BABEŞ-BOLYAI UNIVERSITY CLUJ-NAPOCA
FACULTY OF ECONOMICS AND BUSINESS ADMINISTRATION
BUSINESS INFORMATION SYSTEMS DEPARTMENT

IT INFRASTRUCTURE AUDIT USING ARTIFICIAL INTELIGENCE

~ Summary ~

Scientific advisor: PHD Professor Nicolae Tomai
PhD. Student Ana-Maria Ghiran (Mureşan)

2011

Abstract

IT Infrastructure has spread across all economic processes. The IT Infrastructure Audit, therefore, becomes a necessity in order to assess and also to significantly improve the performance of the business processes. The subject chosen for the current dissertation is of high importance, both for practical and theoretical study and can open numerous applicative and research opportunities. This work intends to divert the auditors' focus (and especially in case of Romanian auditors) towards the need in changing the way auditing is done, from manual techniques to continuous ones, and in changing the object of evaluation, from a financial preponderant audit to an IT audit. Therefore, (as theoretical contributions) we have studied the current approaches in automation the IT audit process, and we have presented our findings in order to facilitate their practical implementation. Our proposed new model and the prototype developed based on it are meant to be practical contributions.

Keywords: *IT Audit, Continuous Audit, Audit standards, Intelligent Agents, Knowledge Formalization, Ontologies*

Summary

1 Introduction

1.1 Preliminaries

The role of auditors is increasingly significant inside an organization in supporting the decisional process.

The auditor will evaluate the controls implemented by managers and will issue a report. If the role of the manager is to ensure the application of controls, the auditor will assure about the way the controls are implemented, if they are efficient and correspond to the purpose for which they have been defined [Gallegos 2008].

World wide, the audit concept is evolving towards continuous audit and IT audit.

As the current users expectations that information would be available in real time are growing, and (not necessarily of financial nature) there will be more and more implementations for the continuous audit concept.

If continuous audit will change the way of conducting an audit but, on the other hand, as the managerial decisions are increasingly supported by technology, the object of evaluation is evolving towards the IT audit (not only *how* but also *what* to audit will change).

Most organizations are dependent on technology, and especially on the risks associated with it. This implies that companies not only need to have control over the IT infrastructure but also to prove it, often through an audit report.

In some countries, this is a strong recommendation in achieving IT Governance, part of Corporate Governance or it is even a legal requirement for public companies, like the Sarbanes Oxley Act[sox 2002] or the Health Insurance Portability and Accountability Act [hip 1996]. Similar legislation regarding data and information protection has been adopted in many countries world wide (including Romania).

IT has gained its own discipline in audit being met under different names: Electronic Data Processing Audit - EDP Audit, Computer Information System Audit - CIS Audit, Information Technology Audit - IT Audit. Initially, it was used only to verify how the financial data was processed over time, but now, IT audit area has expanded to include scrutiny about how all sensitive data is processed, stored and communicated. Progressively, the audit span has enlarged and now includes evaluation of data, applications and infrastructure.

1.2 Problem Statement

Currently, because of the increasing IT support inside an organization, auditors need to evaluate the whole system in order to issue opinions regarding the correctness of data delivered by a certain system.

Efficiency and effectiveness of a process (IT, management or audit process) are generally measured using the following metrics:

- time needed to fulfill the process
- the execution cost
- quality or percentage of correct execution

In order to get good results for these metrics, business processes in general and the IT ones in particular, demanded the use of technology, which in turn, required technology again for their management („using technology to manage technology" [ibm 2006]). Eliminating the manual procedures from the IT management processes, consequently, called for the use of technology in performing the IT audit.

Currently there are few solutions to perform an audit in an autonomous manner or with little human intervention and therefore we consider that this is a problem that needs attention. *Developing such a solution could have a remarkable practical value.*

Through eliminating the manual procedures, process efficiency is increased and inaccuracy is avoided. More, in case of traditional implementation of audit, process repeatability was hardly taken into account but, on the other hand, in a technology based audit that would be low cost and easy to do.

Using traditional (manual) techniques in IT audit makes process reusability difficult and real time assurance impossible.

Firstly, in order to automate the audit process, it was considered eliminating the monotonous and laborious tasks and auditors started to use the so called "Computer Assisted Audit Tools" – CAATs. These are different depending on the type of audit performed. CAATs are defined as any tool or method involving use of computers and which allows auditors to increase productivity in carrying out their work [Gallegos 2008]. The definition is very broad and can include from simple text editors to expert systems,

from simple methods that only show data to complex methods for checking multiple correlations. [Gallegos 2008].

Currently, the audit tools need not only to support the audit process but to actually perform the most of it („Use technology to actually audit as opposed to using technology to automate manual auditing procedures" comment of auditors from Big Four group cited in [Searcy 2003]).

