveness of monitoring of irregular operations is also assured.

However, the identification of an operation as irregular is only possible due to the coexistence of other characteristics pertaining to the compliance dimension. When the prototype is able to verify the non-fulfilling of rules, to detect potential errors or to detect the compliance of existing policies, it is possible, through the prototype, to identify

which irregular operation is causing the negative situation (e.g. delay in execution, unauthorised executor or unexpected operation).

Therefore, we can ensure that the prototype is capable of identifying irregular operations in real time.

iii. Real-time verification of the processing of required operations at all previous steps

This characteristic of the prototype is also checked, but it has to be analysed in parallel with another characteristic of the prototype: the capacity of recognition of execution patterns (dimension compliance).

When an execution pattern (risk profile) is identified in an organisational transaction execution by the prototype, the prototype is ensuring that the sequence of operations is being properly performed in accordance with this risk profile. Thus, when we validate that the prototype is able to correctly identify all risk profiles associated to a transactions execution, we are also validating this characteristic.

Nevertheless, we cannot assertively come to conclusion about the time required for this identification, because proper controls have not been designed in order to collect these data. However, considering the intervals of time which were taken as indicators of the time to send e-mail alerts in negative situations, we are elucidated that the processing time for verification of the required processing of operations at all previous steps precedes that time. Although the method of measuring the time of sending e-mail alerts is not strict, as indicated in the results section, this is indicative of its effectiveness. Being that the verification is performed before the alert (the alert is always a consequence), we can then conclude that this verification is processed in real-time for the same reasons indicated in i.

iv. Real-time detection of lack of operations

This characteristic is also related to the capacity of recognition of execution patterns (dimension compliance), because the lack of an operation in a sequence of operations of an organisational transaction

is detected during the continuous comparison with the defined risk profiles in the Risk Profiles Repository. When an operation is lacking, and this lack is safeguarded in a defined risk profile, this risk profile is automatically indicated and associated with this fault. But if this lack is not safeguarded in any risk profile, this failure will be associated to a situation of unknown risk profile, which is cause of alarm by the prototype.

The real-time aspect is similar to the item iii, i.e. no control was designed to measure the processing time of the algorithm for this detection, but the time spent until sending an alert can be indicative of the effectiveness of this detection, since the detection time always precedes the alert time (the alert is always a consequence).

- Compliance (dimension)

- i. Recognition of execution patterns

As the results section states: the prototype correctly identifies all possible risk profiles, positive and negative, for every transaction execution, regardless of their state of completion when the transaction execution followed one or more known risk profiles defined in the Risk Profiles Repository; the prototype did not incorrectly indicate any possible risk profile; and it did indeed indicate the possible risk profiles, which should have been indicated. Moreover, the prototype correctly identifies an unknown transaction, regardless of their state of completion when its execution did not follow any of the risk profiles which are known and defined in the Risk Profiles Repository.

For these reasons, we can affirm that the prototype is capable of recognising execution patterns.

- ii. Ascertaining of fulfilling of rules

Regarding this characteristic, some issues were addressed and parameterised as rules in the risk profiles: the sequence of operations (already validated in item i of this dimension and in items iii and iv of the dimension monitoring); the time at which each transaction was

executed; the authorisation of users as executors; and the state of completion of transaction executions.

Regarding the time at which each transaction was executed, we can see in the results section that the prototype correctly classifies, as performed in time, all possible risk profiles identified in the transaction executions regarding their time of execution, when all operations were carried out without delay; it correctly classifies, as performed with delay, all possible risk profiles identified in the transaction executions regarding their time of execution, when at least one operation was carried out with delay.

With regard to the auditing of authorisation of users to perform transactions, the prototype correctly audits all possible risk profiles identified in transaction executions as regards the transaction executors, when they were performed only by users with authorised roles and when they were carried out only by users with unauthorised roles.

As regards the classification of the possible risk profiles identified in transaction executions regarding their completion, the prototype correctly classifies as complete the transaction executions whose possible risk profile is also complete; it correctly classifies as incomplete the transaction executions whose possible risk profile is also incomplete.

Because the prototype reveals no deficiencies in these audits, this characteristic is also checked and validated.

iii. Detection of potential errors

Based on the results section: the prototype correctly classifies as negative risk profile all possible negative risk profiles identified in transaction executions; and it correctly identifies an unknown transaction, when its execution did not follow any of the risk profiles which are known and defined in Risk Profiles Repository.

Thus, if all negative risk profiles are correctly identified, as well as all transactions which follow unknown risk profiles, are correctly identified, then we can say that the prototype detects potential errors.

iv. Verification of compliance of existing policies

This characteristic is also validated for the same reasons which were presented in item ii of this dimension. Rule and policy are not differentiated in this thesis, and their implementation is exactly the same, since their only difference lies in their origins. To be more specific, rule refers to all conditions imposed by national or international directives, while policy refers to a set of procedures defined internally by each organisation. In this thesis, this differentiation is not made, because the aim of the study is to validate the ability to audit guidelines, regardless of the fact they are rules or policies.

• Estimation (dimension)

i. Estimation of possible results

This characteristic must be evaluated in combination with the next characteristic, which is also validated. If the prototype is able to determine possible risk profiles for a particular organisational transaction which is not yet fully completed, it is possible to estimate qualitatively the result of this transaction.

On the one hand, if there is not a possible positive risk profile associated with the transaction execution, it means that the organisational transaction will result in a negative or unknown situation for the organisation. On the other hand, if the possible risk profiles associated with the transaction execution are positive, results without negative effects for organisations are predicted.

With the aforementioned, we can validate this characteristic basing on the fact that the prototype is able to: correctly classify as positive risk profiles all possible positive risk profiles identified in transaction executions; correctly classify as negative risk profiles all possible

negative risk profiles identified in transaction executions; correctly identify all possible risk profiles, positive and negative, for every transaction execution, regardless of their state of completion when the transaction execution followed one or more known risk profiles defined in the Risk Profiles Repository; not to incorrectly indicate any possible risk profile; indeed indicate the possible risk profiles, which should have been indicated; correctly identify an unknown transaction, regardless of their state of completion when its execution did not follow any of the risk profiles which are known and defined in Risk Profiles Repository.

ii. Determination of possible execution patterns which are likely to be followed

This characteristic is also validated because, according to the results section, when an organisational transaction is initiated, the prototype presents the possible risk profiles for this transaction execution regardless of their state of completeness. Therefore, before the completion of the transaction execution, the pattern or patterns that are being followed by the transaction execution are already possible to be estimated. As we have seen in previous items, the prototype does not show any deficiencies in the identification of risk profiles.

- Reporting (requirement)

The following set of characteristics comprises the real-time concept. But as aforementioned, no controls have been developed in order to measure the processing time of the algorithm. However, the time of processing of sending e-mail alerts in negative or unknown situations was possible to measure. Despite not being accurate for the reasons already mentioned, this measurement is indicative of the order of greatness of this time interval. Furthermore, because the alert is a consequence, it means that all the other operations have a processing time equal or inferior to the time of processing alerts. Thus, we will consider that the response time of the prototype is

consistent with the pace of execution of organisational transactions, and therefore, the real-time is assured.

i. Real-time presentation of the executed operations which were monitored

The prototype allows the visualisation of the performed operations in two media: consulting the report issued by the system, in which one of its worksheets - "Transaction Details" - presents data about the performed operations for each organisational transaction execution; consulting the interface of the system and by clicking an organisational transaction which is in progress or already completed, thus enabling the user to see the set of performed operations associated with this organisational transaction and some information about each operation. The information is exactly the same in both media, and the difference is their usability: whilst information in the interface is exclusively for reading, the report comes in spreadsheet format allowing its free usage.

Thus, this requirement is validated.

ii. Real-time presentation of execution patterns which are being followed or are likely to be followed

As in the previous item, this information is also provided both by the interface and by the report. In the interface of the system, clicking in a monitored organisational transaction, the possible risk profiles associated with it are immediately displayed. In the report, there is a sheet called "Possible Risk Profiles" which presents data about the possible risk profiles which are being followed or which are likely to be followed by each transaction execution.

Thus, this characteristic is also validated.

iii. Real-time presentation of the compliance verification in transactions execution

The developed prototype enables to: validate sequences of operations or execution patterns associated with each organisation transaction, indicating if a transaction execution is positive, negative or unknown;

audit the users who were executors regarding their authorisation; monitor the status of completion of organisational transactions; and control the time at which transactions are executed. Therefore, regarding the compliance verification, it can attest that results of the previously mentioned controls are reported and presented both in the report and in the interface of the system.

In the interface of the system, this information is located in the area where the possible risk profiles are presented. In the report, this information is available in the "Possible Risk Profiles" worksheet.

iv. Real-time presentation of the risk estimated on determining possible execution patterns

This information is contained in possible risk profiles which were identified for each transaction execution through their classification as positive or negative. In other words, the prototype allows a qualitative estimation of the risk of the execution of transactions.

In addition to textual information, both interface and reports use different font colours to highlight unexpected situations or of higher risk.

Thus, this characteristic is also validated.

v. Real-time alert for irregular situations in monitoring, compliance verification and estimation of negative results

Regarding this characteristic, the prototype is able to: correctly identify almost all situations that are alert caused by the existence of transaction executions whose risk profiles are unknown (the percentage of being emailed an alert is equal to or greater than 99.9%, with a significance level of 1%); and correctly identify all situations that are alert caused by the transaction executions whose risk profiles are negative. In these two types of situations, the prototype sends e-mail alerts.

Regarding the measurement of time of the e-mail alert, it has already been mentioned that it is not very precise, because the clock of the e-

mail servers may not be synchronised. However, this measure may be indicative of the effectiveness of this feature. Thus, it was found that: the overwhelming majority of e-mail alerts were sent up to 9 seconds after the detection of the operation which caused the alert situation; at least 75% of e-mails were sent up to 6 seconds; at least half of the e-mail alerts were sent up to 5 seconds; and in only 25% of the situations, the e-mails were sent up to 4 seconds, despite having been observed cases in which the alerts were sent up to 1 second. In addition, four outliers were observed, ranging between 10 and 23 (these being the maximum values).

6

CONCLUSION AND FUTURE WORK

This thesis has been motivated by the current awareness of corporate governance and of the growing importance of monitoring, auditing and controlling the various organisational transactions. This awareness and solutions concerning it are a way not only to affirmatively respond to the current legislative and regulatory framework on continuous monitoring and continuous auditing, but also to provide organisations with the benefits of the adoption of mechanisms of continuous monitoring and auditing. The adoption of measures and solutions upon this topic enables the improvement and strengthening of risk control structures in order to provide greater security in the effectiveness of risk management activities of the organisations and ensure an appropriate management of key business risks, optimising the operational performance and reducing the associated risks.

Thus, this thesis focuses on answering to the implementation of continuous assurance services in information systems, presenting a solution with assurance services capable of monitoring organisational transactions supported by enterprise information systems. Furthermore, this thesis has brought some innovative elements, including the use of an ontological model to support the representation of organisational transactions and the implementation of a risk profiles repository with the goal to provide services of continuous assurance to the organisational transactions executed in digital format.

The adoption of a model for ontological representation of organisational transactions supports the improvement of assessment and estimation of risk associated with the execution of transactions, since the organisational transactions come to be represented by the essential events that compose them, allowing the construction of risk profiles of organisational transactions, and subsequently, the effective continuous identification of the risk associated with the execution of the transaction.

This view of monitoring, controlling and auditing organisational transactions is innovative since no reference to any implementations of risk profiles repository in the aforementioned way was evident in the literature review. Another innovative aspect of this view is the attempt to provide assurance services to organisational transactions following the structure of an ontology, which presents the transaction at a very low level, at its essence, contrary to what happens in most monitoring of transactions that occur at a high level.

Thus, this thesis focuses on the topic of implementation of continuous assurance services in information systems applicable to any organisational transaction, regardless of their type, dimension, business area or operational information system in which they are executed, having as support an ontological model to represent organisational transactions.

Therefore, the main research question has been emerged. It was intended to ascertain whether it is feasible to develop information systems with continuous assurance services applicable to any organisational transaction represented by an ontological model and executed exclusively in digital format.

To answer this central research question, it has been necessary to identify which characteristics are essential and the most important in an information system with continuous assurance services. Then, after conducting a survey on the topic, we designed a set of characteristics which any information system must have to provide continuous assurance services or, in other words, a set of metrics which enables assessing whether an information system has continuous assurance services. Meanwhile, a study was implemented following the Delphi method in order to validate this set of characteristics. The implementation of the Delphi method collected the opinion of a panel of experts which made it possible to validate all the presented characteristics with high level of consensus among the experts. From this study, we can also conclude that an information system with continuous assurance services has characteristics concerning three dimensions (monitoring, compliance and estimation) and functionalities of reporting.

Also allied to the central research question, another need has come up: to propose a solution to develop an information system with continuous assurance services,

enabling it to be applicable to any organisational transactions, also meeting the objectives of this thesis, i.e. making use of an ontological model to represent organisational transactions and of a risk profiles repository. Thus, this thesis also contributes with the proposal of a solution, based on a functional architecture which is modular and that meets the above requirements.

This proposal has been developed and the prototype has been implemented in a case study in a simulated environment, following the Design Science methodology. A scientifically rigorous research path was traced, including: assessing the relevance of the problem; designing a solution; its evaluation; development; definition of methods for data collection; and data analysis, enabling to determine the contributions that the developed artefact provides in the resolution of the problem under consideration. The presented results enable us to conclude that the proposed solution strongly contributes to a positive response to the central research question, because all the characteristics of an information system with continuous assurance services were checked, the effectiveness of the Risk Profiles Repository were also validated as well as the use of an ontological model to support the representation of organisational transactions. Moreover, the dual concepts of observability and controllability, which are requirements that should be applied to any system, are also verified in the developed system, as already demonstrated.

In conclusion, we can state that this thesis contributes to:

- a more comprehensive and better understanding upon the essential and most important features and functionalities of an information system with continuous assurance services;
- the design, validation and presentation of a model comprising dimensions and metrics, which allows it to be used as a tool or as a set of guidelines to evaluate information systems with continuous assurance services;
- ensure the feasibility of development and the effective use of an information system with full continuous assurance services, having as support an ontological model, and which is considerably flexible and adaptable in order to be applicable to any organisational transactions;

- ensure the feasibility of development of a risk profiles repository of organisational transactions, based on an ontological model and database technologies;
- demonstrate that a risk profiles repository is an important element in information systems with continuous assurance services, as a source of references to support continuous monitoring, continuous auditing and controlling of the risk associated with the execution of organisational transactions.

Moreover, this research contributes to a new vision of organisational auditing focused on assurance services in transactions executed and supported in a digital format in compliance with the formalisms of a business ontological model of organisational transactions.

However, there is still some work to be carried out. Some suggestions for future work are presented below:

- develop a more functional interface from the point of view of usability, both in the dissemination of the results of monitoring and auditing and in the management of risk profiles in the Risk Profiles Repository, because in this work the risk profiles are directly inserted in the repository by the DBMS without the assistance of any interface;
- developing an additional module which allows the system self-learning of risk profiles. In other words, the system should be able to suggest new risk profiles to the user based on information regarding to unknown risk profiles, which are constantly identified by the system.
- determine the effectiveness of the proposed solution with organisational transactions, whose operations are not solely performed in a single operational information system or solely in digital format. This suggestion poses new challenges, namely regarding the combination of different types of internal control mechanisms (e.g. internal control in paper-based business processes (R. P. Marques, Santos, & Santos, 2010; R. P. Marques, Santos, & Santos, 2012a)) to monitor the operations and the way they should interact with the system;

- develop a model which allows to validate the compliance of risk profiles in relation to legislative and regulatory framework, by which organisational transactions are governed. This thesis only focuses on the issue of technology, but it would be interesting to combine the socio-economic side in order to develop a model that allows the validation of risk profiles recorded in the repository;
- determine the net benefits of implementing the solution proposed.

REFERENCES

- Abadi, D., Ahmad, Y., Balazinska, M., Cetintemel, U., Cherniack, M., Hwang, J., . . . Zdonik, S. (2005). *The Design of the Borealis Stream Processing Engine*. Paper presented at the Second Biennial Conference on Innovative Data Systems Research (CIDR'05), Asilomar.
- Abadi, D. J., Carney, D., Cetintemel, U., Cherniack, M., Convey, C., Lee, S., . . . Zdonik, S. (2003). Aurora: a new model and architecture for data stream management. *The VLDB Journal — The International Journal on Very Large Data Bases* 12(2), 120-139.
- ACL. (2006). New Demands, New Priorities - The Evolving Role of Internal Audit. In A. Services (Ed.), *Global Audit Executives Survey Report: ACL Services Ltd*.
- Adams, S. J. (2001). Projecting the next decade in safety management. *computer science*, 3(4).
- Albani, A., & Dietz, J. G. (2006). The Benefit of Enterprise Ontology in Identifying Business Components. In D. Avison, S. Elliot, J. Krogstie & J. Pries-Heje (Eds.), *The Past and Future of Information Systems: 1976–2006 and Beyond* (Vol. 214, pp. 243-254): Springer US.
- Albani, A., & Dietz, J. L. G. (2009). Benefits of Enterprise Ontology for the Development of ICT-Based Value Networks. In J. Filipe, B. Shishkov, M. Helfert & L. A. Maciaszek (Eds.), *Software and Data Technologies* (Vol. 22, pp. 3-22): Springer Berlin Heidelberg.
- Albani, A., & Dietz, J. L. G. (2011). Enterprise ontology based development of information systems. *International Journal of Internet and Enterprise Management*, 7(1), 41-63. doi: 10.1504/ijiem.2011.038382
- Alles, M., Brennan, G., Kogan, A., & Vasarhelyi, M. (2006). Continuous monitoring of business process controls: A pilot implementation of a continuous auditing system at Siemens. *International Journal of Accounting Information Systems*, 7(2), 137-161.
- Alles, M., Kogan, A., & Vasarhelyi, M. (2002). Feasibility and Economics of Continuous Assurance. *Auditing: A Journal of Practice & Theory*, 21(1), 125-138.
- Alles, M., Kogan, A., & Vasarhelyi, M. (2003). Black Box Logging and Tertiary Monitoring of Continuous Assurance Systems. *Information Systems Control Journal* 1, 37-39.

References

- Alles, M., Kogan, A., & Vasarhelyi, M. (2004). Restoring auditor credibility: tertiary monitoring and logging of continuous assurance systems *International Journal of Accounting Information Systems*, 5(2), 183-202.
- Alles, M., Kogan, A., & Vasarhelyi, M. (2008). Putting Continuous Auditing Theory into Practice: Lessons from Two Pilot Implementations. *Journal of Information Systems*, 22(3), 195-214.
- Alles, M., Tostes, F., Vasarhelyi, M., & Riccio, E. L. (2006). Continuous Auditing: The USA Experience and Considerations for its Implementations in Brazil. *Journal of Information Systems and Technology Management*, 3(2), 211-224.
- Arasu, A., Babcock, B., Babu, S., Cieslewicz, J., Datar, M., Ito, K., . . . Widom, J. (2004). STREAM: The Stanford Data Stream Management System. *IEEE Data Engineering Bulletin*, 26(1), 19 -26.
- Aveiro, D. (2010). *G.O.D. (Generation, Operationalization & Discontinuation) and Control (sub)organizations: a DEMO-based approach for continuous real-time management of organizational change caused by exceptions*. Ph.D Thesis, Instituto Superior Técnico, Portugal.
- Babbie, E. (1993). *The practice of social research*. Belmont, CA: Wadsworth Publishing Company.
- Balazinska, M., Balakrishnan, H., & Stonebraker, M. (2004). *Load management and high availability in the Medusa distributed stream processing system*. Paper presented at the ACM SIGMOD international conference on management of data, Paris, France.
- Barbara, G., Melanie, J., David, H., & Anne, W. (2002). Applying the Delphi technique in a study of GPs' information requirements. *Health Soc Care Community*, 7(3), 198-205. doi: 10.1046/j.1365-2524.1999.00176.x
- Barjis, J., Rychkova, I., & Yilmaz, L. (2011). *Modeling and simulation driven software development*. Paper presented at the Proceedings of the 2011 Emerging M&S Applications in Industry and Academia Symposium, Boston, Massachusetts.
- Batista, J. (2012). *O Uso das Tecnologias da Comunicação no Ensino Superior*. PhD Thesis, Universidade de Aveiro e Universidade do Porto, Portugal.
- Bland, J. M., & Altman, D. G. (1997). Statistics notes: Cronbach's alpha. *British Medical Journal*, 314(7080), 572. doi: 10.1136/bmj.314.7080.572

- Bodoni, S. (2014). Kaupthing Creditors, Madoff, A-Tec, Lehman Brothers: Bankruptcy. *Bloomberg News*, Retrieved January 12, 2014, from <http://www.bloomberg.com/news/2010-11-25/kaupthing-creditors-madoff-a-tec-lehman-brothers-bankruptcy.html>
- Brandl, H.-M., & Guschakowski, D. (2007). *Complex Event Processing in the context of Business Activity Monitoring - An evaluation of different approaches and tools taking the example of the Next Generation easyCredit*. Diploma Thesis, University of Applied Sciences Regensburg, Regensburg.
- Brown, C. E., Wong, J. A., & Baldwin, A. A. (2007). A review and analysis of the existing research streams in Continuous Auditing. *Journal of Emerging Technologies in Accounting*, 4(1), 1-28.
- Bunge, M. (1979). *Treatise on Basic Philosophy: Volume 4: Ontology II: A World of Systems*: Springer.
- Caetano, A., Assis, A., & Tribolet, J. (2012, 4-7 Jan. 2012). *Using Business Transactions to Analyse the Consistency of Business Process Models*. Paper presented at the System Science (HICSS), 2012 45th Hawaii International Conference on.
- Caldwell, F., & Proctor, P. E. (2009). Continuous Controls Monitoring for Transactions: The Next Frontier for GRC Automation. In G. Research (Ed.): Gartner, Inc.
- Caldwell, F., & Proctor, P. E. (2010). Magic Quadrant for Continuous Controls Monitoring. In G. Research (Ed.): Gartner, Inc.
- Cantu, I., Liu, L., & Zhou, H. (2008). *Continuous Auditing*. Paper presented at the SWDSI 2008, Houston, Texas.
- Chen, P. P.-S. (1976). The entity-relationship model toward a unified view of data. *ACM Trans. Database Syst.*, 1(1), 9-36. doi: 10.1145/320434.320440
- Clemente, M. (2011). *Contributos do turismo para a qualidade de vida*. Mestrado Master's Thesis, Universidade de Aveiro, Aveiro.
- Coderre, D. (2005). Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment. In T. I. o. I. Auditors (Ed.), *Global Technology Audit Guide*. Florida: The Institute of Internal Auditors.
- Cohen, J. R., Ding, Y., Lesage, C., & Stolowy, H. (2010). Corporate Fraud and Managers' Behavior: Evidence from the Press. *Journal of Business Ethics*, 95(2), 271-315.

References

- Collier, P. M. M., Berry, A., & Burke, G. T. T. (2007). *Risk and Management Accounting - Best practice guidelines for enterprise-wide internal control procedures*. CIMA Publishing
- Coolican, H. (2004). *Research Methods and Statistics in Psychology* (5th ed.). London: Hodder & Stoughton.
- Dalkey, N., & Helmer, O. (1963). An experimental application of the Delphi method to the use of experts. *Management science*, 9(3), 458-467.
- Dayal, U., Hsu, M., & Ladin, R. (1990). Organizing long-running activities with triggers and transactions. *SIGMOD Rec.*, 19(2), 204-214. doi: citeulike-article-id:6593886
- Denning, D. E. (1987). An Intrusion-Detection Model. *IEEE Transactions on Software Engineering*, 13(2), 222-232.
- Dietz, J. L. G. (2003). The atoms, molecules and fibers of organizations. *Data Knowl. Eng.*, 47(3), 301-325. doi: [http://dx.doi.org/10.1016/S0169-023X\(03\)00062-4](http://dx.doi.org/10.1016/S0169-023X(03)00062-4)
- Dietz, J. L. G. (2006a). Enterprise Ontology - Understanding the Essence of Organizational Operation *Enterprise Information Systems VII* (pp. 19-30): Springer Netherlands.
- Dietz, J. L. G. (2006b). *Enterprise Ontology: Theory and Methodology*. New York: Springer-Verlag Inc.
- Dietz, J. L. G., & Habing, N. (2004). The Notion of Business Process Revisited *On the Move to Meaningful Internet Systems 2004: CoopIS, DOA, and ODBASE* (Vol. 3290/2004, pp. 85-100). Heidelberg: Springer Berlin
- Dietz, J. L. G., & Hoogervorst, J. A. P. (2008). *Enterprise ontology in enterprise engineering*. Paper presented at the 2008 ACM symposium on Applied computing, Fortaleza, Ceara, Brazil.
- Ettema, R., & Dietz, J. G. (2009). ArchiMate and DEMO – Mates to Date? In A. Albani, J. Barjis & J. G. Dietz (Eds.), *Advances in Enterprise Engineering III* (Vol. 34, pp. 172-186): Springer Berlin Heidelberg.
- Feitosa, W. M. d. N., & Nascimento, J. V. d. (2003). The professional's specific competencies of physical education that acts in the orientation of physical activities: a study Delphi. *Revista Brasileira de Ciência e Movimento*, 11(4), 19-26.
- Ferreira, D. R., Alves, S., & Thom, L. H. (2011). *Ontology-Based Discovery of Workflow Activity Patterns*. Paper presented at the 2nd International Workshop on Reuse in Business Process Management, Clermont-Ferrand, France.

- Ferreira, D. R., & Gillblad, D. (2009). *Discovering Process Models from Unlabelled Event Logs*. Paper presented at the 7th International Conference on Business Process Management, Ulm, Germany.
- Fish, L. S., & Busby, D. M. (1996). The delphi method. In D. h. Sprenkle & F. P. Piercy (Eds.), *Research methods in family therapy* (2nd edition ed., pp. 469-482). New York: Guilford Press.
- Fisher, I. E. (2003). On the structure of financial accounting standards to support digital representation, storage and retrieval. *Journal of Emerging Technologies in Accounting* 1(1).
- Fonseca, E. (2012). *Paralelo político Portugal/Brasil sobre eficiência energética*. Mestrado Master's Thesis, Universidade de Aveiro, Aveiro.
- Franklin, G. F., Powell, J. D., & Emami-Naeini, A. (1994). *Feedback control of dynamic systems* (Vol. 3): Addison-Wesley Reading.
- Garrod, B., & Fyall, A. (2005). Revisiting Delphi : the Delphi Technique in Tourism Research. *Tourism Research Methods*, 85-98. doi: citeulike-article-id:1443830
- Goossen, W. T. F. (2000). *Towards strategic use of nursing information in the Netherlands*. Dissertation, University of Groningen, Groningen.
- Graham, B., Regehr, G., & Wright, J. G. (2003). Delphi as a method to establish consensus for diagnostic criteria. *Journal of clinical epidemiology*, 56(12), 1150-1156.
- Greiner, T., Duster, W., Pouatcha, F., & Ammon, R. v. (2006). *Business Activity Monitoring of norisbank Taking the Example of the Application easyCredit and the Future Adoption of Complex Event Processing*. Paper presented at the IEEE Services Computing Workshops Chicago.
- Grilo, R. M. M. (2008). *Investigação em Sistemas de Informação Organizacionais em Portugal*. Master Dissertation, Universidade de Trás-Os-Montes e Alto Douro, Vila Real.
- Gruber, T. R. (1995). Toward principles for the design of ontologies used for knowledge sharing. *Int. J. Hum.-Comput. Stud.*, 43(5-6), 907-928. doi: 10.1006/ijhc.1995.1081
- Guerreiro, S. (2012). *Enterprise Dynamic Systems Control enforcement of run-time business transactions using DEMO: principles of design and implementation*. Ph.D Thesis, Instituto Superior Técnico, Portugal.

References

- Gupta, U. G., & Clarke, R. E. (1996). Theory and applications of the Delphi technique: A bibliography (1975–1994). *Technological Forecasting and Social Change*, 53(2), 185-211. doi: [http://dx.doi.org/10.1016/S0040-1625\(96\)00094-7](http://dx.doi.org/10.1016/S0040-1625(96)00094-7)
- Halpin, T. (2001). *Information modeling and relational databases: from conceptual analysis to logical design*. San Francisco: Morgan Kaufmann Publishers Inc.
- Hargadon, A., & Fanelli, A. (2002). Action and possibility: Reconciling dual perspectives of knowledge in organizations. *Organization Science*, 13(3), 290-302.
- Hasson, F., Keeney, S., & McKenna, H. (2000). Research guidelines for the Delphi survey technique. *Journal of Advanced Nursing*, 32(4), 1008-1015.
- Helmer, O. (1967). *Convergence of Expert Consensus Through Feedback*. Los Angeles CA: Rand Corporation.
- Hevner, A., & Chatterjee, S. (2010). Design Science Research in Information Systems *Design Research in Information Systems* (Vol. 22, pp. 9-22): Springer US.
- Hevner, A. R. (2007). The three cycle view of design science research. *Scandinavian Journal of Information Systems*, 19(2), 87-92.
- Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS quarterly*, 28(1), 75-105.
- IFAC. (2004). Auditing and Assurance. In IFAC (Ed.), *Handbook of International Auditing, Assurance and Ethics Pronouncements* (Vol. 1). New York: International Federation of Accountants.
- Institute, E. E. (2011). DEMO - Design & Engineering Methodology for Organizations, 2011, from <http://www.demo.nl/>
- Joonsoo, B., Hyerim, B., Suk-Ho, K., & Yeongho, K. (2004). Automatic control of workflow processes using ECA rules. *Knowledge and Data Engineering, IEEE Transactions on*, 16(8), 1010-1023.
- Kaynak, E., Bloom, J., & Leibold, M. (1994). Using the Delphi Technique to Predict Future Tourism Potential. *Marketing Intelligence & Planning*, 12(7), 18-29.
- Keeney, S., Hasson, F., & McKenna, H. P. (2001). A critical review of the Delphi technique as a research methodology for nursing. *International Journal of Nursing Studies*, 38(2), 195-200. doi: [http://dx.doi.org/10.1016/S0020-7489\(00\)00044-4](http://dx.doi.org/10.1016/S0020-7489(00)00044-4)
- Kendall, M. G., & Smith, B. B. (1939). The problem of m rankings. *The annals of mathematical statistics*, 10(3), 275-287.

- Kuhn, J. R., & Sutton, S. G. (2006). Learning from WorldCom: Implications for Fraud Detection through Continuous Assurance. *Journal of Emerging Technologies in Accounting*, 3(1), 61-80.
- Landeta, J. (2006). Current validity of the Delphi method in social sciences. *Technological Forecasting and Social Change*, 73(5), 467-482.
- Langefors, B. (1977). Information systems theory. [doi: DOI: 10.1016/0306-4379(77)90009-6]. *Information Systems*, 2(4), 207-219.
- Lankhorst, M. (2013). *Enterprise architecture at work: Modelling, communication and analysis*. Heidelberg: Springer.
- Li-Ling Hsu, R. S. Q. L., Yu-Te Weng (2008). Understanding the critical factors effect user satisfaction and impact of ERP through innovation of diffusion theory *International Journal of Technology Management* 2008 43(1-3), 30-47.
- Linstone, H. A., & Turoff, M. (1975). *The Delphi Method - Techniques and Applications*. London: Addison-Wesley Publishing Company.
- Littley, K., Minnaar, D., farineau, D., Soles, R., Nardin, D., LoPiccolo, D. D., . . . Kaldrovics, H. (2010). *What is driving Continuous Auditing & Continuous Monitoring Today?* USA: KPMG.
- Markham, J. W. (2006). *Financial history of modern United States corporate scandals* (Vol. 1). New York: M.E. Sharpe
- Marques, R. P., Santos, C., & Santos, H. (2010). Automation of the Approval and Control Process of Documents. In J. E. Quintela Varajão, M. M. Cruz-Cunha, G. D. Putnik & A. Trigo (Eds.), *ENTERprise Information Systems* (Vol. 109, pp. 328-337): Springer Berlin Heidelberg.
- Marques, R. P., Santos, H., & Santos, C. (2012a). Automation of the Approval and Control Process of Documents. In J. Varajão, M. M. Cruz-Cunha & A. Trigo (Eds.), *Organizational Integration of Enterprise Systems and Resources: Advancements and Applications* (pp. 312-326): IGI Global.
- Marques, R. P., Santos, H., & Santos, C. (2012b). *Continuous Assurance on Organizational Transactions*. Paper presented at the 2012 IEEE/ACIS 11th International Conference on Computer and Information Science, Shangai, China.
- Marques, R. P., Santos, H., & Santos, C. (2012c). A solution for real time monitoring and auditing of organizational transactions. *Procedia Technology*, 5(1), 190-198. doi: <http://dx.doi.org/10.1016/j.protcy.2012.09.021>

References

- Marques, R. P., Santos, H., & Santos, C. (2013a). A Conceptual Model for Evaluating Systems with Continuous Assurance Services. *Procedia Technology*, 9, 304-309. doi: <http://dx.doi.org/10.1016/j.protcy.2013.12.034>
- Marques, R. P., Santos, H., & Santos, C. (2013b). *An Enterprise Ontology-Based Database for Continuous Monitoring Application*. Paper presented at the IEEE 15th Conference on Business Informatics (CBI), Vienna, Austria.
- Marques, R. P., Santos, H., & Santos, C. (2014, 18-21 June 2014). *Management of internal control mechanisms in ERP for continuous monitoring purposes*. Paper presented at the 2014 9th Iberian Conference on Information Systems and Technologies (CISTI).
- Marques, R. P., Santos, H., & Santos, C. (in press). Evaluating Information Systems with Continuous Assurance Services. *International Journal of Information Systems in the Service Sector*.
- Marques, R. P., Santos, H. M. D., & Santos, C. (2013c). Organizational transactions with real time monitoring and auditing. *The Learning Organization*, 20(6), 390-405.
- Mauch, J. E., & Park, N. (2003). *Guide to the Successful Thesis and Dissertation - A Handbook for Students and Faculty*. New York: Marcel Dekker Inc.
- McCoy, D. W. (2002). *Business activity monitoring: Calm before the storm*. Stamford: Gartner Inc.
- Miller, G. (2001). The development of indicators for sustainable tourism: results of a Delphi survey of tourism researchers. *Tourism Management*, 22(4), 351 - 362.
- Minnaar, D., Little, J., & Farineau, D. (2008). Continuous Auditing and Continuous Monitoring: Transforming Internal Audit and Management Monitoring to Create Value. In K. LLP (Ed.). New York: KPMG LLP.
- Möller, M. O. (2002). *Structure and Hierarchy in Real-Time Systems*. PhD Thesis PhD Thesis, University of Aarhus, Aarhus.
- Morais, M. G. C. T. (2008). *A importância da auditoria interna para a gestão: caso das empresas portuguesas*. Paper presented at the 18º Congresso Brasileiro de Contabilidade Gramado, Brazil.
- Murcia, F. D.-R., Souza, F. C. d., & Borba, J. A. (2008). Continuous Auditing: A Literature Review. *Organizações em contexto*, 4(7), 1-17.
- Murphy, M., Sanderson, C., Black, N., Askham, J., Lamping, D., Marteau, T., & McKee, C. (1998). Consensus development methods, and their use in clinical guideline development. *Health Technol Assessment*, 2(3).