Even if there are already solutions that have been used by all big audit companies for evaluation of risks, controls or for general audit, many of these are created on proprietary formats. Therefore, their approaches have not been under scientific review and could hide certain errors. Also, because of this confidentiality combining advantages from various methods is difficult to achieve. *We can state that scientific efforts are needed in this area as well.*

After analyzing some of the methods currently used in order to automatically generate the audit results, we have found that they perform compliance tests against a model considered good or benchmarking tests.

Our approach differs from others in the field and described in Chapter 3 because it will enable conducting an audit much closer to reality as it will be individually conceived: a preliminary analysis would determine risk level, which can be used to build customized model against which the test is performed. Thus our approach brings a qualitative improvement to audit results because they were generated for each particularly situation and also fits the general pattern of audit.

1.3 Our objectives

Our main objectives for this dissertation is that starting with a general model for audit to develop an architecture for continuous IT audit and a prototype based on it. For the design and implementation we intend to use "state of the art" methods and technologies in the field.

We propose to overcome the limitations identified in the previous section in the following ways:

(i) by delegating auditing tasks to intelligent agents. We strive to improve the efficiency and to minimize the inconsistency or inaccuracy which may occur due to subjective human judgments or potential errors. Using intelligent agents we can deliver almost real time assurance,

(ii) by using ontology based semantic description of auditor's knowledge. As expert knowledge is captured and formalized explicitly, process reusability is enhanced

(iii) by applying automated reasoning techniques. New knowledge can be generated through deduction.

Starting from the requirements of IT auditors we intend to develop a prototype that can verify compliance with functional and non-functional requirements that are given by certain codes of good practice and expressed in abstract terms. For this, we propose a general architecture of the audit process, we provide a way of describing the knowledge of auditors in an ontology and a concrete example.

1.4 Motivations

The motivations that drove us in our research for this dissertation can be divided into research motivations and approach motivations.

Research motivations are consequences from the problem statement, namely the need to find a solution that will make a small contribution to automation of an IT audit process.

The reasons for choosing our approach result from the advantages offered by these methodologies and techniques, which enable much of the requirements of the proposed model. Thus we have identified: reasons for choosing multi-agent systems, reasons for choosing ontology and motivations for choosing.

A multi-agent system allows integration of multiple knowledge sources. Also using intelligent agents will lead to increased efficiency in the audit process by eliminating possible human errors and obtaining the same results in a much shorter time. It will get a near real-time evaluation.

An important part of the prototype proposed in this paper is the formalization of an auditor's expertise so that his knowledge can be kept separately from the implementation and reused later. This can be easily made using ontologies that allow separation of knowledge from its processing.

The knowledge described in an ontology should include many concepts and heuristics used by auditors and for its construction can collaborate more experts. For this reason, it is necessary to check the correctness of ontology. OWL-DL ontologies can be translated into a Descriptive Logic representation and in this way it is possible to achieve automated reasoning over the ontology using a Description Logic reasoner. Such an engine will perform various tasks such as deduction of superclasses, subclasses, and can determine if a class is consistent.

1.5 Thesis Structure

The dissertation evolves as follows: In the first chapter we have shortly introduced the audit concept and which are the actual trends. We have identified the changes towards the evaluation object in audit (IT audit) but also the way it must be performed in present conditions (continuous/automated).

Based on these new audit requirements, we have shown the need for new approaches, which are the objectives that we have set to accomplish in this work and which are research motivations and the reasons that led us to choose methods and technologies used for implementation.

The thesis is divided into two major parts: the first part will address the current state in the fields and will describe in more details continuous IT auditing, the methods currently used and the concepts and technologies necessary for our approach; the second part will focus on presenting the contributions: an architecture for our own IT audit model and a case study by implementing a prototype for firewall audit.

Chapter 2 Continuous IT Audit

2.1 Concepts definitions

2.1.1 IT Audit

2.1.2 Continuous Audit

2.1.3 Audit relationship with management

2.1.4 Audit, Corporate Governance, IT Governance

2.2 IT Risk

2.2.1 Risk analysis

2.2.2 Risk treatment

2.3 IT Control

2.3.1 Control frameworks

2.3.2 Information security controls and security models

In this chapter we tried to clarify the concepts related to the continuous IT auditing and its two major components. First, we presented what is meant by IT audit, information system audit. I adapted one of the definitions to clarify the scope to which we refer in this work, namely IT infrastructure audit. Next we showed the important role that audit plays within an organization first as a tool to support management activities by providing advice and second to offer general assurance for third parties regarding the manner in which the management follows the principles of corporate governance.

To perform an audit process one will assess the effectiveness of controls implemented by managers. For this, it is important to know the risks that controls must manage. Thus, auditors will perform tasks similar to those of managers but separately: determining the risk level for each item being audited and then identifying appropriate controls for risk treatment. In the chapter were detailed methods for risk analysis (both qualitative and quantitative) and risk treatment (reduction, elimination or acceptance) and frameworks used to implement an internal control system. We emphasized IT risk and IT control.