- Musaji, Y. F. (2002). *Integrated Auditing of ERP Systems* (Vol. 1). New York: John Wiley & Sons, Inc.
- Myers, M. D. (1997a). Qualitative Research in Information Systems Retrieved March 1, 2011, 2011, from <http://www.qual.auckland.ac.nz/>
- Myers, M. D. (1997b). Qualitative Research in Information Systems Retrieved 01-03-2011
- Nogueira, M. A. A., Azeredo, Z. A., & Santos, A. S. (2012). Competências do cuidador informal atribuídas pelos enfermeiros comunitários: um estudo Delphi. *Revista Eletrónica de Enfermagem*, 14(4), 749-759.
- O'Neill, S., Scott, M., & Conboy, K. (2010). A Delphi study on collaborative learning in distance education: The faculty perspective. *British Journal of Educational Technology*, 42(6), 939-949.
- Okoli, C., & Pawlowski, S. D. (2004). The Delphi method as a research tool: an example, design considerations and applications. *Information & Management*, 42(1), 15-29. doi: <http://dx.doi.org/10.1016/j.im.2003.11.002>
- Oliveira, J. J. R. d. (2011). *Descoberta de Processos em Tempo Real*. Master Degree Master Dissertation, Univesidade Técnica de Lisboa, Lisboa.
- Op't Land, M., & Dietz, J. G. (2012). Benefits of Enterprise Ontology in Governing Complex Enterprise Transformations. In A. Albani, D. Aveiro & J. Barjis (Eds.), *Advances in Enterprise Engineering VI* (Vol. 110, pp. 77-92): Springer Berlin Heidelberg.
- Oringel, J. (2010). *A Framework for Continuous Auditing and Continuous Controls Monitoring*. Paper presented at the 19th annual World Continuous Audit and Reporting Symposium New Jersey.
- Patton, M. Q. (2002). *Qualitative Evaluation and Research Methods* (3 ed.). Thousand Oaks: Sage Publications Inc.
- Peppers, K., Tuunanen, T., Gengler, C. E., Rossi, M., Hui, W., Virtanen, V., & Bragge, J. (2006). *The design science research process: a model for producing and presenting information systems research*. Paper presented at the Proceedings of the first international conference on design science research in information systems and technology (DESRIST 2006).
- Pereira, C. S. M. (2008). *Contributo para a implementação da classificação internacional de funcionalidade para a identificação de ganhos em saúde nas doenças crónicas*. Mestrado em Gestão dos Serviços de Saúde Master's Thesis, Universidade Nova de Lisboa, Lisbon.

References

- Powell, C. (2003). The Delphi technique: myths and realities. *Journal of Advanced Nursing*, 41(4), 376-382.
- PricewaterhouseCoopers. (2006). *State of the internal audit profession study: Continuous auditing gains momentum*: PricewaterhouseCoopers LLP.
- PricewaterhouseCoopers. (2007). *Internal Audit 2012*. New York: PricewaterhouseCoopers LLP.
- Primavera, B. (2013). Primavera Corporate BSS Retrieved 30 January 2013, 2013, from <http://www.primaverabss.com/>
- Quivy, R., & Campenhoudt, L. V. (1998). *Manual de Investigação em Ciências Sociais*. Lisbon: Gradiva.
- Randall, R. C., Vrijhoef, M. M. A., & Wilson, N. H. F. (2002). Current trends in restorative dentistry in the UK: a Delphi approach. *Journal of Dentistry*, 30(4), 177-187. doi: [http://dx.doi.org/10.1016/S0300-5712\(02\)00008-8](http://dx.doi.org/10.1016/S0300-5712(02)00008-8)
- Rayens, M. K., & Hahn, E. J. (2000). Building Consensus Using the Policy Delphi Method. *Policy, Politics, & Nursing Practice*, 1(4), 308-315.
- Ribeiro, M. I. (2002). *Análise de Sistemas Lineares*: IST Press.
- Rizvi, S. (2005). *Complex Event Processing Beyond Active Databases: Streams and Uncertainties*. Master Dissertation, University of California, Berkeley. (UCB/EECS-2005-26)
- Roth, H., Schiefer, J., Obweger, H., & Rozsnyai, S. (2010, 19-21 May 2010). *Event data warehousing for Complex Event Processing*. Paper presented at the Research Challenges in Information Science (RCIS), 2010 Fourth International Conference on.
- Rowe, G., & Wright, G. (1999). The Delphi technique as a forecasting tool: issues and analysis. *International Journal of Forecasting*, 15(4), 353-375. doi: [http://dx.doi.org/10.1016/S0169-2070\(99\)00018-7](http://dx.doi.org/10.1016/S0169-2070(99)00018-7)
- Sandford, B. A., & Hsu, C.-C. (2007). The Delphi Technique: Making Sense Of Consensus. *Practical Assessment, Research & Evaluation*, 12(4).
- Sant'Ana, P. (2005). *Análise prospectiva de tecnologias de energia: validação e análises de uma consulta Delphi com especialistas do Brasil*. Master's Thesis, Universidade Estadual de Campinas, Campinas.
- Santos, C. (2009). *Modelo Conceptual para Auditoria Organizacional Contínua com Análise em Tempo Real* (1 ed.). Penafiel: Editorial Novembro.

- Santos, L. D. d., & Amaral, L. (2004). *Estudos Delphi com Q-Sort sobre a web: a sua utilização em sistemas de informação*. Paper presented at the Conferência da Associação Portuguesa de Sistemas de Informação, Lisbon.
- Silva, F. (2009). *As Tecnologias da Informação e Comunicação e o Ensino da Contabilidade*. Master Dissertation, University of Aveiro, Portugal, Aveiro.
- Silva, L., & Machado, S. (2008). *Um Estudo Sobre os Impactos da Lei Sarbanes-Oxley na Área de Auditoria Interna de uma Empresa Brasileira com Ações Negociadas nos Estados Unidos* Paper presented at the 18º Congresso Brasileiro de Contabilidade, Gramado, Rio Grande do Sul, Brazil.
- Singleton, T., & Singleton, A. J. (2005). Auditing headaches? Relieve them with CAR. *Journal of Corporate Accounting & Finance*, 16(4), 17-27. doi: 10.1002/jcaf.20114
- Skulmoski, G. J., Hartman, F. T., & Krahn, J. (2007). The Delphi method for graduate research. *Journal of information technology education*, 6, 1.
- Soltani, B. (2007). An Introduction to Auditing and Assurance *Auditing: An International Approach* (Vol. 1, pp. 1-26): FT Prentice Hall
- Sousa, P. A. F. d., MHLBC, F., & Mendonça, D. (2005). Um modelo de organização e partilha de informação de enfermagem entre hospital e centro de saúde: estudo delphi. *Acta Paul Enferm*, 18(4), 368-381.
- SOX. (2002). The Sarbanes-Oxley Act Retrieved September 2013, 2013, from <http://www.soxlaw.com/>
- Stevens, B., McGrath, P., Yamada, J., Gibbins, S., Beyene, J., Breau, L., . . . Ohlsson, A. (2006). Identification of pain indicators for infants at risk for neurological impairment: A Delphi consensus study. *BMC Pediatrics*, 6(1), 1-9. doi: 10.1186/1471-2431-6-1
- Tavakol, M., & Dennick, R. (2011). Making sense of Cronbach's alpha. *International Journal of Medical Education*, 2, 53-55.
- ter Hofstede, A., van der Aalst, W., & Weske, M. (2003). Business Process Management: A Survey
Business Process Management. In M. Weske (Ed.), (Vol. 2678, pp. 1019-1019): Springer Berlin / Heidelberg.
- Toscano, R. (2009). *Alignment in Real Time on Corporate Governance, Business Processes and Information Systems*. Master Dissertation, Universidade Técnica de Lisboa, Lisbon.

References

- Van der Horst, P. (2010). *From business transactions to business processes work flows: Using DEMO and BPMN*. Master's thesis, Delft University of Technology.
- Van Kervel, S. J. H. (2012). *Ontology driven Enterprise Information Systems Engineering*. Ph.D Thesis, Delft University of Technology, Netherlands.
- Vasarhelyi, M. (2002). Concepts in Continuous Assurance In V. Arnold & S. G. Sutton (Eds.), *Researching accounting as an information systems discipline* Sarasota, Florida: American Accounting Association, Information Accounting Section.
- Vasarhelyi, M., Alles, M., & Kogan, A. (2004). Principles of Analytic Monitoring for Continuous Assurance. *Journal of Emerging Technologies in Accounting*, 1, 1-21.
- Vasarhelyi, M., Alles, M., & Williams, K. T. (2010). *Continuous Assurance for the Now Economy* (1st ed.). Sydney: Institute of Chartered Accountants in Australia.
- Vasarhelyi, M. A., Alles, M., & Williams, K. T. (2010). *Continuous assurance for the now economy* (1st ed.). Sydney: Institute of Chartered Accountants in Australia.
- Verver, J. (2003). Risk Management and Continuous Monitoring Retrieved March 1, 2011, 2011, from <http://www.acl.com/pdfs/0303-Auditnet.pdf>
- Verver, J. (2008). Continuous Monitoring and Auditing: What is the difference? Retrieved May 20, 2011, from <http://www.protiviti.com/en-US/Insights/Browse-by-Content/Featured-Articles/Pages/Continuous-Monitoring-and-Auditing.aspx>
- Weigand, H., & Moor, A. d. (2003). Workflow analysis with communication norms. *Data & Knowledge Engineering*, 47(3), 349–369.
- Wheeller, B., Hart, T., & Whysall, P. (1990). Application of the Delphi technique: A reply to Green, Hunter and Moore. *Tourism Management*, 11(2), 121-122. doi: [http://dx.doi.org/10.1016/0261-5177\(90\)90027-7](http://dx.doi.org/10.1016/0261-5177(90)90027-7)
- Wiederkehr, P. (2007). From Active Databases to Complex Event Processing. In A. T. i. I. Systems (Ed.), *Event Stream Processing Seminar*. Zurich: Swiss Federal Institute of Technology Zurich
- Worrell, J. L., Di Gangi, P. M., & Bush, A. A. (2012). Exploring the use of the Delphi method in accounting information systems research. *International Journal of Accounting Information Systems*.
- Yousuf, M. I. (2007). Using experts' opinions through Delphi technique. *Practical Assessment, Research & Evaluation*, 12(4), 1-8.

- Zimmer, D., & Unland, R. (23-26 Mar 1999). *On the semantics of complex events in active database management systems*. Paper presented at the 15th International Conference on Data Engineering.
- Zolingen, S. J. v., & Klaassen, C. A. (2003). Selection processes in a Delphi study about key qualifications in Senior Secondary Vocational Education. *Technological Forecasting and Social Change*, 70(4), 317-340. doi: [http://dx.doi.org/10.1016/S0040-1625\(02\)00202-0](http://dx.doi.org/10.1016/S0040-1625(02)00202-0)
- Zwick, M., Lettner, C., & Hawel, C. (2007). Implementing Automated Analyses in an Active Data Warehouse Environment Using Workflow Technology (pp. 341-354).

APPENDIXES

This chapter includes the appendixes which support some other chapters of the thesis with detailed data. This appendixes are:

- Appendix A – Questionnaires of the Delphi method;
- Appendix B – Pre-test to the questionnaires of the Delphi method;
- Appendix C – E-mails which were used to interact with the members of the panel of experts of the Delphi method;
- Appendix D – Results of the questionnaires of the Delphi method.

Furthermore, this thesis includes a support CD which contains other appendixes that are not viable to include in this document by their nature and extension. These appendixes are:

- Appendix I – The source code of the prototype;
- Appendix II – The database scripts of creation and instantiation of the prototype databases;
- Appendix III – A report of the prototype;
- Appendix IV - The support file with the analysed data;
- Appendix V – Other aggregates about the analysed data;
- Appendix VI – Detailed answers of the questionnaires of the Delphi method.

APPENDIX A – QUESTIONNAIRES


This appendix supports chapter 3 of this thesis and presents the questionnaires which were used in the application of the Delphi method to validate the model for evaluation of information systems with continuous assurance services. It is structured in three parts:

A1. Questionnaire before pre-test

A2. Questionnaire of first iteration of Delphi method

A3. Questionnaire of second iteration of Delphi method

A1. Questionnaire before pre-test



Questionnaire on Continuous Assurance Services in Information Systems

This questionnaire is part of a study which is being carried out under the Doctoral Program in Computer Science MAP-i, taught jointly by the Universities of Minho, Aveiro and Porto. The questionnaire is limited to a set of previously selected experts.

The objective of this study is to validate a model for implementation of Continuous Assurance services in information systems.

The questionnaire is divided into two parts: in the first one you should indicate your agreement to the given statements, and in the second you should assign a degree of importance to a set of metrics.


All questions of this questionnaire are mandatory and the estimated time to complete it is 10 minutes.

Your participation in the questionnaire is completely anonymous and confidential, and the results will only be presented in aggregate form.

Your collaboration will be of utmost importance for the success of this study.

Any questions may be sent to ruimarques@ua.pt

Thank you.



Universidade de Minho Universidade de Aveiro U.PORTO M A P i DOCTORAL PROGRAMME IN COMPUTER SCIENCE CENTRALGORITHM

Characterization of Expert

1. Area of expertise:
Note: if you are expert in more than one area, please choose the one you have more years of experience in.

Auditing

Management

Management Information Systems

Other Please indicate which:

2. Years of experience in your area of expertise:

<2 years

≥2 e <10 years

≥10 years

3. Scientific publications on your area of expertise

Yes

No



Part I

Consider that an information system with continuous service assurance means, in a brief way, a system which continuously controls, monitors and audits organizational transactions.

1 - strongly disagree; 2 – disagree; 3 - neither agree nor disagree; 4 – agree; 5 – strongly agree

| 1. Regarding a model for implementing continuous assurance services in information systems, the inclusion of dimensions is essential for evaluating: | | 1 | 2 | 3 | 4 | 5 |
|--|---|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|
| 1.1 | Dimension "monitoring" - the ability of the system to monitor transactions which are intended to be audited. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 1.2 | Dimension "compliance" – the ability of the system to verify conformity and integrity with which transactions are executed. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 1.3 | Dimension "estimation" – the ability of the system to estimate assurance, coherence and consistency of transactions which are being executed. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 2. Dimension "monitoring" may include the following metrics to evaluate the system: (Note: for real-time refers to a minimum period in which it is necessary or useful to have information) | | | | | | |
| 2.1 | Real-time monitoring of operations. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 2.2 | Real-time identification of irregular operations. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 2.3 | Verification of the processing of required operations at all previous steps. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 2.4 | Detection of lack of operations. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 3. Dimension "compliance" may include the following metrics to evaluate the system: | | | | | | |
| 3.1 | Recognition of execution patterns. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 3.2 | Ascertaining of fulfilling of rules. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 3.3 | Detection of potential errors. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 3.4 | Verification of compliance of existing policies. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 4. Dimension "estimation" may include the following metrics to evaluate the system: | | | | | | |
| 4.1 | Estimation of possible risks. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 4.2 | Determination of possible execution patterns. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 5. Regarding a model for implementing continuous assurance services in information systems, the inclusion of the requirement "reporting" is essential so that the results of "monitoring", "compliance" and "estimation" functions can be presented and reported to the users of the system. | | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 6. The requirement "reporting" may include the following specificities: | | | | | | |
| 6.1 | Real-time presentation of the executed operations which were monitored. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 6.2 | Real-time presentation of execution patterns which are being followed or are likely to be followed. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 6.3 | Presentation of the compliance verification in transactions executions. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 6.4 | Real-time presentation of the risk estimated on determining possible execution patterns. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 6.5 | Real-time alert for irregular situations in monitoring, compliance verification and estimation of negative results. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |



Part II

This part of the questionnaire intends to compare and rank the relevance of the identified metrics in the dimension in which they are inserted. Thus, you should indicate the degree of importance ascribed to each of them.

Note: you may indicate the same degree of importance to more than one metric in each dimension.






1 - unimportant; 2 – of little importance; 3 – moderately important; 4 – important; 5 – very important

| 7. Degree of importance of the metrics of dimension "monitoring": | | 1 | 2 | 3 | 4 | 5 |
|--|---|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|
| 7.1 | Real-time monitoring of operations. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 7.2 | Real-time identification of irregular operations. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 7.3 | Verification of the processing of required operations at all previous steps. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 7.4 | Detection of lack of operations. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 8. Degree of importance of the metrics of dimension "compliance": | | | | | | |
| 8.1 | Recognition of execution patterns. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 8.2 | Ascertaining of fulfilling of rules. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 8.3 | Detection of potential errors. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 8.5 | Verification of compliance of existing policies. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 9. Degree of importance of the metrics of dimension "estimation": | | | | | | |
| 9.1 | Estimation of possible risks. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 9.2 | Determination of possible execution patterns. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 10. Degree of importance of the specificities of the requirement "report": | | | | | | |
| 10.1 | Real-time presentation of the executed operations which were monitored. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 10.2 | Real-time presentation of execution patterns which are being followed or are likely to be followed. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 10.3 | Presentation of the compliance verification in transactions executions. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 10.4 | Real-time presentation of the risk estimated on determining possible execution patterns. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 10.5 | Real-time alert for irregular situations in monitoring, compliance verification and estimation of negative results. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

Thank you for your participation.

Any questions may be sent to ruimarques@ua.pt

Questionnaire of first iteration of Delphi method

Questionnaire on Continuous Assurance Services in Information Systems

This questionnaire is part of a study which is being carried out under the Doctoral Program in Computer Science MAP-i, taught jointly by the Universities of Minho, Aveiro and Porto. The questionnaire is limited to a set of previously selected experts.

The objective of this study is to validate a model for implementation of Continuous Assurance services in information systems.

The questionnaire is divided into two parts: in the first one you should indicate your agreement to the given statements, and in the second you should assign a degree of importance to a set of metrics.


All questions of this questionnaire are mandatory and the estimated time to complete it is 10 minutes.

Your participation in the questionnaire is completely anonymous and confidential, and the results will only be presented in aggregate form.

Your collaboration will be of utmost importance for the success of this study.

Any questions may be sent to ruimarques@ua.pt

Thank you.



Universidade de Minho

universidade de aveiro

U.PORTO

M A P i DOCTORAL PROGRAMME IN COMPUTER SCIENCE

CENTRALALGORITMI

Questionnaire on Continuous Assurance Services in Information Systems

0% 100%

Characterization of Expert

*** 1. Area of expertise:**
Note: If you are expert in more than one area, please choose the one you have more years of experience in.
Choose one of the following answers

- Auditing
- Management
- Management Information Systems
- Other. Please indicate which:


*** 2. Years of experience in your area of expertise:**
Choose one of the following answers

- < 2 years
- >= 2 and <10 years
- >= 10 years

*** 3. Scientific publications on your area of expertise**

- Yes
- No

eLearning
universidade de aveiro



Questionnaire on Continuous Assurance Services in Information Systems

0% 100%

Part I

Consider that an information system with continuous assurance services means, in a brief way, a system which continuously controls, monitors and audits organizational transactions.

*** 1. Regarding a model for implementing continuous assurance services in information systems, the inclusion of dimensions is essential for evaluating:**

| | Strongly disagree | Disagree | Neither agree nor disagree | Agree | Strongly agree |
|--|-----------------------|-----------------------|----------------------------|-----------------------|-----------------------|
| The ability of the system to monitor transactions which are intended to be audited (Dimension "monitoring") | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| The ability of the system to verify conformity and integrity with which transactions are executed (Dimension "compliance") | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| The ability of the system to estimate assurance, coherence and consistency of transactions which are being executed (Dimension "estimation") | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

*** 2. Dimension "monitoring" may include the following metrics to evaluate the system:**
(Note: for real-time refers to a minimum period in which it is necessary or useful to have information)

| | Strongly disagree | Disagree | Neither agree nor disagree | Agree | Strongly agree |
|---|-----------------------|-----------------------|----------------------------|-----------------------|-----------------------|
| Real-time monitoring of operations. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Real-time identification of irregular operations (e.g. poorly executed operations, incongruities, etc). | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Real-time verification of the processing of required operations at all previous steps. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Real-time detection of lack of operations. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

*** 3. Dimension "compliance" may include the following metrics to evaluate the system:**

| | Strongly disagree | Disagree | Neither agree nor disagree | Agree | Strongly agree |
|--|-----------------------|-----------------------|----------------------------|-----------------------|-----------------------|
| Recognition of execution patterns. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Ascertaining of fulfilling of rules. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Detection of potential errors. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Verification of compliance of existing policies. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

*** 4. Dimension "estimation" may include the following metrics to evaluate the system:**


| | Strongly disagree | Disagree | Neither agree nor disagree | Agree | Strongly agree |
|---|-----------------------|-----------------------|----------------------------|-----------------------|-----------------------|
| Estimation of possible risks. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Determination of possible execution patterns which are likely to be followed. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |


*** 5. Regarding a model for implementing continuous assurance services in information systems**

| | Strongly disagree | Disagree | Neither agree nor disagree | Agree | Strongly agree |
|--|-----------------------|-----------------------|----------------------------|-----------------------|-----------------------|
| The inclusion of the requirement "reporting" is essential. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |


* 6. The requirement "reporting" may include the following specificities:

| | Strongly disagree | Disagree | Neither agree nor disagree | Agree | Strongly agree |
|---|-----------------------|-----------------------|----------------------------|-----------------------|-----------------------|
| Real-time presentation of the executed operations which were monitored. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Real-time presentation of execution patterns which are being followed or are likely to be followed. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Real-time presentation of the compliance verification in transactions executions. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Real-time presentation of the risk estimated on determining possible execution patterns. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Real-time alert for irregular situations in monitoring, compliance verification and estimation of negative results. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |





Questionnaire on Continuous Assurance Services in Information Systems



Part II

This part of the questionnaire intends to compare and rank the relevance of the identified metrics in the dimension in which they are inserted. Thus, you should indicate the degree of importance ascribed to each of them.

Note: you may indicate the same degree of importance to more than one metric in each dimension.

*** 7. Degree of importance of the metrics of dimension "monitoring":**

| | Unimportant | Of little importance | Moderately important | Important | Very important |
|--|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|
| Real-time monitoring of operations. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Real-time identification of irregular operations. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Real-time verification of the processing of required operations at all previous steps. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Real-time detection of lack of operations. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

*** 8. Degree of importance of the metrics of dimension "compliance":**

| | Unimportant | Of little importance | Moderately important | Important | Very important |
|--|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|
| Recognition of execution patterns. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Ascertaining of fulfilling of rules. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Detection of potential errors. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Verification of compliance of existing policies. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

*** 9. Degree of importance of the metrics of dimension "estimation":**


| | Unimportant | Of little importance | Moderately important | Important | Very important |
|---|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|
| Estimation of possible risks. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Determination of possible execution patterns which are likely to be followed. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

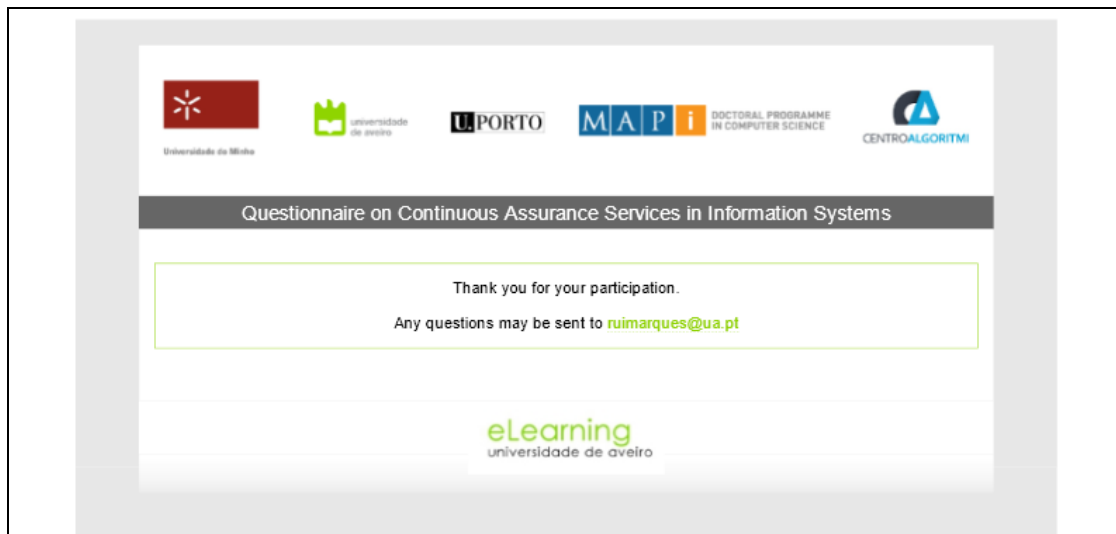
*** 10. Degree of importance of the specificities of the requirement "report":**

| | Unimportant | Of little importance | Moderately important | Important | Very important |
|---|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|
| Real-time presentation of the executed operations which were monitored. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Real-time presentation of execution patterns which are being followed or are likely to be followed. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Real-time presentation of the compliance verification in transactions executions. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Real-time presentation of the risk estimated on determining possible execution patterns. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Real-time alert for irregular situations in monitoring, compliance verification and estimation of negative results. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

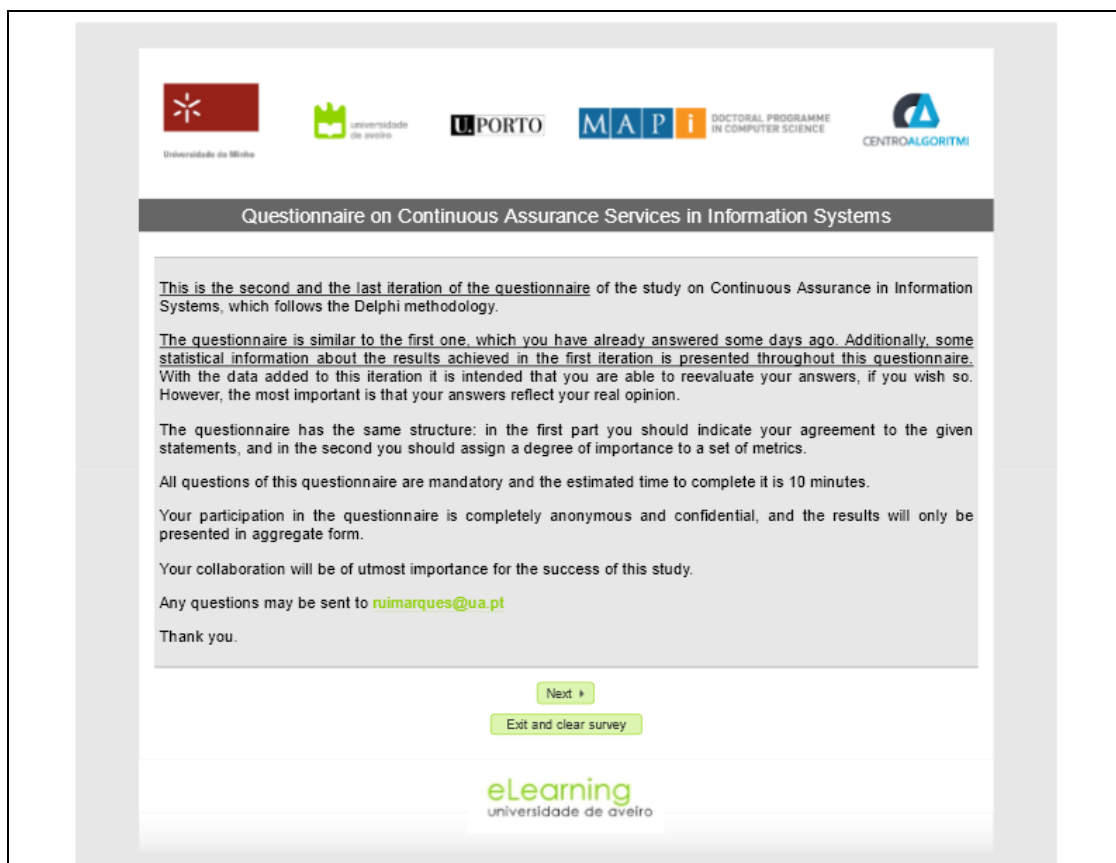
◀ Previous
Submit

Exit and clear survey





A3. Questionnaire of second iteration of Delphi method



Universidade de Minho

Universidade de Aveiro

U.PORTO

M.A.P.I. DOCTORAL PROGRAMME IN COMPUTER SCIENCE

CENTROALGORITMI

Questionnaire on Continuous Assurance Services in Information Systems

0% 100%

Characterization of Expert

*** 1. Area of expertise:**
Note: If you are expert in more than one area, please choose the one you have more years of experience in.
Choose one of the following answers

- Auditing
- Management
- Management Information Systems
- Other. Please indicate which:

*** 2. Years of experience in your area of expertise:**
Choose one of the following answers

- < 2 years
- >= 2 and <10 years
- >= 10 years


*** 3. Scientific publications on your area of expertise**

- Yes
- No


← Previous Next →

Exit and clear survey

eLearning
universidade de aveiro



Questionnaire on Continuous Assurance Services in Information Systems



Part I

Note: Immediately next to each answer option, you will find a value that corresponds to the percentage of responses obtained for that answer option in the first iteration of this questionnaire.

Consider that an information system with continuous assurance services means, in a brief way, a system which continuously controls, monitors and audits organizational transactions.