Chapter 3 Current methodologies for Continuous IT Audit

3.1 Vulnerabilities assessment

3.2 Penetration tests

3.3 Tools used by auditors

3.4 Current audit process particularities

3.5 Current approaches in order to automate the IT audit process

3.5.1 SCAP - Security Content Automation Protocol

3.5.2 CAPEC - Common Attack Pattern Enumeration and Classification

In Chapter 3 we intended to describe the existing approaches the IT audit field both those already tested in practice and those found in literature which are rather recommendations. The most common methods found in IT audit practice are vulnerabilities assessment and penetration tests. They determine the level of risk on each item under evaluation and the existence of countermeasures designed to mitigate it. Regarding the tools used by IT auditors, generally are the same as those used by system managers. Theoretical research offers audit recommendations that relate to standardization and formalization of vulnerabilities descriptions, providing them as nomenclatures and as publicly available database. The predominant aspect that theoretical research is concerned about refers to security.

Chapter 4 Methodologies used in our approach

4.1 Management information systems

4.1.1 Existing implementations

4.1.2 Towards the process automation

4.2 Knowledge formalization

4.2.1 Ontology concept

4.2.2 Ontologies description languages

4.2.3 Ontology Building

4.2.4 Ontology Instantiation

4.2.5 Ontology Reasoning

4.3 Agents and multi-agent systems

4.3.1 JADE Platform

4.3.2 Agent creation

4.3.3 Agent Behaviour

4.3.4 Agent Communication

Chapter 4 is describing the technologies used in our approach. First we examined information management systems to identify the most effective option for retrieving the information from evaluated elements. The choice of methods used in our approach has been done considering their full integration, to achieve maximum functionality, to make use of their most advantages and which have proven to be the most effective: formalized ontologies to describe knowledge, reasoning engines in order to generate new knowledge, multi agent systems for distributing tasks and information and, not in the least information management systems.

Chapter 5 General Proposed Architecture

5.1 Conceptual Model

5.1.1 Human Users Level

5.1.2 MAS Level

5.1.3 Managed Device Level

5.1.4 Managed Resource Level

5.2 System functionality

In Chapter 5 we described a model for the general audit process and a multi-layer architecture for implementing this model using a multi agent system. Next, the four levels of architecture (the human user level, the MAS level, the managed device level, the managed resources level) were described through detailed use cases. Then we proceeded to explain the functionality of the system.

Chapter 6 Case study

6.1 Firewall audit problem

6.1.1 Particularities in firewall configuration evaluation

6.1.2 Conflicts in firewall security policy

6.1.3 Conflicts in different firewall security policies

6.2 Ontology modeling for firwwall domain knowledge representation

6.3 System detailed design

6.3.1 System initialization

6.3.2 Gathering the initial data

6.3.3 Displaying the user interface

6.3.4 Gathering user data

6.3.5 Risk level evaluation

6.3.6 Evaluation of implemented controls

The last chapter is a case study of IT audit using the proposed architecture. We have shown the reasons for auditing a firewall: its evaluation covers both the situation of a simple element but also when it is a control for other elements. Further, we described the characteristics and challenges encountered in assessing firewalls and how these are treated in the present research. The issue of conflicts in the firewall policy has been discussed extensively in theoretical research, but very few approaches are using ontological descriptions because of the particular way to express access rules in a firewall policy. Briefly, we gave an example of how firewall domain knowledge can be modeled in an ontology for assessing the rules of security policy and applying reasoning to identify potential conflicts. We hope we were able to show what differentiates our approach from others.

Conclusions

Throughout this work we tried to demonstrate the applicability of intelligent agents for IT infrastructure audit to automate the process and eliminate the human intervention as much as possible.

The theme was selected with the belief that the transition to an automated approach in achieving the audit process is a clear necessity of the moment.

The audit has slowly moving from a completely practitioners' concern into a research domain, with an increasingly interest of the educational field.

There is a need for identifying new methods that could facilitate an objective, real time and cost-effective assurance.

Prototype is developed using JADE platform, which is most often used for multi-agent systems. Knowledge of agents is stored in OWL ontologies can thus be built

separately from the implementation of agents. These ontologies will allow the translation from the human user requirements (which are expressed in abstract language) in concrete terms that an agent can understand. Also, ontologies are necessary to achieve the reverse operation, to return the result.

Agents can access information directly through OWL ontology API - which allows add new knowledge in ontology (agents will need to build their own model of reality). The agents can use an inference engine that will allow them to reason on knowledge.

In order to extract information from the managed network elements we used SNMP protocol, which is still the most common. SNMP offers a simple method to access information about a certain managed device or even to modify it, implementing a reduced number of commands. As the scope of this work does not reside on device information management and we need only a simple way to extract auditing information from managed devices, we will use SNMP, because its simplicity and its compliance with new devices as well as legacy systems. Most major network equipment providers offer simultaneously the possibility to access management information through more advanced protocols such as those based on Web services (WS-Management). For example, Microsoft provides both SNMP and WMI service - Windows Management Instrumentation, for managing Windows systems. As perspectives we would consider the changes in adoption of other network management protocols.