*** 1. Regarding a model for implementing continuous assurance services in information systems, the inclusion of dimensions is essential for evaluating:**

| | Strongly disagree | Disagree | Neither agree nor disagree | Agree | Strongly agree |
|--|--------------------------|--------------------------|----------------------------|---------------------------|---------------------------|
| The ability of the system to monitor transactions which are intended to be audited (Dimension "monitoring") | <input type="radio"/> 0% | <input type="radio"/> 0% | <input type="radio"/> 0% | <input type="radio"/> 10% | <input type="radio"/> 90% |
| The ability of the system to verify conformity and integrity with which transactions are executed (Dimension "compliance") | <input type="radio"/> 0% | <input type="radio"/> 0% | <input type="radio"/> 0% | <input type="radio"/> 20% | <input type="radio"/> 80% |
| The ability of the system to estimate assurance, coherence and consistency of transactions which are being executed (Dimension "estimation") | <input type="radio"/> 0% | <input type="radio"/> 0% | <input type="radio"/> 0% | <input type="radio"/> 50% | <input type="radio"/> 50% |

*** 2. Dimension "monitoring" may include the following metrics to evaluate the system:**
(Note: for real-time refers to a minimum period in which it is necessary or useful to have information)

| | Strongly disagree | Disagree | Neither agree nor disagree | Agree | Strongly agree |
|---|--------------------------|--------------------------|----------------------------|---------------------------|----------------------------|
| Real-time monitoring of operations. | <input type="radio"/> 0% | <input type="radio"/> 0% | <input type="radio"/> 0% | <input type="radio"/> 20% | <input type="radio"/> 80% |
| Real-time identification of irregular operations (e.g. poorly executed operations, incongruities, etc). | <input type="radio"/> 0% | <input type="radio"/> 0% | <input type="radio"/> 0% | <input type="radio"/> 0% | <input type="radio"/> 100% |
| Real-time verification of the processing of required operations at all previous steps. | <input type="radio"/> 0% | <input type="radio"/> 0% | <input type="radio"/> 0% | <input type="radio"/> 40% | <input type="radio"/> 60% |
| Real-time detection of lack of operations. | <input type="radio"/> 0% | <input type="radio"/> 0% | <input type="radio"/> 0% | <input type="radio"/> 20% | <input type="radio"/> 80% |

*** 3. Dimension "compliance" may include the following metrics to evaluate the system:**

| | Strongly disagree | Disagree | Neither agree nor disagree | Agree | Strongly agree |
|--|--------------------------|--------------------------|----------------------------|---------------------------|---------------------------|
| Recognition of execution patterns. | <input type="radio"/> 0% | <input type="radio"/> 0% | <input type="radio"/> 0% | <input type="radio"/> 40% | <input type="radio"/> 60% |
| Ascertaining of fulfilling of rules. | <input type="radio"/> 0% | <input type="radio"/> 0% | <input type="radio"/> 0% | <input type="radio"/> 50% | <input type="radio"/> 50% |
| Detection of potential errors. | <input type="radio"/> 0% | <input type="radio"/> 0% | <input type="radio"/> 0% | <input type="radio"/> 10% | <input type="radio"/> 90% |
| Verification of compliance of existing policies. | <input type="radio"/> 0% | <input type="radio"/> 0% | <input type="radio"/> 0% | <input type="radio"/> 50% | <input type="radio"/> 50% |

*** 4. Dimension "estimation" may include the following metrics to evaluate the system:**


| | Strongly disagree | Disagree | Neither agree nor disagree | Agree | Strongly agree |
|---|--------------------------|--------------------------|----------------------------|---------------------------|---------------------------|
| Estimation of possible risks. | <input type="radio"/> 0% | <input type="radio"/> 0% | <input type="radio"/> 0% | <input type="radio"/> 40% | <input type="radio"/> 60% |
| Determination of possible execution patterns which are likely to be followed. | <input type="radio"/> 0% | <input type="radio"/> 0% | <input type="radio"/> 0% | <input type="radio"/> 30% | <input type="radio"/> 70% |


*** 5. Regarding a model for implementing continuous assurance services in information systems**

| | Strongly disagree | Disagree | Neither agree nor disagree | Agree | Strongly agree |
|--|--------------------------|--------------------------|----------------------------|---------------------------|---------------------------|
| The inclusion of the requirement "reporting" is essential. | <input type="radio"/> 0% | <input type="radio"/> 0% | <input type="radio"/> 0% | <input type="radio"/> 20% | <input type="radio"/> 80% |

* 6. The requirement "reporting" may include the following specificities:

| | Strongly disagree | Disagree | Neither agree nor disagree | Agree | Strongly agree |
|---|--------------------------|--------------------------|----------------------------|---------------------------|---------------------------|
| Real-time presentation of the executed operations which were monitored. | <input type="radio"/> 0% | <input type="radio"/> 0% | <input type="radio"/> 10% | <input type="radio"/> 20% | <input type="radio"/> 70% |
| Real-time presentation of execution patterns which are being followed or are likely to be followed. | <input type="radio"/> 0% | <input type="radio"/> 0% | <input type="radio"/> 10% | <input type="radio"/> 30% | <input type="radio"/> 60% |
| Real-time presentation of the compliance verification in transactions executions. | <input type="radio"/> 0% | <input type="radio"/> 0% | <input type="radio"/> 0% | <input type="radio"/> 30% | <input type="radio"/> 70% |
| Real-time presentation of the risk estimated on determining possible execution patterns. | <input type="radio"/> 0% | <input type="radio"/> 0% | <input type="radio"/> 10% | <input type="radio"/> 40% | <input type="radio"/> 50% |
| Real-time alert for irregular situations in monitoring, compliance verification and estimation of negative results. | <input type="radio"/> 0% | <input type="radio"/> 0% | <input type="radio"/> 0% | <input type="radio"/> 20% | <input type="radio"/> 80% |





Questionnaire on Continuous Assurance Services in Information Systems

0% 100%

Part II

This part of the questionnaire intends to compare and rank the relevance of the identified metrics in the dimension in which they are inserted. Thus, you should indicate the degree of importance ascribed to each of them.

Note: you may indicate the same degree of importance to more than one metric in each dimension.

*** 7. Degree of importance of the metrics of dimension "monitoring":**

| | Unimportant | Of little importance | Moderately important | Important | Very important |
|--|--------------------------|--------------------------|--------------------------|---------------------------|---------------------------|
| Real-time monitoring of operations. | <input type="radio"/> 0% | <input type="radio"/> 0% | <input type="radio"/> 0% | <input type="radio"/> 10% | <input type="radio"/> 90% |
| Real-time identification of irregular operations. | <input type="radio"/> 0% | <input type="radio"/> 0% | <input type="radio"/> 0% | <input type="radio"/> 10% | <input type="radio"/> 90% |
| Real-time verification of the processing of required operations at all previous steps. | <input type="radio"/> 0% | <input type="radio"/> 0% | <input type="radio"/> 0% | <input type="radio"/> 30% | <input type="radio"/> 70% |
| Real-time detection of lack of operations. | <input type="radio"/> 0% | <input type="radio"/> 0% | <input type="radio"/> 0% | <input type="radio"/> 20% | <input type="radio"/> 80% |

*** 8. Degree of importance of the metrics of dimension "compliance":**

| | Unimportant | Of little importance | Moderately important | Important | Very important |
|--|--------------------------|--------------------------|---------------------------|---------------------------|---------------------------|
| Recognition of execution patterns. | <input type="radio"/> 0% | <input type="radio"/> 0% | <input type="radio"/> 10% | <input type="radio"/> 30% | <input type="radio"/> 60% |
| Ascertaining of fulfilling of rules. | <input type="radio"/> 0% | <input type="radio"/> 0% | <input type="radio"/> 0% | <input type="radio"/> 40% | <input type="radio"/> 60% |
| Detection of potential errors. | <input type="radio"/> 0% | <input type="radio"/> 0% | <input type="radio"/> 0% | <input type="radio"/> 10% | <input type="radio"/> 90% |
| Verification of compliance of existing policies. | <input type="radio"/> 0% | <input type="radio"/> 0% | <input type="radio"/> 10% | <input type="radio"/> 30% | <input type="radio"/> 60% |

*** 9. Degree of importance of the metrics of dimension "estimation":**


| | Unimportant | Of little importance | Moderately important | Important | Very important |
|---|--------------------------|--------------------------|---------------------------|---------------------------|---------------------------|
| Estimation of possible risks. | <input type="radio"/> 0% | <input type="radio"/> 0% | <input type="radio"/> 0% | <input type="radio"/> 50% | <input type="radio"/> 50% |
| Determination of possible execution patterns which are likely to be followed. | <input type="radio"/> 0% | <input type="radio"/> 0% | <input type="radio"/> 10% | <input type="radio"/> 30% | <input type="radio"/> 60% |

*** 10. Degree of importance of the specificities of the requirement "report":**

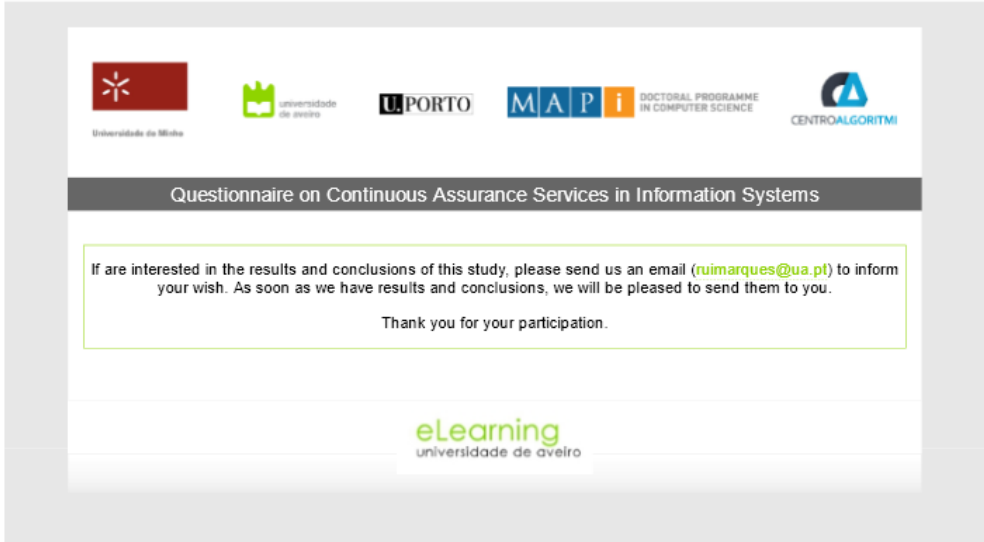
| | Unimportant | Of little importance | Moderately important | Important | Very important |
|---|--------------------------|--------------------------|---------------------------|---------------------------|---------------------------|
| Real-time presentation of the executed operations which were monitored. | <input type="radio"/> 0% | <input type="radio"/> 0% | <input type="radio"/> 10% | <input type="radio"/> 30% | <input type="radio"/> 60% |
| Real-time presentation of execution patterns which are being followed or are likely to be followed. | <input type="radio"/> 0% | <input type="radio"/> 0% | <input type="radio"/> 10% | <input type="radio"/> 40% | <input type="radio"/> 50% |
| Real-time presentation of the compliance verification in transactions executions. | <input type="radio"/> 0% | <input type="radio"/> 0% | <input type="radio"/> 0% | <input type="radio"/> 50% | <input type="radio"/> 50% |
| Real-time presentation of the risk estimated on determining possible execution patterns. | <input type="radio"/> 0% | <input type="radio"/> 0% | <input type="radio"/> 10% | <input type="radio"/> 40% | <input type="radio"/> 50% |
| Real-time alert for irregular situations in monitoring, compliance verification and estimation of negative results. | <input type="radio"/> 0% | <input type="radio"/> 0% | <input type="radio"/> 0% | <input type="radio"/> 10% | <input type="radio"/> 90% |

← Previous
Submit

Exit and clear survey



Appendixes



The image shows a questionnaire slide with a header containing logos for Universidade de Minho, universidade de aveiro, U.PORTO, M.A.P.i DOCTORAL PROGRAMME IN COMPUTER SCIENCE, and CENTROALGORITMI. The main title is "Questionnaire on Continuous Assurance Services in Information Systems". The body text asks for contact information if interested in results and concludes with a thank you. The footer features the "eLearning universidade de aveiro" logo.

Universidade de Minho

universidade de aveiro

U.PORTO

M.A.P.i DOCTORAL PROGRAMME IN COMPUTER SCIENCE

CENTROALGORITMI

Questionnaire on Continuous Assurance Services in Information Systems

If are interested in the results and conclusions of this study, please send us an email (ruimarques@ua.pt) to inform your wish. As soon as we have results and conclusions, we will be pleased to send them to you.

Thank you for your participation.

eLearning
universidade de aveiro

APPENDIX B – PRE-TEST

This appendix supports chapter 3 of this thesis and presents the pre-tests to questionnaire which were used in the application of the Delphi method to validate the model for evaluation of information systems with continuous assurance services. It is structured in three parts:

- B1. Summary of pre-tests with the record sheets of each participant
- B2. Analysis of results of pre-tests by topic, namely weaknesses and strengths
- B3. Proposal of amendments to questionnaire

B1. Summary of Pre-Tests

Record Sheet - Participant 1

Date: 25-06-2013

Characterisation of the participant

- | | |
|--|--------------------------------|
| 1. Area of expertise: | Management Information Systems |
| 2. Years of experience in the area of expertise: | ≥ 10 years |
| 3. Scientific publications on the area of expertise: | Yes |

Time to complete the questionnaire: 9 minutes

Interview recording: Yes

General notes about the participation:

The pre-test took place with no external disruptions, and in a calm environment.

The participant showed concentration and interest when doing the whole pre-test. In addition, the participant has experience of developing questionnaires and participating in pre-tests.

When filling the questionnaire, the participant showed calmness when answering to all questions, and skimmed through the questionnaire (moved forward and backwards through the several parts) without any difficulties. The questionnaire was fully answered.

Comments of the participant:

“Em termos da clareza e do tempo está tudo impecável... está tudo muito ‘clean’, muito direto, o inglês está bem e as frases estão simples.” [“In terms of clarity and time, everything’s impeccable...everything is very “clean”, very direct. The English is good and the sentences are simple.”]

“Está equilibrado e faz-se com muita fluidez”. “As duas partes referem-se basicamente aos mesmos aspetos, e, portanto, a posição das questões também é semelhante. O que ajuda. Quando eu quis fazer a ‘ponte’ com a parte anterior, fui ver e foi fácil de perceber.” [“It is well balanced and fluid.” “The two parts basically refer to the same aspects and so the placement of questions is also similar, which helps. When I wanted to connect it to the previous part, I saw it and it was easy to understand.”]

“Não é daquele género de questionários confusos, em que ficamos com a sensação que estamos a responder a perguntas que se referem às mesmas coisas. Desse ponto de visto, acho que está muito bem.” [“This one is not like the other confusing questionnaires, in which we get the feeling that we are answering to questions that refer to the same things. From this perspective, I think it is really well done.”]

“Eu respondi no pressuposto que isto está relacionado com sistemas financeiros ou suficientemente críticos para justificar algo deste género. E isso não é indicado no questionário, e portanto considerei que estávamos a falar de sistemas críticos ou que se pretendam reduzir drasticamente o risco.” [“I answered on the assumption that this is related with financial or sufficiently critical systems to justify something of this kind. And this is not indicated in the questionnaire, and therefore I considered we were talking about critical systems or that it is intended to sharply reduce the risk.”]

“O formato da questão 5 não é semelhante às outras, e isso saltou-me logo à vista. Se for possível, de visualmente, que isto não chame a atenção é melhor, porque pretende-se o utilizador concentrado no questionário.” [“The format of question 5 is not similar to the others, and that’s why it stood out. If it is possible that it doesn’t visually stand out, it is better, because it is intended that the user focuses on the questionnaire.”]

“As escalas estão bem, e no que diz respeito a escalas de concordância, esta é a melhor.” [“The scales are really well done, and concerning scales of agreement, this is the best.”]

Record sheet - Participant 2

Date: 25-06-2013

Characterisation of the participant

- | | |
|--|---------------------------|
| 1. Area of expertise: | Accounting |
| 2. Years of experience in the area of expertise: | ≥ 2 and < 10 years |
| 3. Scientific publications on the area of expertise: | No |

Time to complete the questionnaire: 9 minutes

Interview recording: No

General notes about the participation:

The pre-test took place with a few external disruptions, which slightly affected the participant's concentration although interest and motivation were shown during the pre-test.

The pre-test was interrupted a few times, including for looking up some words used in the questionnaire.

The questionnaire was fully answered.

Comments of the participant:

The participant referred that looking up words in the dictionary is due to the participant's elementary level of English.

The participant referred that the time to complete the questionnaire is great, because it does not make the questionnaire a long and boring one.

The participant also referred that there is nothing negative to mention regarding the scales, structure and layouts used.

However, the participant mentioned it felt as though there was redundancy of questions in both parts although it was explicitly indicated that in the first part it was intended to know about the agreement and in the second part about the importance of metrics. But still, the participant thinks that there may be some repetition.

Record Sheet - Participant 3

Date: 25-06-2013

Characterisation of the participant

- | | |
|--|--------------------------------|
| 1. Area of expertise: | Management Information Systems |
| 2. Years of experience in the area of expertise: | >= 10 years |
| 3. Scientific publications on the area of expertise: | Yes |

Time to complete the questionnaire: 12 minutes

Interview recording: Yes

General notes about the participation:

The pre-test took place with no external disruptions, and in a calm environment.

The participant showed concentration and interest when doing the whole pre-test. In addition, the participant has experience of developing questionnaires.

When filling the questionnaire, the participant showed calmness when answering to all questions.

The questionnaire was fully answered.

Comments of the participant:

“Na primeira parte custou-me a perceber o que eram as dimensões, e não sei se a frase está muito bem construída. Da forma com está, dá-me a sensação que ‘a inclusão das dimensões é essencial para avaliar as dimensões monitoring, compliance’,... quebrando o ritmo da leitura e interpretação da questão. Talvez ficasse melhor colocar ‘a inclusão das dimensões é essencial para avaliar: a capacidade... ‘ e no fim, entre parêntesis ou logo a seguir, indicar o nome da dimensão.” [“In the first part it was hard for me to understand what was understood as dimensions, and I don’t actually know if the sentence is well structured. In the way it is structured, I understand that

‘the inclusion of the dimensions is essential to assess dimensions monitoring, compliance, ...’ affecting readability. It could be better to write ‘the inclusion of dimensions is essential to assess: capacity...’ and in the end, between brackets or immediately after, indicate the dimension.”]

“A formatação da questão 5 é diferente, e julgo que não deveria ser.” E acrescentou “Talvez partir a questão e colocar ‘Regarding a model for implementing continuous assurance services in information systems’ em cima e a bold, tal como as outras, e na alínea colocar apenas ‘the inclusion of the requirement...’.” [“The structure of question 5 is different and I believe it shouldn’t be so.” And added “The question could be split into two parts and it should be written ‘Regarding a model for implementing continuous assurance services in information systems’ above and in bold, like the others, and in the row only write ‘the inclusion of the requirement...’.”]

“Tudo o resto parece-me bem, incluindo a escolha das escalas.” [“Except for this, everything is really well done for me, including the choice of scales.”]

Record sheet - Participant 4

Date: 25-06-2013

Characterisation of the participant

- | | |
|--|-------------|
| 1. Area of expertise: | Auditing |
| 2. Years of experience in the area of expertise: | >= 10 years |
| 3. Scientific publications on the area of expertise: | No |

Time to complete the questionnaire: 7 minutes

Interview recording: Yes

General notes about the participation:

The pre-test took place with no external disruptions, and in a calm environment.

The participant showed concentration and interest when doing the whole pre-test. The participant had never participated in a pre-test.

When filling the questionnaire, the participant showed calmness when answering to all questions.

The questionnaire was fully answered.

Comments of the participant:

“Gostei do questionário, talvez porque conheço o tema e isso facilitou a interpretação. De uma maneira geral, não vi nada que deva ser acrescentado ou alterado.” [“I liked the questionnaire maybe because I am familiar with the topic and that facilitated my interpretation. In general, I wouldn’t add or change anything.”]

“Não sei se a escala tem muitos graus de concordância, talvez 5 sejam demais e penso que 3 seriam suficientes, por exemplo: discordo, nem concordo nem discordo e concordo. Neste tipo de trabalho, e neste tema em particular, penso que não há necessidade de enfatizar a concordância, basta concordar ou discordar. E penso o mesmo para a escala de importância na segunda parte.” [“I don’t know if the scale has many degrees of agreement, maybe 5 are too many. I believe 3 would be enough, for example: disagree, neither agree nor disagree and agree. In this type of work, and mainly this subject, I think there is no need to enhance the agreement. Agreeing or disagreeing is enough. I have the same opinion as regards the scale of importance in the second part.”]

“Está bem escrito porque, até eu que não domino inglês, percebi tudo na primeira leitura. E a duração está boa, porque demora menos de 10 minutos e não cansa.” [“For me it is well written because I’m not fluent in English and I understood everything when I read it for the first time. And the time for completion is good, because it takes less than 10 minutes and it’s not tiring.”]

Record Sheet - Participant 5

Date: 25-06-2013

Characterisation of the participant

- | | |
|--|--------------------|
| 1. Area of expertise: | Management |
| 2. Years of experience in the area of expertise: | >= 2 and <10 years |
| 3. Scientific publications on the area of expertise: | Yes |

Time to complete the questionnaire: 13 minutes

Interview recording:

Yes

General notes about the participation:

The pre-test took place with no external disruptions, and in a calm environment.

The participant showed concentration and interest when doing the whole pre-test. When filling the questionnaire, the participant showed calmness when answering to all questions.

The questionnaire was fully answered.

Comments of the participant:

“De um modo geral, parece-me bem. No entanto há alguns pormenores que podem ser melhorados, ou talvez clarificados. Por exemplo, o que se entende por ‘irregular situations’? Talvez uma pequena nota ou observação poderia ajudar.” [“In general, I think it’s well done. However, there are some details that could be improved, or maybe made clear. For example, what do you understand by ‘irregular situations’? Maybe a note or observation could help.”]

“Um aspeto que anotei é o facto de todas as alíneas da questão 6 contemplar tempo real exceto uma, porquê? Algum motivo em especial para que a ‘presentation of the compliance verification in transactions executions’ não seja em tempo real? E o mesmo acontece na questão 2, apenas duas alíneas contemplam o tempo real, e no entanto, na minha opinião, também há interesse que as restantes também sejam em tempo real.” [“An aspect that I wrote down was the fact that all lines of question 6 include real time except one, why? Is there any especial reason for ‘presentation of the compliance verification in transactions executions’ not being in real time? The same happens in question 2, where only two lines include the real time, and however, in my opinion it would also be interesting that the others would be in real time too.”]

“A métrica ‘Determination of possible execution patterns’ na questão 4, quando li a primeira vez pareceu-me igual à métrica ‘Recognition of execution patterns.’ da questão 3. Só depois de pensar melhor é que percebi que na questão 3 refere-se ao reconhecimento dos padrões de execução com base nas operações já executadas ou transações concluídas, e na questão 4 refere-se à previsão de possíveis padrões de

execução que podem vir a ser seguidas em transações ainda não concluídas.” [“The metric ‘Determination of possible execution patterns’ in question 4, when I read it for the first time, seemed equal to the metric ‘Recognition of execution patterns.’ of question 3. Only later could I understand that question 3 refers to the recognition of execution patterns based on already executed operations or completed transactions, and question 4 refers to the estimation of possible execution patterns that can be followed in not yet concluded transactions.”]

“Relativamente à parte 2, apesar de eu compreender que tem um significado diferente da parte 1, mas penso que é lógico pensar que se eu estou totalmente de acordo numa das métricas na primeira parte, é óbvio que vou classifica-la como importante na segunda parte. Mas também compreendo da pertinência disto, porque eu posso concordar totalmente com a inclusão de duas métricas mas atribuir mais importância a uma do que a outra. E apenas neste sentido, penso que a segunda parte justifica-se.” [“Concerning part 2, although I understand that it differs from part 1, in my opinion it is logical to think that I strongly agree with one of the metrics in the first part and then it seems obvious that I will classify it as important in the second part. But I also understand the pertinence of this, because I can strongly agree with the inclusion of two metrics but assign more importance to either one or the other. And only in this regard, I think that it justifies having the second part.”]

“As duas escalas utilizadas, tanto a de concordância como a de importância, parecem-me adequadas e ajustadas.” [“The two scales used, both the agreement and the importance, seem suitable and adjusted.”]

“Quando estava a caracterizar o perito lembrei-me que faltaria um campo para o respondente indicar as suas habilitações académicas, só depois lembrei-me que realmente não faz falta, porque se os peritos são previamente selecionados, deve haver um conjunto de requisitos que devem ter sido verificados e um deles, deve ter sido as habilitações.” [“When I was characterizing the expert I remembered that a field for the respondent to indicate the qualifications was missing. Only after did I remember that this is not important since experts are previously selected and there should be a series of requirements that may have been verified, being the qualifications one of them.”]

“Ainda na questão 5 da primeira parte aparece lá um asterisco isolado, há qualquer coisa de diferente naquela questão.” [“Still in question 5 of the first part, there is an isolated asterisk. There is something different in that question.”] The participant also referred “Bastaria ‘Regarding a model for implementing continuous assurance services in information systems, the inclusion of the requirement reporting is essential’, porque subentende-se que se refere às funcionalidades das dimensões anteriores.” [“Having ‘Regarding a model for implementing continuous assurance services in information systems, the inclusion of the requirement reporting is essential’ would be enough because it is inherent that it refers to the functionalities of the previous dimensions.”]

“E para finalizar, gostei da interface gráfica, é muito intuitiva, e da forma como o questionário está implementado.” [“At last, I liked the graphical interface - it is very intuitive, and the way the questionnaire is implemented.”]

B2. Result analysis

Contents

Positive Aspects

1. “This is not like the other confusing questionnaires, in which we get the feeling that we are answering to questions that refer to the same things. From this perspective, I think it is really well done.” (Participant 1)
2. “Concerning part 2, although I understand that it differs from part 1, in my opinion it is logical to think that I strongly agree with one of the metrics in the first part and then it seems obvious that I will classify it as important in the second part. But I also understand the pertinence of this, because I can strongly agree with the inclusion of two metrics but assign more importance to either one or the other. And only in this regard, I think that it justifies having the second part.” (Participant 5)
3. “When I was characterizing the expert I remembered that a field for the respondent to indicate the qualifications was missing. Only after did I remember that this is not important since experts are previously selected and

there should be a series of requirements that may have been verified, being the qualifications one of them.” (Participant 5)

Negative Aspects

4. It feels as though there are redundant questions in both parts although it was explicitly indicated that in the first part it was intended to know about the agreement and in the second part about the importance of metrics. But still, the participant thinks there may have been some repetition. (Participant 2)
5. “An aspect that I wrote down was the fact that all lines of question 6 include real time except one, why? Is there any especial reason for ‘presentation of the compliance verification in transactions executions’ not being in real time? The same happens in question 2. Only two lines include the real time, and however, in my opinion it would also be interesting that the others would be in real time too.” (Participant 5)

Analysis

The positive aspects mentioned show in general that the contents are pertinent and adequate to the topic of the questionnaire. The aspects mentioned mainly enhance that no redundancies were found, and that the need to have Part II of the questionnaire was strengthened as well as the verification that the items of characterisation of experts are enough.

Aspect 4 shouldn’t be considered since the participant refers that it is only a “feeling that something is repeated” that may be justified, as indicated in the general notes of the record sheet of this participation, by the fact that the pre-test has been interrupted and has affected the concentration of the participant.

Aspect 5 should be considered taking into account the researcher’s objectives.

Duration

Positive Aspects

6. “In terms of clarity and time, everything’s impeccable.” (Participant 1)

7. The participant referred that the time to complete the questionnaire is great, because it does not make the questionnaire a long and boring one. (Participant 2)
8. The duration is good, because it takes less than 10 minutes and it's not tiring." (Participant 4)

Negative Aspects

Nothing negative was mentioned.

Analysis

The comment obtained from the pre-tests show that the duration of the questionnaire is good.

Scale

Positive Aspects

9. "The scales are really well done, and regarding scales of agreement, this is the best." (Participant 1)
10. Has nothing negative to mention in what regards the used scales. (Participant 2)
11. "Everything else appears well done to me, including the choice of scales." (Participant 3)
12. "The two scales used, both the agreement and the importance, seem suitable and adjusted." (Participant 5)

Negative Aspects

13. "I don't know if the scale has many degrees of agreement, maybe 5 are too many. I believe 3 would be enough, for example: disagree, neither agree nor disagree and agree. In this type of work, and mainly this subject, I think there is no need to enhance the agreement. Agreeing or disagreeing is enough. I have the same opinion as regards the scale of importance in the second part." (Participant 4)

Analysis

The comments obtained from the pre-tests show that the adopted scales are adequate, since 4 out of the 5 participants agree with the scales. Aspect 13 should not be considered because, besides having a minority opinion, the literature recommends the use of linear scales of agreement with an odd number of items (5, 7 or 9 items are the most used).

Structure

Positive Aspects

14. “It is well balanced and fluid. “The two parts basically refer to the same aspects and so the placement of questions is also similar, which helps. When I wanted to connect it to the previous part, I saw it and it was easy to understand.” (Participant 1)
15. Has nothing negative to mention regarding the scales used. (Participant 2)
16. “At last, I liked the graphical interface - it is very intuitive, and the way the questionnaire is implemented.” (Participant 5)

Negative Aspects

17. “The format of question 5 is not similar to the others, and that’s why it stood out. If it is possible that it doesn’t visually stand out it is better, because it is intended that the user focuses on the questionnaire.” (Participant 1)
18. “The structure of question 5 is different and I believe it shouldn’t be so.” And added “The question could be split into two parts and it should be written ‘Regarding a model for implementing continuous assurance services in information systems’ above and in bold, like the others, and in the row only write ‘the inclusion of the requirement...’.” (Participant 3)
19. “Still in question 5 of the first part, there is an isolated asterisk. There is something different in that question.” (Participant 5)

Analysis

The comments obtained from the pre-tests show that the structure of the questionnaire is adequate. However, 3 out of the 5 participants indicated the way question 5 of Part I is presented, because it is the only one with a different structure. This aspect should be corrected, following the suggestion given by participant 3 (see aspect 18).

Interpretation

Positive Aspects

20. "In terms of clarity and time, everything's impeccable...everything is very "clean", very direct. The English is good and the sentences are simple. (Participant 1)
21. "I liked the questionnaire maybe because I am familiar with the subject and that facilitated my interpretation. (Participant 4)
22. "For me it is well written because I'm not fluent in English and I understood everything when I read it for the first time." (Participant 4)

Negative Aspects

23. "I answered on the assumption that this is related with financial or sufficiently critical systems to justify something of this kind. And this is not indicated in the questionnaire and therefore I considered we were talking about critical systems or that it is intended to sharply reduce the risk." (Participant 1)
24. "In the first part it was hard for me to understand what was understood as dimensions, and I don't actually know if the sentence is well structured. In the way it is structured, I understand that 'the inclusion of the dimensions is essential to assess dimensions monitoring, compliance, ...' affecting readability. It could be better to write 'the inclusion of dimensions is essential to assess: capacity...' and in the end, between brackets or immediately after, indicate the dimension." (Participant 3)

25. “What do you understand by ‘irregular situations’? Maybe a note or observation could help.” (Participant 5)
26. “The metric ‘Determination of possible execution patterns’ in question 4, when I read it for the first time, seemed equal to the metric ‘Recognition of execution patterns.’ of question 3. “Only later could I understand that question 3 refers to the recognition of execution patterns based on already executed operations or completed transactions, and question 4 refers to the estimation of possible execution patterns that can be followed in not yet concluded transactions.” (Participant 3)
27. “Having ‘Regarding a model for implementing continuous assurance services in information systems, the inclusion of the requirement reporting is essential’ would be enough because it is inherent that it refers to the functionalities of the previous dimensions.” (Participant 5)

Analysis

The comments obtained from the pre-tests show that in general the contents of the questionnaire are clear and are well interpreted. Only a few details that should be solved with the clarification of some concepts used in the questionnaire were quoted (25 and 26).

As for aspect 23, no clarification will be added to the questionnaire because the respondents have expertise in the subject and understand that this type of systems is applied in situations in which it is intended to minimize the risk.

Regarding aspect 24, participant 3 was the only one to refer problem with interpretation in question 1 Part I, but the suggestion given can be used to improve the interpretation of the sentence.

Question 5 can be shortened, as follows “Regarding a model for implementing continuous assurance services in information systems, the inclusion of the requirement “reporting” is essential”, as suggested and due to the reasons presented by the participant.

Completeness

Positive Aspects

All participants completed the questionnaire.

Negative Aspects

Nothing negative to mention.

Analysis

The questionnaire does not show obstacles and/or problems that prevent respondents from completing the questionnaire and submitting their answers.

B3. Amendments to the questionnaire

Taking into account the comments obtained from the pre-tests and the researcher's objectives for this work, the following amendments are proposed:

Contents

1. Question 2 Part I should be altered so that the last two lines also include the "real time" (see Table 20).
2. Question 6 Part I should be altered so that the requirement 'Presentation of the compliance verification in transactions executions.' also includes "real time" (see Table 21).
3. Questions 7 and 10 Part II should be adjusted according to the previously indicated amendments, since these are correlated.

Duration

Nothing to change.

Scale

Nothing to change.