Finally, we can state that the evolution of current technology allows their embracing to areas previously considered human specific, such as carrying out audits.

7.1 Personal contributions

The thesis “IT Infrastructure Audit using Artificial Intelligence” presents the results of the research in multiple interdisciplinary domains.

A short list with the thesis contributions can include:

- development of some synthesis for IT audit field and for methodologies used in our approach
- proposal of a generic model for the IT audit process

- development of an architecture with multiple layers of a multi agent system for the proposed model
- presentation in details of how a platform for multi agent systems like JADE can be implemented in order to automate the described IT audit process
- we have shown how the auditors' knowledge can be described through ontologies
- we have presented a case study which implements the proposed model

7.2 Future research plans

Considering the content of this thesis, we can state that researches for the proposed directions are only at the beginning and we are planning for future improvements and developments:

- development of multiple agent types in order to include a comprehensive list of auditors' tasks.
- a better assimilation of public services for vulnerabilities and threats description
- integration with multiple information management services like those based on web services.
- researches of implications and influences in a mobile environment or in cloud computing.
- integration of some security mechanisms into the prototype.

7.3 Thesis publications

The proposed approach for this dissertation has first been discussed during the PHD Symposium collocated with European Semantic Web Conference ESWC in 2006.

The main contributions of the thesis have been disseminated with the BIS Conference presentations in 2009 [Ghiran 2009], and respectively in 2011 [Ghiran 2011], both with proceedings in Lecture Notes in Business Information Processing, the special edition of Springer dedicated for results in area of Economic Informatics.

1) [Ghiran 2009] **Ghiran (Mureşan) Ana-Maria,** Silaghi Gheorghe-Cosmin, Tomai Nicolae**,** *Ontology-Based Tools for Automating Integration and Validation of Firewall*

http://www.springerlink.com/content/p124578166010p14/?p=fd586ab81f154fe4bab507e706fdb65e&pi=4

In this article, we have shown a considerable part of our case study, how conflicts can be identified inside the security policies from a firewall using automated reasoning capabilities over the ontological descriptions of domain knowledge.

2) [Ghiran 2011] **Ghiran (Mureşan) Ana Maria,** Silaghi Gheorghe-Cosmin, Tomai Nicolae**,** *Deploying an Agent Platform to Automate the IT Infrastructure Auditing Process*, in Business Information Systems 14th International Conference, BIS 2011, Poznan, Poland, Proceedings, Springer Berlin Heidelberg, Editor: Witold Abramowicz

The paper presents the general model proposed to achieve automated IT audit process and multi-layer architecture based on a multi-agent system. Also, it includes an introductory description of how a multi-agent platform such as JADE can be deployed to achieve the proposed architecture.

Besides these publications, the research conducted during the Phd studies has been materialized with the following articles:

3) [Ghiran 2010a] **Ghiran (Mureşan) Ana-Maria –** Network Management Framework Based on Intelligent Agents, Semantic Modeling and Web Services, The Second Romanian Workshop on Mobile Business, Cluj-Napoca, 2010, Economy Informatics, Vol. 10, No1/2010

In this article we presented a model and architecture that formed the base of our approach and led to the design and architecture of the current model detailed in an article disseminated this year.

4) [Ghiran 2010b] **Ghiran (Mureşan) Ana-Maria** – Semantic Modeling for Autonomic Network Management, The Second International Conference Software, Services and Semantic Technologies,Varna, Bulgaria, 2010, ISBN 978-954-9526-71-4

The paper presents the requirements for performing an autonomous network management, and the possibilities of formalizing knowledge through ontologies.

5) [Ghiran 2007] **Ghiran (Muresan) Ana-Maria**, Monica Vancea – Risk Identification Method based on Ontology, in Proceedings of the International Conference Competitiveness and European Integration, 2007,Ed. Risoprint,ISBN 978-973-751-597-1
This study refers to the evaluation of the opportunity for using ontologies in identifying risks.