Table 20 - Amendments to the questionnaire (question 2)

| | | | | | | |
|---|---|--|-----------------------|-----------------------|-----------------------|-----------------------|
| 2. Dimension "monitoring" may include the following metrics to evaluate the system: (Note: for real-time refers to a minimum period in which it is necessary or useful to have information) | | | | | | |
| 2.1 | Real-time monitoring of operations. | | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 2.2 | Real-time identification of irregular operations (e.g. poorly executed operations, incongruities, etc). | | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 2.3 | Real-time verification of the processing of required operations at all previous steps. | | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 2.4 | Real-time detection of lack of operations. | | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

Table 21 - Amendments to the questionnaire (question 6)

| | | | | | | |
|--|---|--|-----------------------|-----------------------|-----------------------|-----------------------|
| 6. The requirement "reporting" may include the following specificities: | | | | | | |
| 6.1 | Real-time presentation of the executed operations which were monitored. | | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 6.2 | Real-time presentation of execution patterns which are being followed or are likely to be followed. | | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 6.3 | Real-time presentation of the compliance verification in transactions executions. | | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 6.4 | Real-time presentation of the risk estimated on determining possible execution patterns. | | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 6.5 | Real-time alert for irregular situations in monitoring, compliance verification and estimation of negative results. | | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

Structure

- Question 5 Part I should have the same structure and should be formatted according to the other questions. Thus, text ‘5. Regarding a model for implementing continuous assurance services in information systems:’ should be included in bold in section 1 (highlighted in Figure 42), and the text ‘The inclusion of the requirement “reporting” is essential so that the results of “monitoring”, “compliance”, and “estimation” functions can be presented and reported to the users of the system.’ should be kept in section 2 (highlighted in Figure 42).

| * 4. Dimension "estimation" may include the following metrics to evaluate the system: | | | | | |
|---|-----------------------|-----------------------|----------------------------|-----------------------|-----------------------|
| | Strongly disagree | Disagree | Neither agree nor disagree | Agree | Strongly agree |
| Estimation of possible risks. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Determination of possible execution patterns. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

Section 1

| 5. Regarding a model for implementing continuous assurance services in information systems, the inclusion of the requirement "reporting" is essential so that the results of "monitoring", "compliance" and "estimation" functions can be presented and reported to the users of the system: | | | | | |
|--|-----------------------|-----------------------|----------------------------|-----------------------|-----------------------|
| | Strongly disagree | Disagree | Neither agree nor disagree | Agree | Strongly agree |
| | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

Section 2

| * 6. The requirement "reporting" may include the following specificities: | | | | | |
|---|-----------------------|-----------------------|----------------------------|-----------------------|-----------------------|
| | Strongly disagree | Disagree | Neither agree nor disagree | Agree | Strongly agree |
| Real-time presentation of the executed operations which | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

Figure 42 - Amendments to the questionnaire (question 5)

Interpretation

- 5. Question 1 Part I should be rewritten for a better understanding (see table 3).

Table 22 - Amendments to the questionnaire (question 1)

| 1. Regarding a model for implementing continuous assurance services in information systems, the inclusion of dimensions is essential for evaluating: | | | | | |
|---|---|-----------------------|-----------------------|-----------------------|-----------------------|
| 1.1 | The ability of the system to monitor transactions which are intended to be audited (Dimension "monitoring"). | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 1.2 | The ability of the system to verify conformity and integrity with which transactions are executed (Dimension "compliance"). | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 1.3 | The ability of the system to estimate assurance, coherence and consistency of transactions which are being executed (Dimension "estimation"). | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

- 6. A clarification of the term 'irregular operations' should be added by using examples (see Table 20).
- 7. In question 4 Part I, the line 'Determination of possible execution patterns.' should be rewritten as 'Determination of possible execution patterns which are likely to be followed.' in order to avoid confusion of redundancy with line 'Recognition of execution patterns.' of question 3.

Appendixes

8. Question 9 Part II should be altered according to alteration indicated in the previous point.
9. Question 5 should be shortened as follows “Regarding a model for implementing continuous assurance services in information systems, the inclusion of the requirement “reporting” is essential”.

Completeness

Nothing to change.

APPENDIX C – E-MAILS

This appendix supports chapter 3 of this thesis and presents the e-mails which were sent within the scope of application of the Delphi method to validate the model for evaluation of information systems with continuous assurance services. It is structured in five parts:

- C1. E-mail requesting collaboration to be a member of the panel of experts
- C2. Email to send the link of questionnaire (1st iteration) to experts
- C3. E-mail to reinforce the request of questionnaire completion (1st iteration)
- C4. Email to send the link of questionnaire (2nd iteration) to experts
- C5. E-mail to reinforce the request for questionnaire completion (2nd iteration)

C1. E-mail requesting collaboration to be a member of the panel of experts

Subject: Request for collaboration in a panel of experts

Dear [Title] [Name],

An ongoing study in the area of Information Systems with Continuous Assurance services is being carried out under the Doctoral Program in Computer Science MAP-i, taught jointly by the Universities of Minho, Aveiro and Porto (Portugal). The study is being conducted by the student Rui Pedro Figueiredo Marques, and supervised by Professor Henrique Manuel Dinis dos Santos (University of Minho) and Professor Carlos Alberto Lourenço dos Santos (University of Aveiro).

This study is following the Delphi methodology, which aims to gather the opinions of a panel of experts in the study area in order to achieve consensus on a set of factors. For this study, the collaboration by experts is required for completing a questionnaire (about 10 minutes) which will be distributed at most in three rounds.

We would also like to emphasize that the participation in the panel is completely anonymous and confidential, both during and after the study, and the results will only be presented in aggregate form.

Thus, we would like you to participate in this panel. We would like to confirm your acceptance as soon as possible so that we can start the distribution of the first questionnaire in the coming days.

Your collaboration will be of utmost importance for the success of this study. We hope to hear from you soon and look forward to your participation. Thank you.

Best regards,

Rui Marques

C2. Email to send the link of the questionnaire (1st iteration) to experts

Subject: RE: Request for collaboration in a panel of experts

Dear [Title] [Name],

First of all, thank you for accepting to participate in this study.

The questionnaire for the first round of collection of opinions is available at the following link: <http://questionarios.ua.pt/index.php/583212/lang-en>.

The estimated time to complete it is 10 minutes. Remember that your participation is completely anonymous and confidential.

We would appreciate if you could complete the questionnaire by July 11th.
Thankyou.

BestRegards,

Rui Marques

C3. E-mail to reinforce the request of questionnaire completion (1st iteration)

Dear [Title][Name],

If you have already completed the questionnaire (1st iteration), please do not consider this email and I apologize for the inconvenience of receiving it. I also appreciate the fact you have already participated.

If you have not had the opportunity to complete the questionnaire, I would ask you to complete it within the next two days so that this iteration can be successfully completed, and we can thus send the second iteration of questionnaire. I would like to enhance that your participation is crucial to the success of this study.

The questionnaire is still available at:

<http://questionarios.ua.pt/index.php/583212/lang-en>.

Thank you for your attention.

Best regards,

Rui Marques

Email to send the link of the questionnaire (2nd iteration) to experts

Dear [Title][Name]

First of all, thank you for your participation in the first iteration of this questionnaire.

Now, we ask you to participate in the second iteration of the questionnaire of this study.

The questionnaire of this iteration is exactly equal to the one of the first iteration but some statistical data on the results of the previous iteration were added. Thus, you are able to reevaluate your answers, if you wish so. However, the most important is that your answers reflect your real opinion about each of the statements.

The questionnaire for the second round of collection of opinions is available at the following link: <http://questionarios.ua.pt/index.php/522841/lang-en>.

Remember that your participation is completely anonymous and confidential.

We would appreciate if you could complete the questionnaire by July 27th. Thank you.

Best regards,

Rui Marques

C5. E-mail to reinforce the request of questionnaire completion (2nd iteration)

Dear [Title][Name],

If you have already completed the second iteration of the questionnaire, please do not consider this email and I apologize for the inconvenience of receiving it. I also appreciate the fact you have already participated.

Appendixes

If you have not had the opportunity to complete this iteration of the questionnaire, I would ask you to complete it within the next two days, so that this iteration can be successfully completed, and we can thus send the second iteration of questionnaire. I would like to enhance that your participation is crucial to the success of this study.

The questionnaire is still available at:

<http://questionarios.ua.pt/index.php/522841/lang-en>.

Thank you for your attention.

Best regards,

Rui Marques

APPENDIX D – RESULTS OF QUESTIONNAIRES

This appendix supports chapter 3 of this thesis and presents the questionnaires which were used in the application of the Delphi method to validate the model for evaluation of information systems with continuous assurance services. It is structured in two parts:

D1. Distribution of answers of the questionnaires

D2. Statistical data from answers of questionnaire and determination of consensus

D1. Distribution of answers of the questionnaires

Table 23 - Distribution of answers of participants for Part I of questionnaire (1st iteration)

| Statements | Strongly disagree (1) | Disagree (2) | Neither agree nor disagree (3) | Agree (4) | Strongly agree (5) |
|--|-----------------------|--------------|--------------------------------|-----------|--------------------|
| Regarding a model for implementing continuous assurance services in information systems, the inclusion of dimensions is essential for evaluating: [The ability of the system to monitor transactions which are intended to be audited (Dimension "monitoring")] | 0% | 0% | 0% | 100% | 90% |
| Regarding a model for implementing continuous assurance services in information systems, the inclusion of dimensions is essential for evaluating: [The ability of the system to verify conformity and integrity with which transactions are executed (Dimension "compliance")] | 0% | 0% | 0% | 200% | 80% |
| Regarding a model for implementing continuous assurance services in information systems, the inclusion of dimensions is essential for evaluating: [The ability of the system to estimate assurance, coherence and consistency of transactions which are being executed (Dimension "estimation")] | 0% | 0% | 0% | 500% | 50% |
| Dimension "monitoring" may include the following metrics to evaluate the system: [Real-time monitoring of operations] | 0% | 0% | 0% | 200% | 80% |
| Dimension "monitoring" may include the following metrics to evaluate the system: [Real-time identification of irregular operations (e.g. poorly executed operations, incongruities, etc.)] | 0% | 0% | 0% | 0% | 100% |
| Dimension "monitoring" may include the following metrics to evaluate the system: [Real-time verification of the processing of required operations at all previous steps.] | 0% | 0% | 0% | 40% | 60% |
| Dimension "monitoring" may include the following metrics to evaluate the system: [Real-time detection of lack of operations.] | 0% | 0% | 0% | 200% | 80% |
| Dimension "compliance" may include the following metrics to evaluate the system: [Recognition of execution patterns.] | 0% | 0% | 0% | 40% | 60% |
| Dimension "compliance" may include the following metrics to evaluate the system: [Ascertainment of fulfilling of rules.] | 0% | 0% | 0% | 50% | 50% |
| Dimension "compliance" may include the following metrics to evaluate the system: [Detection of potential errors.] | 0% | 0% | 0% | 10% | 90% |
| Dimension "compliance" may include the following metrics to evaluate the system: [Verification of compliance of existing policies.] | 0% | 0% | 0% | 50% | 50% |
| Dimension "estimation" may include the following metrics to evaluate the system: [Estimation of possible risks.] | 0% | 0% | 0% | 40% | 60% |
| Dimension "estimation" may include the following metrics to evaluate the system: Determination of possible execution patterns which are likely to be followed.] | 0% | 0% | 0% | 30% | 70% |
| Regarding a model for implementing continuous assurance services in information systems [The inclusion of the requirement "reporting" is essential] | 0% | 0% | 0% | 200% | 80% |
| The requirement "reporting" may include the following specificities: [Real-time presentation of the executed operations which were monitored.] | 0% | 0% | 10% | 20% | 70% |
| The requirement "reporting" may include the following specificities: [Real-time presentation of execution patterns which are being followed or are likely to be followed.] | 0% | 0% | 10% | 30% | 60% |
| The requirement "reporting" may include the following specificities: [Real-time presentation of the compliance verification transactions executions.] | 0% | 0% | 0% | 300% | 70% |
| The requirement "reporting" may include the following specificities: [Real-time presentation of the risk estimated on determining possible execution patterns.] | 0% | 0% | 10% | 40% | 50% |
| The requirement "reporting" may include the following specificities: [Real-time alert for irregular situations in monitoring compliance verification and estimation of negative results.] | 0% | 0% | 0% | 200% | 80% |

Table 24 - Distribution of answers of participants for Part II of questionnaire (1st iteration)

| Statements | Unimportant (1) | Of little importance (2) | Moderately important (3) | Important (4) | Very important (5) |
|--|--------------------|--------------------------------|--------------------------------|------------------|--------------------------|
| Degree of importance of the metrics of dimension "monitoring": [Real-time monitoring of operations.] | 0% | 0% | 0% | 10% | 90% |
| Degree of importance of the metrics of dimension "monitoring": [Real-time identification of irregular operations.] | 0% | 0% | 0% | 10% | 90% |
| Degree of importance of the metrics of dimension "monitoring": [Real-time verification of the processing of required operations at all previous steps.] | 0% | 0% | 0% | 30% | 70% |
| Degree of importance of the metrics of dimension "monitoring": [Real-time detection of lack of operations.] | 0% | 0% | 0% | 20% | 80% |
| Degree of importance of the metrics of dimension "compliance": [Recognition of execution patterns.] | 0% | 0% | 10% | 30% | 60% |
| Degree of importance of the metrics of dimension "compliance": [Ascertaining of fulfilling of rules.] | 0% | 0% | 0% | 40% | 60% |
| Degree of importance of the metrics of dimension "compliance": [Detection of potential errors.] | 0% | 0% | 0% | 10% | 90% |
| Degree of importance of the metrics of dimension "compliance": [Verification of compliance of existing policies.] | 0% | 0% | 10% | 30% | 60% |
| Degree of importance of the metrics of dimension "estimation": [Estimation of possible risks.] | 0% | 0% | 0% | 50% | 50% |
| Degree of importance of the metrics of dimension "estimation": [Determination of possible execution patterns which are likely to be followed.] | 0% | 0% | 10% | 30% | 60% |
| Degree of importance of the specificities of the requirement "report": [Real-time presentation of the executed operations which were monitored.] | 0% | 0% | 10% | 30% | 60% |
| Degree of importance of the specificities of the requirement "report": [Real-time presentation of execution patterns which are being followed or are likely to be followed.] | 0% | 0% | 10% | 40% | 50% |
| Degree of importance of the specificities of the requirement "report": [Real-time presentation of the compliance verification in transactions executions.] | 0% | 0% | 0% | 50% | 50% |
| Degree of importance of the specificities of the requirement "report": [Real-time presentation of the risk estimated on determining possible execution patterns.] | 0% | 0% | 10% | 40% | 50% |
| Degree of importance of the specificities of the requirement "report": [Real-time alert for irregular situations in monitoring, compliance verification and estimation of negative results.] | 0% | 0% | 0% | 10% | 90% |

Table 25 - Distribution of answers of participants for Part I of questionnaire (2nd iteration)

| Statements | Strongly disagree (1) | Disagree (2) | Neither agree nor disagree (3) | Agree (4) | Strongly agree (5) |
|--|-----------------------|--------------|--------------------------------|-----------|--------------------|
| Regarding a model for implementing continuous assurance services in information systems, the inclusion of dimensions is essential for evaluating: [The ability of the system to monitor transactions which are intended to be audited (Dimension "monitoring")] | 0% | 0% | 0% | 0% | 100% |
| Regarding a model for implementing continuous assurance services in information systems, the inclusion of dimensions is essential for evaluating: [The ability of the system to verify conformity and integrity with which transactions are executed (Dimension "compliance")] | 0% | 0% | 0% | 0% | 100% |
| Regarding a model for implementing continuous assurance services in information systems, the inclusion of dimensions is essential for evaluating: [The ability of the system to estimate assurance, coherence and consistency of transactions which are being executed (Dimension "estimation")] | 0% | 0% | 0% | 22% | 78% |
| Dimension "monitoring" may include the following metrics to evaluate the system: [Real-time monitoring of operations.] | 0% | 0% | 0% | 0% | 100% |
| Dimension "monitoring" may include the following metrics to evaluate the system: [Real-time identification of irregular operations (e.g. poorly executed operations, incongruities, etc).] | 0% | 0% | 0% | 0% | 100% |
| Dimension "monitoring" may include the following metrics to evaluate the system: [Real-time verification of the processing of required operations at all previous steps.] | 0% | 0% | 0% | 22% | 78% |
| Dimension "monitoring" may include the following metrics to evaluate the system: [Real-time detection of lack of operations.] | 0% | 0% | 0% | 0% | 100% |
| Dimension "compliance" may include the following metrics to evaluate the system: [Recognition of execution patterns.] | 0% | 0% | 0% | 33% | 67% |
| Dimension "compliance" may include the following metrics to evaluate the system: [Ascertaining of fulfilling of rules.] | 0% | 0% | 0% | 44% | 56% |
| Dimension "compliance" may include the following metrics to evaluate the system: [Detection of potential errors.] | 0% | 0% | 0% | 0% | 100% |
| Dimension "compliance" may include the following metrics to evaluate the system: [Verification of compliance of existing policies.] | 0% | 0% | 0% | 22% | 78% |
| Dimension "estimation" may include the following metrics to evaluate the system: [Estimation of possible risks.] | 0% | 0% | 0% | 22% | 78% |
| Dimension "estimation" may include the following metrics to evaluate the system: Determination of possible execution patterns which are likely to be followed.] | 0% | 0% | 0% | 22% | 78% |
| Regarding a model for implementing continuous assurance services in information systems [The inclusion of the requirement "reporting" is essential.] | 0% | 0% | 0% | 0% | 100% |
| The requirement "reporting" may include the following specificities: [Real-time presentation of the executed operations which were monitored.] | 0% | 0% | 0% | 0% | 100% |
| The requirement "reporting" may include the following specificities: [Real-time presentation of execution patterns which are being followed or are likely to be followed.] | 0% | 0% | 0% | 11% | 89% |
| The requirement "reporting" may include the following specificities: [Real-time presentation of the compliance verification in transactions executions.] | 0% | 0% | 0% | 0% | 100% |
| The requirement "reporting" may include the following specificities: [Real-time presentation of the risk estimated on determining possible execution patterns.] | 0% | 0% | 0% | 33% | 67% |
| The requirement "reporting" may include the following specificities: [Real-time alert for irregular situations in monitoring compliance verification and estimation of negative results.] | 0% | 0% | 0% | 0% | 100% |