7.4 Complete list of research papers

1. Tomai Nicolae, **Muresan Ana-Maria** - Agent Technology in Wireless Networks, InfoBusiness 2006 – The International Conference on Business Information Systems, Ed. Universităţii Al. Ioan Cuza, Iaşi, ISBN: 978-973-703-207-2
2. Tomai Nicolae, **Mureşan Ana-Maria** – Cooperative Agents in Mobile Ad-Hoc Networks, Annals of the Tiberiu Popoviciu Seminar of Functional Equations Approximation and Convexity, Vol. 4, 2006, Mediamira Science Publisher, Cluj-Napoca, ISSN 1584-4536
3. **Mureşan Ana-Maria** – Intelligent Agents for Collaborative Work, Annals of the Tiberiu Popoviciu Seminar of Functional Equations Approximation and Convexity, Vol. 4, 2006, Mediamira Science Publisher, Cluj-Napoca, ISSN 1584-4536
4. **Mureşan Ana-Maria** – Technology Issues in Adopting Continuous Audit, Informatics in Knowledge Society, The Proceedings of the Eight International Conference on Informatics in Economy, may 2007, Ed. Economică, ISBN 978-973-594-921-1
5. Tomai Nicolae, **Muresan Ana-Maria**, Mican Daniel – Wireless Network Design Considerations, in Proceedings of KEPT 2007, Knowledge Engineering Principles and Techniques, Cluj University Press, ISBN: 978-973-610-567-8
6. **Ghiran (Muresan) Ana-Maria**, Monica Vancea – Risk Identification Method based on Ontology, in Proceedings of the International Conference Competitiveness and European Integration, 2007, Ed. Risoprint, ISBN 978-973-751-597-1
7. Mican Daniel, Bologa Cristian Sorin**, Ghiran (Mureşan) Ana-Maria,** Optimized Advertising Content Delivery, Annals Of The Tiberiu Popoviciu Seminar Of Functional Equations, Approximation And Convexity, Categ CNCSIS C, 6/1, 2008, P.230 - 240
8. **Ghiran (Mureşan) Ana-Maria,** Mican Daniel – Firewalls on Mobile Devices, The Ninth International Conference on Informatics in Economy, 2009, Ed. Economica, ASE, ISBN 978-606-505-178-2

9. **Ghiran (Mureşan) Ana-Maria,** Silaghi Gheorghe-Cosmin, Tomai Nicolae**,** *Ontology-Based Tools for Automating Integration and Validation of Firewall Rules*, Business Information Systems 12th International Conference, BIS 2009, Poznan, Poland, 27-29 April, Proceedings, Springer Berlin Heidelberg, Editor: Witold Abramowicz, 978-3-642-01189-4, http://www.springerlink.com/content/p124578166010p14/?p=fd586ab81f154fe4bab507e706fdb65e&pi=4
10. **Ghiran (Mureşan) Ana-Maria** – Semantic Modeling for Autonomic Network Management, The Second International Conference Software, Services and Semantic Technologies,Varna, Bulgaria, 2010, ISBN 978-954-9526-71-4
11. **Ghiran (Mureşan) Ana-Maria –** Network Management Framework Based on Intelligent Agents, Semantic Modeling and Web Services, The Second Romanian Workshop on Mobile Business, Cluj-Napoca, 2010, Economy Informatics, Vol. 10, No1/2010
12. **Ghiran (Mureşan) Ana Maria,** Silaghi Gheorghe-Cosmin, Tomai Nicolae**,** *Deploying an Agent Platform to Automate the IT Infrastructure Auditing Process*, in Business Information Systems 14th International Conference, BIS 2011, Poznan, Poland, Proceedings, Springer Berlin Heidelberg, Editor: Witold Abramowicz
13. Breşfelean Vasile Paul, **Ghiran (Mureşan) Ana-Maria** Ontology Importance towards Enhancing Suggestions in a News Recommender System for a Financial Investor, to appear in Metadata and Semantics Research Conference Proceedings, MTSR 2011, Iymir, Turkey, Proceedings, Springer Berlin Heidelberg

Bibliography

[1] [Andone 2005] Ioan Andone. Ontologiile şi modelarea informațională a întreprinderii. Analele Ştiințifice ale Universitatii "Al.I.Cuza", Secțiunea Ştiințe Economice, nr. 26, 2005. 83

[2] [Barnum 2010] Sean Barnum. Common Attack Pattern Enumeration and Classifcation CAPEC Schema Description. 2010. 69

[3] [Bellifemine 2007] Fabio Luigi Bellifemine, Giovanni Caire and Dominic Greenwood. Developing multi-agent systems with jade. Wiley, 2007. 100, 102, 103, 106, 107, 109

[4] [Bellifemine 2008a] Fabio Bellifemine, Giovanni Caire, Agostino Poggi and Giovanni Rimassa. JADE: A software framework for developing multi-agent applications. Lessons learned. Inf. Softw. Technol., vol. 50, pages 10-21, January 2008. 100

[5] [Bellifemine 2008b] Fabio Luigi Bellifemine, Giovanni Caire and Tiziana Trucco. Jade programmer's guide. Jade Documentation, 2008. 100, 101, 102, 103, 104, 105, 106, 107, 108, 110, 111, 170

[6] [Borst 1997] Willem Nico Borst. Construction of Engineering Ontologies for knowledge sharing and reuse. PhD thesis, University of Twente, Enschede, 1997. 82

[7] [Boutaba 2002] Raouf Boutaba and Jin Xiao. Network Management: State of the Art. In Communication Systems: The State of the Art (IFIP World Computer Congress)'02, pages 127-146, 2002. 74, 76

[8] [Buraga 2004] Sabin Corneliu Buraga. Semantic web, fundamente şi aplicatii. Matrix ROM, Bucureşti, 2004. 86

[9] [Burtescu 2004] Emil Burtescu. Securitatea datelor în sisteme informatice. Teza de doctorat, 2004. 28

[10] [Caire 2009] Giovanni Caire. Jade tutorial, jade programming for beginners. Jade Documentation, 2009. 101, 102, 104, 106, 109

[11] [Cis 2003] Internetworking technologies handbook, forth edition. Cisco Press, 2003. 74

[12] [Clark 2003] David D. Clark, Craig Partridge, J. Christopher Ramming and John T. Wroclawski. A knowledge plane for the internet. In Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications, SIGCOMM '03, pages 3-10, New York, NY, USA, 2003. ACM. 79, 81

[13] [Cob 2007] Cobit 4.1, versiunea în limba română. IT Governance Institute, 2007. vii, 21, 36, 37

[14] [Coderre 2005] David Coderre. Global technology audit guide, continuous auditing: Implications for assurance, monitoring and risk assessment. The Institute of Internal Auditors, 2005. vii, 2, 17, 18, 19

[15] [Damianou 2001] Nicodemos Damianou, Naranker Dulay, Emil Lupu and Morris Sloman. The Ponder Policy Specifcation Language. In Lecture Notes in Computer Science, pages 18-38. Springer-Verlag, 2001. 75

[16] [Davies 2006] John Davies, Rudi Studer and Paul Warren. Semantic web technologies: Trends and research in ontology-based systems. John Wiley & Sons, 2006. 82, 89, 91

[17] [Derbel 2009] Hajer Derbel, Nazim Agoulmine and Mikael Salaln. ANEMA: Autonomic network management architecture to support self-confguration and self-optimization in IP networks. Computer Networks, vol. 53, no. 3, pages 418 -430, 2009. 80, 81

[18] [Dobson 2006] Simon Dobson, Spyros Denazis, Antonio Fernandez, Dominique Gaiti, Erol Gelenbe, Fabio Massacci, Paddy Nixon, Fabrice Safre, Nikita Schmidt and Franco Zambonelli. A survey of autonomic communications. ACM Trans. Auton. Adapt. Syst., vol. 1, pages 223-259, December 2006. 81

[19] [Domingue 2009] John Domingue and Dieter Fensel. Problem solving methods in a global networked age. Artif. Intell. Eng. Des. Anal. Manuf., vol. 23, pages 373-390, 2009. 77

[20] [Gallegos 2008] Frederick Gallegos and Sandra Senft. Information technology control and audit, third edition. Auerbach Publications, 2008. 1, 5

[21] [Gavalas 2000] Damianos Gavalas, Dominic Greenwood, Mohammed Ghanbari and Mike OMahony. Advanced Network Monitoring Applications Based on Mobile/Intelligent Agent Technology. Computer Communications Journal, vol. 23, pages 720-730, 2000. 77

[22] [Gavalas 2009] Damianos Gavalas, George E. Tsekouras and Christos Anagnostopoulos. A mobile agent platform for distributed network and systems management. J. Syst. Softw., vol. 82, pages 355-371, February 2009. 76, 77, 132

[23] [Gheorghe 2006] Mirela Gheorghe. Guvernanța IT -Cheia optimizării unei afaceri. The Journal of the Faculty of Economics -Economic Science Series, vol. II, pages 1104-1107, 2006. 23

[24] [Ghiran 2009] Ana-Maria Ghiran, Gheorghe Cosmin Silaghi and Nicolae Tomai. Ontology-Based Tools for Automating Integration and Validation of Firewall Rules. In BIS'09, pages 37-48, 2009. vii, 10, 122, 146, 148, 153, 155

[25] [Ghiran 2010] Ana-Maria Ghiran. Semantic Modeling for Autonomic Network Management. In Proceedings of The Second International Conference on Software, Services and Semantic Technologies, S3T Conference, pages 15-26, 2010. 78, 122

[26] [Ghiran 2011] Ana-Maria Ghiran, Gheorghe Cosmin Silaghi and Nicolae Tomai. Deploying an Agent Platform to Automate the IT Infrastructure Auditing Process. In to appear in BIS'11, 2011. vii, 10, 121, 122, 123, 125, 126, 127, 128, 130, 131, 133, 137, 168

[27] [Ghita 2009] Marcel Ghiță, Cornelia Nicolau, Zaharica Florea-Ianc, Ion Peres, Ovidiu Constantin Bunget and Cristian Elian Peres. Guvernanța corporativă şi auditul intern. Editura Mirton, 2009. 21, 22, 35, 36

[28] [Gouda 2007] Mohamed G. Gouda and Alex X. Liu. Structured firewall design. Computer Networks Journal, vol. 51, 2007. 147, 151, 152

[29] [Gruber 1993] Thomas R. Gruber. A translation approach to portable ontology specifcations. Knowl. Acquis., vol. 5, pages 199-220, June 1993. 82

[30] [GTA 2005] Global technology audit guide, information technology controls. The Institute of Internal Auditors, 2005. vii, 33, 36

[31] [Hamed 2006] Hazem Hamed and Ehab Al-shaer. Taxonomy of conficts in network security policies. In In IEEE Communications Magazine, pages 134-141, 2006. 147, 148, 151