Table 26 - Distribution of answers of participants for Part II of questionnaire (2nd iteration)

| Statements | Unimportant (1) | Of little importance (2) | Moderately important (3) | Important (4) | Very important (5) |
|--|--------------------|--------------------------------|--------------------------------|------------------|--------------------------|
| Degree of importance of the metrics of dimension "monitoring": [Real-time monitoring of operations.] | 0% | 0% | 0% | 0% | 100% |
| Degree of importance of the metrics of dimension "monitoring": [Real-time identification of irregular operations.] | 0% | 0% | 0% | 0% | 100% |
| Degree of importance of the metrics of dimension "monitoring": [Real-time verification of the processing of required operations at all previous steps.] | 0% | 0% | 0% | 11% | 89% |
| Degree of importance of the metrics of dimension "monitoring": [Real-time detection of lack of operations.] | 0% | 0% | 0% | 0% | 100% |
| Degree of importance of the metrics of dimension "compliance": [Recognition of execution patterns.] | 0% | 0% | 0% | 22% | 78% |
| Degree of importance of the metrics of dimension "compliance": [Ascertaining of fulfilling of rules.] | 0% | 0% | 0% | 44% | 56% |
| Degree of importance of the metrics of dimension "compliance": [Detection of potential errors.] | 0% | 0% | 0% | 0% | 100% |
| Degree of importance of the metrics of dimension "compliance": [Verification of compliance of existing policies.] | 0% | 0% | 0% | 11% | 89% |
| Degree of importance of the metrics of dimension "estimation": [Estimation of possible risks.] | 0% | 0% | 0% | 33% | 67% |
| Degree of importance of the metrics of dimension "estimation": [Determination of possible execution patterns which are likely to be followed.] | 0% | 0% | 0% | 33% | 67% |
| Degree of importance of the specificities of the requirement "report": [Real-time presentation of the executed operations which were monitored.] | 0% | 0% | 0% | 11% | 89% |
| Degree of importance of the specificities of the requirement "report": [Real-time presentation of execution patterns which are being followed or are likely to be followed.] | 0% | 0% | 0% | 22% | 78% |
| Degree of importance of the specificities of the requirement "report": [Real-time presentation of the compliance verification in transactions executions.] | 0% | 0% | 0% | 33% | 67% |
| Degree of importance of the specificities of the requirement "report": [Real-time presentation of the risk estimated on determining possible execution patterns.] | 0% | 0% | 0% | 33% | 67% |
| Degree of importance of the specificities of the requirement "report": [Real-time alert for irregular situations in monitoring, compliance verification and estimation of negative results.] | 0% | 0% | 0% | 0% | 100% |

D3. Statistical data from answers of questionnaire and determination of consensus

Table 27 - Statistical data from answers for Part I of questionnaire (1st iteration)

| Statements | Mode | Percentiles | | | Consensus |
|--|------|-------------|------|------|-----------|
| | | 25 | 50 | 75 | |
| Regarding a model for implementing continuous assurance services in information systems, the inclusion of dimensions is essential for evaluating. The ability of the system to monitor transactions which are intended to be audited (Dimension Monitoring) | 5 | 5,00 | 5,00 | 5,00 | Excellent |
| Regarding a model for implementing continuous assurance services in information systems, the inclusion of dimensions is essential for evaluating. The ability of the system to verify conformity and integrity with which transactions are executed (Dimension Compliance) | 5 | 4,75 | 5,00 | 5,00 | High |
| Regarding a model for implementing continuous assurance services in information systems, the inclusion of dimensions is essential for evaluating. The ability of the system to estimate assurance, coherence and consistency of transactions which are being executed (Dimension Estimation) | 4* | 4,00 | 4,50 | 5,00 | Moderate |
| Dimension "monitoring" may include the following metrics to evaluate the system: Real-time monitoring of operations | 5 | 4,75 | 5,00 | 5,00 | High |
| Dimension "monitoring" may include the following metrics to evaluate the system: Real-time identification of irregular operations (e.g. poorly executed operations, incongruities, etc) | 5 | 5,00 | 5,00 | 5,00 | Excellent |
| Dimension "monitoring" may include the following metrics to evaluate the system: Real-time verification of the processing of required operations at all previous steps | 5 | 4,00 | 5,00 | 5,00 | High |
| Dimension "monitoring" may include the following metrics to evaluate the system: Real-time detection of lack of operations | 5 | 4,75 | 5,00 | 5,00 | High |
| Dimension "compliance" may include the following metrics to evaluate the system: Recognition of execution patterns | 5 | 4,00 | 5,00 | 5,00 | High |
| Dimension "compliance" may include the following metrics to evaluate the system: Ascertainment of fulfilling of rules | 4* | 4,00 | 4,50 | 5,00 | Moderate |
| Dimension "compliance" may include the following metrics to evaluate the system: Detection of potential errors | 5 | 5,00 | 5,00 | 5,00 | Excellent |
| Dimension "compliance" may include the following metrics to evaluate the system: Verification of compliance of existing policies | 4* | 4,00 | 4,50 | 5,00 | Moderate |
| Dimension "compliance" may include the following metrics to evaluate the system: Estimation of possible risks | 5 | 4,00 | 5,00 | 5,00 | High |
| Dimension "estimation" may include the following metrics to evaluate the system: Determination of possible execution patterns which are likely to be followed | 5 | 4,00 | 5,00 | 5,00 | High |
| Regarding a model for implementing continuous assurance services in information systems: The inclusion of the requirement "reporting" is essential | 5 | 4,75 | 5,00 | 5,00 | High |
| The requirement "reporting" may include the following specificities: Real-time presentation of the executed operations which were monitored | 5 | 4,00 | 5,00 | 5,00 | High |
| The requirement "reporting" may include the following specificities: Real-time presentation of execution patterns which are being followed or are likely to be followed | 5 | 4,00 | 5,00 | 5,00 | High |
| The requirement "reporting" may include the following specificities: Real-time presentation of the compliance verification in transactions executions | 5 | 4,00 | 5,00 | 5,00 | High |
| The requirement "reporting" may include the following specificities: Real-time presentation of the risk estimated on determining possible execution patterns | 5 | 4,00 | 4,50 | 5,00 | High |
| The requirement "reporting" may include the following specificities: Real-time alert for irregular situations in monitoring compliance verification and estimation of negative results | 5 | 4,75 | 5,00 | 5,00 | High |

* Multiple modes exist. The smallest value is shown.

Table 28 - Statistical data from answers for Part II of questionnaire (1st iteration)

| Statements | Mode | Percentiles | | | Consensus |
|---|------|-------------|------|------|-----------|
| | | 25 | 50 | 75 | |
| Degree of importance of the metrics of dimension "monitoring": Real-time monitoring of operations | 5 | 5,00 | 5,00 | 5,00 | Excellent |
| Degree of importance of the metrics of dimension "monitoring": Real-time identification of irregular operations | 5 | 5,00 | 5,00 | 5,00 | Excellent |
| Degree of importance of the metrics of dimension "monitoring": Real-time verification of the processing of required operations at all previous steps | 5 | 4,00 | 5,00 | 5,00 | High |
| Degree of importance of the metrics of dimension "monitoring": Real-time detection of lack of operations | 5 | 4,75 | 5,00 | 5,00 | High |
| Degree of importance of the metrics of dimension "compliance": Recognition of execution patterns | 5 | 4,00 | 5,00 | 5,00 | High |
| Degree of importance of the metrics of dimension "compliance": Ascertaining of fulfilling of rules | 4 | 4,00 | 4,00 | 5,00 | Moderate |
| Degree of importance of the metrics of dimension "compliance": Detection of potential errors | 5 | 5,00 | 5,00 | 5,00 | Excellent |
| Degree of importance of the metrics of dimension "compliance": Verification of compliance of existing policies | 5 | 4,00 | 5,00 | 5,00 | High |
| Degree of importance of the metrics of dimension "estimation": Estimation of possible risks | 4* | 4,00 | 4,50 | 5,00 | Moderate |
| Degree of importance of the metrics of dimension "estimation": Determination of possible execution patterns which are likely to be followed | 5 | 4,00 | 5,00 | 5,00 | High |
| Degree of importance of the specificities of the requirement "report": Real-time presentation of the executed operations which were monitored | 5 | 4,00 | 5,00 | 5,00 | High |
| Degree of importance of the specificities of the requirement "report": Real-time presentation of execution patterns which are being followed or are likely to be followed | 5 | 4,00 | 4,50 | 5,00 | High |
| Degree of importance of the specificities of the requirement "report": Real-time presentation of the compliance verification in transactions executions | 4* | 4,00 | 4,50 | 5,00 | Moderate |
| Degree of importance of the specificities of the requirement "report": Real-time presentation of the risk estimated on determining possible execution patterns | 5 | 4,00 | 4,50 | 5,00 | High |
| Degree of importance of the specificities of the requirement "report": Real-time alert for irregular situations in monitoring, compliance verification and estimation of negative results | 5 | 5,00 | 5,00 | 5,00 | Excellent |

* Multiple modes exist. The smallest value is shown.

Table 29 - Statistical data from answers for Part I of questionnaire (2nd iteration)

| Statements | Mode | Percentiles | | | Consensus |
|--|------|-------------|----|----|-----------|
| | | 25 | 50 | 75 | |
| Regarding a model for implementing continuous assurance services in information systems, the inclusion of dimensions is essential for evaluating. The ability of the system to monitor transactions which are intended to be audited (Dimension Monitoring) | 5 | 5 | 5 | 5 | Excellent |
| Regarding a model for implementing continuous assurance services in information systems, the inclusion of dimensions is essential for evaluating. The ability of the system to verify conformity and integrity with which transactions are executed (Dimension Compliance) | 5 | 5 | 5 | 5 | Excellent |
| Regarding a model for implementing continuous assurance services in information systems, the inclusion of dimensions is essential for evaluating. The ability of the system to estimate assurance, coherence and consistency of transactions which are being executed (Dimension Estimation) | 5 | 4,5 | 5 | 5 | High |
| Dimension "monitoring" may include the following metrics to evaluate the system: Real-time monitoring of operations | 5 | 5 | 5 | 5 | Excellent |
| Dimension "monitoring" may include the following metrics to evaluate the system: Real-time identification of irregular operations (e.g. poorly executed operations, incongruities, etc) | 5 | 5 | 5 | 5 | Excellent |
| Dimension "monitoring" may include the following metrics to evaluate the system: Real-time verification of the processing of required operations at all previous steps | 5 | 4,5 | 5 | 5 | High |
| Dimension "monitoring" may include the following metrics to evaluate the system: Real-time detection of lack of operations | 5 | 5 | 5 | 5 | Excellent |
| Dimension "compliance" may include the following metrics to evaluate the system: Recognition of execution patterns | 5 | 4 | 5 | 5 | High |
| Dimension "compliance" may include the following metrics to evaluate the system: Ascertainment of fulfilling of rules | 5 | 4 | 5 | 5 | High |
| Dimension "compliance" may include the following metrics to evaluate the system: Detection of potential errors | 5 | 5 | 5 | 5 | Excellent |
| Dimension "compliance" may include the following metrics to evaluate the system: Verification of compliance of existing policies | 5 | 4,5 | 5 | 5 | High |
| Dimension "estimation" may include the following metrics to evaluate the system: Estimation of possible risks | 5 | 4,5 | 5 | 5 | High |
| Dimension "estimation" may include the following metrics to evaluate the system: Determination of possible execution patterns which are likely to be followed | 5 | 4,5 | 5 | 5 | High |
| Regarding a model for implementing continuous assurance services in information systems: The inclusion of the requirement "reporting" is essential | 5 | 5 | 5 | 5 | Excellent |
| The requirement "reporting" may include the following specificities: Real-time presentation of the executed operations which were monitored | 5 | 5 | 5 | 5 | Excellent |
| The requirement "reporting" may include the following specificities: Real-time presentation of execution patterns which are being followed or are likely to be followed | 5 | 5 | 5 | 5 | Excellent |
| The requirement "reporting" may include the following specificities: Real-time presentation of the compliance verification in transactions executions | 5 | 5 | 5 | 5 | Excellent |
| The requirement "reporting" may include the following specificities: Real-time presentation of the risk estimated on determining possible execution patterns | 5 | 4 | 5 | 5 | High |
| The requirement "reporting" may include the following specificities: Real-time alert for irregular situations in monitoring, compliance verification and estimation of negative results | 5 | 5 | 5 | 5 | Excellent |

Table 30 - Statistical data from answers for Part II of questionnaire (2nd iteration)

| Statements | Mode | Percentiles | | | Consensus |
|--|------|-------------|----|----|-----------|
| | | 25 | 50 | 75 | |
| Regarding a model for implementing continuous assurance services in information systems, the inclusion of dimensions is essential for evaluating. The ability of the system to monitor transactions which are intended to be audited (Dimension Monitoring) | 5 | 5 | 5 | 5 | Excellent |
| Regarding a model for implementing continuous assurance services in information systems, the inclusion of dimensions is essential for evaluating. The ability of the system to verify conformity and integrity with which transactions are executed (Dimension Compliance) | 5 | 5 | 5 | 5 | Excellent |
| Regarding a model for implementing continuous assurance services in information systems, the inclusion of dimensions is essential for evaluating. The ability of the system to estimate assurance, coherence and consistency of transactions which are being executed (Dimension Estimation) | 5 | 4,5 | 5 | 5 | High |
| Dimension "monitoring" may include the following metrics to evaluate the system: Real-time monitoring of operations | 5 | 5 | 5 | 5 | Excellent |
| Dimension "monitoring" may include the following metrics to evaluate the system: Real-time identification of irregular operations (e.g. poorly executed operations, incongruities, etc) | 5 | 5 | 5 | 5 | Excellent |
| Dimension "monitoring" may include the following metrics to evaluate the system: Real-time verification of the processing of required operations at all previous steps | 5 | 4,5 | 5 | 5 | High |
| Dimension "monitoring" may include the following metrics to evaluate the system: Real-time detection of lack of operations | 5 | 5 | 5 | 5 | Excellent |
| Dimension "compliance" may include the following metrics to evaluate the system: Recognition of execution patterns | 5 | 4 | 5 | 5 | High |
| Dimension "compliance" may include the following metrics to evaluate the system: Ascertainning of fulfilling of rules | 5 | 4 | 5 | 5 | High |
| Dimension "compliance" may include the following metrics to evaluate the system: Detection of potential errors | 5 | 5 | 5 | 5 | Excellent |
| Dimension "compliance" may include the following metrics to evaluate the system: Verification of compliance of existing policies | 5 | 4,5 | 5 | 5 | High |
| Dimension "estimation" may include the following metrics to evaluate the system: Estimation of possible risks | 5 | 4,5 | 5 | 5 | High |
| Dimension "estimation" may include the following metrics to evaluate the system: Determination of possible execution patterns which are likely to be followed | 5 | 4,5 | 5 | 5 | High |
| Regarding a model for implementing continuous assurance services in information systems: The inclusion of the requirement "reporting" is essential | 5 | 5 | 5 | 5 | Excellent |
| The requirement "reporting" may include the following specificities: Real-time presentation of the executed operations which were monitored | 5 | 5 | 5 | 5 | Excellent |
| The requirement "reporting" may include the following specificities: Real-time presentation of execution patterns which are being followed or are likely to be followed | 5 | 5 | 5 | 5 | Excellent |
| The requirement "reporting" may include the following specificities: Real-time presentation of the compliance verification in transactions executions | 5 | 5 | 5 | 5 | Excellent |
| The requirement "reporting" may include the following specificities: Real-time presentation of the risk estimated on determining possible execution patterns | 5 | 4 | 5 | 5 | High |
| The requirement "reporting" may include the following specificities: Real-time alert for irregular situations in monitoring, compliance verification and estimation of negative results | 5 | 5 | 5 | 5 | Excellent |