[32] [Hebeler 2009] John Hebeler, Matthew Fisher, Ryan Blace, Andrew Perez Lopez and Mike Dean. Semantic web programming. John Wiley & Sons Inc., Chichester, West Sussex, Hoboken, NJ, 2009. 83

[33] [Hill 2003] Ernest Friedman Hill. Jess in action: Java rule-based systems. Manning Publications Co., Greenwich, CT, USA, 2003. 98

[34] [Hillson 2002] David Hillson. Extending the risk process to manage opportunities. International Journal of Project Management, vol. 20, no. 3, pages 235 -240, 2002. 24

[35] [hip 1996] The health insurance portability and accountability act. U.S. Government Printing Ofce, 1996. http://www.hipaa.org. 3

[36] [Horridge 2007] Matthew Horridge, Simon Jupp, Georgina Moulton, Alan Rector, Robert Stevens and Chris Wroe. A practical guide to building owl ontologies using protege 4 and co-ode tools, edition 1.1, technical report. The University of Manchester, 2007. 95, 96

[37] [Horrocks 2004] Ian Horrocks, Peter F. Patel-Schneider, Harold Boley, Said Tabet, Benjamin Grosof and Mike Dean. Swrl: A semantic web rule language combining owl and ruleml. W3C Member Submission, 2004. 96, 97

[38] [ibm 2006] An Architectural Blueprint for Autonomic Computing. IBM Autonomic Computing White Paper. June 2006. 4, 80, 81

[39] [ITG 2003] Board briefng on it governance, second edition. IT Governance Institute, 2003. 23

[40] [Jennings 2007] B. Jennings, S. van der Meer, S. Balasubramaniam, D. Botvich, M. O Foghlu, W. Donnelly and J. Strassner. Towards autonomic management of communications networks. Communications Magazine, IEEE, vol. 45, issue 10, pages 112-121, 2007. 79, 80, 81

[41] [Kephart 2007] Jefrey O. Kephart and Rajarshi Das. Achieving Self-Management via Utility Functions. IEEE Internet Computing, vol. 11, pages 40-48, January 2007. 81

[42] [MartinFlatin 1999] Jean-Philippe Martin-Flatin, Simon Znaty and Jean-Pierre Hubaux. A Survey of Distributed Enterprise Network andSystems Management Paradigms. J. Netw. Syst. Manage., vol. 7, pages 9-26, March 1999. 7, 75

[43] [Martin 2008] R.A. Martin. Making security measurable and manageable. In Military Communications Conference, 2008. MILCOM 2008. IEEE, pages 1 -9, nov. 2008. 58, 59

[44] [Mell 2007] Peter Mell, Karen Scarfone and Sasha Romanosky. Cvss a complete guide to the common vulnerability scoring system, version 2.0. FIRST Forum of Incident Response and Security Teams, 2007. http://www.frst.org/cvss/cvss-guide.pdf. 66, 67, 68

[45] [Moeller 2010] Rober Moeller. It audit, control and security. John Wiley and Sons Inc, 2010. 37, 45

[46] [Munteanu 2001] Adrian Munteanu. Auditul sistemelor informationale contabile cadru general. Editura Polirom, 2001. 26, 28, 31

[47] [Munteanu 2005] Adrian Munteanu and Doina Fotache. Auditing Integrated Systems A Romanian Approach. In Proceedings of the International Workshop on Collaborative Support Systems in Business and Education. Risoprint, 2005. 2

[48] [Nastase 2007] Pavel Nastase, Victoria Stanciu and Ali Eden. Auditul şi controlul sistemelor informationale. Editura Economica, 2007. 15, 16, 19, 23

[49] [Nikraz 2006] Magid Nikraz, Giovanni Caire and Parisa A. Bahri. A methodology for the development of multi-agent systems using the JADE platform. Comput. Syst. Sci. Eng., vol. 21, no. 2, 2006. 7

[50] [Noy 2001] Natalya F. Noy and Deborah L. McGuinness. Ontology Development 101: A Guide to Creating Your First Ontology. Rapport technique, Stanford Knowledge Systems Laboratory and Stanford Medical Informatics, 2001. 83, 84

[51] [Oprean 2002] Dumitru Oprean. Audit. Presa Universitara Clujeana, 2002. 1

[52] [Ova 2006] Introduction to oval language, version 5. MITRE Corporation, 2006. 63, 64

[53] [Ozier 2004] Will Ozier. Risk analysis and assessment, information security management handbook. Auerbach Publications, 2004. 24

[54] [Pranothi 2010] N. Pranothi and R. Hemavathy. A Survey of Network Device Configuration Audit Tools. Int. J. of Advanced Networking and Applications, vol. 02, issue 02, pages 532-538, 2010. 56, 58

[55] [Puliafto 2000] Antonio Puliafto and Orazio Tomarchio. Using Mobile Agents to implement flexible Network Management strategies. Computer Communication Journal, vol. 23, pages 708-719, 2000. 77

[56] [Quinn 2009] Stephen Quinn, David Waltermire, Christopher Johnson, Karren Scarfone and John Banghart. The technical specification for the security content automation protocol (scap), scap version

[57] NIST, 2009. http://csrc.nist.gov/publications/nistpubs/800-126/sp800-126.pdf. 47, 61, 62, 64, 65

[58] [Rogers 2008] Russ Rogers. Nessus network auditing, second edition. Syngress Publishing, 2 edition, 2008. 48, 52, 54, 55, 57

[59] [Rothke 2004] Ben Rothke. How to perform a security review of a check-point firewall information security management handbook. Auerbach Publications, 2004. 142, 143, 144

[60] [Rughiniş 2010] Răzvan Rughiniş, Răzvan Deaconescu, Andrei Ciorba and Bogdan Doinea. Retele locale. Ed Printech, 2010. 25, 55

[61] [Scarfone 2009] Karen Scarfone and Paul Hofmann. Guidelines on firewalls and firewall policy. NIST, 2009. http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf. 141, 142

[62] [Schonwalder 2009] Jurgen Schonwalder, Marc Fouquet, Gabi Dreo Rodosek and Iris C. Hochstatter. Future internet = content + services + management. Comm. Mag., vol. 47, pages 27-33, July 2009. 77

[63] [Searcy 2003] DeWayne Searcy, Jon Woodroof and Bruce Behn. Continuous Audit: The Motivations, Benefits, Problems, and Challenges Identifed by Partners of a Big 4 Accounting Firm. Hawaii International Conference on System Sciences, vol. 7, page 210, 2003. 5, 17

[64] [Segaran 2009] Toby Segaran, Colin Evans, Jamie Taylor, Segaran Toby, Evans Colin and Taylor Jamie. Programming the semantic web. O'Reilly Media, Inc., 1st edition, 2009. 86

[65] [Siorpaes 2004] Katharina Siorpaes, Kathrin Prantner and Anna V. Zhdanova. Ontology instantiation, sw portal working draft, d13v0.2. DERI Semantic Web Portal Group, 2004. 92, 93, 94, 95

[66] [sox 2002] Sarbanes-oxley act of 2002. public law 107-204. U.S. Government Printing Ofce, 2002. http://www.gpo.gov/fdsys/pkg/PLA\-107publ204/content-detail.html. 3

[67] [SP80053 2009] Computer Security Division Publication SP800-53. Recommended security controls for federal information systems and organizations. NIST, 2009. 34, 146

[68] [Staab 2004] Stefen Staab and Rudi Studer. Handbook on ontologies (international handbooks on information systems). SpringerVerlag, 2004. 82

[69] [Stoneburner 2002] Gary Stoneburner, Alice Goguen and Alexis Feringa. Risk management guide for information technology systems. NIST, 2002. http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/nist800-30.pdf. 24, 25, 35, 127

[70] [Strassner 2006] John Strassner, Nazim Agoulmine and Elyes Lehtihet. FOCALE A Novel Autonomic Networking Architecture. In Latin American Autonomic Computing Symposium (LAACS), 2006. 79, 80

[71] [Studer 1998] Rudi Studer, V. Richard Benjamins and Dieter Fensel. Knowledge Engineering: Principles and Methods. Data and Knowledge Engineering, vol. 25, no. 12, pages 161-197, March 1998. 82

[72] [Trauşan-Matu 2003] Stefan Trausan-Matu. Inteligenţa artificială -suport curs. 2003. 8, 95

[73] [Uszok 2004] Andrzej Uszok, Jefrey M. Bradshaw, Matthew Johnson, Renia Jefers, Austin Tate, Jef Dalton and Stuart Aitken. KAoS Policy Management for Semantic Web Services. IEEE Intelligent Systems, vol. 19, pages 32-41, July 2004. 75

[74] [Vasarhelyi 2009] Miklos A. Vasarhelyi, Siripan Kuenkaikaew, James Littley and Katie Williams. Continuous Auditing technology adoption in leading internal audit organizations, working paper. 2009. 17

[75] [Verma 2008] Vijay K. Verma, Ramesh C. Joshi, Bin Xie and Dharma P. Agrawal. Combating the bloated state problem in mobile agents based network monitoring applications. Comput. Netw., vol. 52, pages 3218-3228, December 2008. 77

[76] [Wallin 2009] Stefan Wallin and Viktor Leijon. Telecom Network and Service Management: An Operator Survey. In MMNS'09, pages 15-26, 2009. 77

[77] [Watermire 2011] David Watermire and Karen Scarfone. Guide to using vulnerability naming schemes. NIST, 2011. http://csrc.nist.gov/publications/nistpubs/800-51-rev1/SP800-51rev1.pdf. 60, 61

[78] [Wooldridge 2009] Michael Wooldridge. An introduction to multiagent systems. second edition. John Wiley and Sons, 2009. 98