BABEŞ-BOLYAI UNIVERSITY CLUJ-NAPOCA
FACULTY OF ECONOMICS AND BUSINESS ADMINISTRATION
DOCTORAL SCHOOL IN ECONOMICS AND BUSINESS ADMINISTRATION

CONTRIBUTIONS TO SECURITY OF BUSINESS INFORMATION SYSTEMS

- Thesis Summary -

Scientific advisor
Prof. univ dr. TOMAI Nicolae

PhD Student
MIHUŢ Marius

Cluj-Napoca
2014

CONTENTS

INTRODUCTION 1
Opportunity and motivation of thesis 2
Thesis objectives 2
Thesis structure 3
1. THEORETICAL OVERVIEW OF INFORMATION SYSTEMS SECURITY 6
1.1 SECURITY MODELS 6
1.1.1 Multilevel security model 6
1.1.2 Bell-LaPadula model 7
1.1.3 Biba integrity model 11
1.1.4 Clark-Wilson integrity model 12
1.1.5 Comparison of multilevel security models 14
1.2 MULTILATERAL SECURITY MODELS 15
1.2.2 Chinese Wall Model 16
1.2.3 BMA Model 17
1.3 DOMAIN SPECIFIC SECURITY MODELS 18
1.3.1 Graham-Denning Model 18
1.3.2 Take-Grant Model 18
1.4 ASPECTS OF COLLABORATIVE SYSTEMS SECURITY 19
1.5 ASPECTS OF UBIQUITOUS COMPUTING SECURITY 21
1.5.1 Ubiquitous computing features 22
1.5.2 Ubiquitous computing particularities 23
1.6 ASPECTS OF WEB-SERVICES SECURITY 26
1.7 CONCLUSIONS FROM THIS CHAPTER 29
2. INFORMATION SECURITY MANAGEMENT 31
2.1 CURRENT SITUATION 31
2.2 IT GOVERNANCE 34
2.3 COBIT FRAMEWORK 35
2.4 ITIL BEST PRACTICES 46
2.5 ISO/IEC 27000 SECURITY STANDARDS 47
2.5.1 ISO SECURITY MEASURES 48
2.6 NIST STANDARDS 53
2.7 ALIGNEMENT AND INTEGRATION OF COBIT, ITL, ISO AND NIST STANDARDS 54
2.7.1 Vertical integration 55
2.7.3 Horizontal alignment 56
2.8 CONCLUSIONS FROM THIS CHAPTER 57
3. RISK MANAGEMENT 62
3.1 THREATS IDENTIFICATION 63
3.2 VULNERABILITIES IDENTIFICATION 65
3.3 RISK ASSESSMENT METHODS 67
3.3.1 Qualitative analysis 68
3.3.2 Quantitative analysis 69
3.3.3 Job position analysis 71
3.3.4 Comparison of risk evaluation methods 72
3.5 RISK REDUCTION 73
3.6 CONCLUSIONS FROM THIS CHAPTER 80
4. CALCULATION OF SECURITY COSTS 82

4.1 METHODS FOR CALCULATIONS OF PARTIAL COSTS 82
4.2 METHODS FOR CALCULATIONS OF TOTAL COSTS 82
4.3 ABC CALCULATION METHOD 83
4.4 COST MODEL HP LABORATORIES 87
4.5 EVALUATION OF TOTAL COST OF DEVELOPMENTE 89
4.6 ABC-HP COMBINED CALCULATION METHOD 90
4.7 CONCLUSIONS FROM THIS CHAPTER 92
5. BUSINESS INFORMATION SYSTEMS SECURITY: CASE STUDIES 94
5.1 THE NECESSITY OF MULTIDISCIPLINARY APPROACH 94
5.2 ABC-HP COMBINED CALCULATION METHOD: CASE STUDY 95
5.3 PPP SECURITY ANALYSIS: CASE STUDY 100
5.3.1 Introduction 100
5.3.2 Security analysis based on protection, price and performance 101
5.3.3. Results and discussions 104
5.3.3.1 Initial situation 104
5.3.3.2 First scenario 106
5.3.3.3 Second scenario 108
5.3.3.4 Third scenario 110
5.3.3.5 Results centralization 112
5.4 CONCLUSIONS FROM THIS CHAPTER 113
6. ELEMENTS USED IN SECURITY MODEL 116
6.1 PARETO PRINCIPLE 116
6.1.1 Application of Pareto Principle in management and informatics 117
6.1.2 Application of Pareto Principle in security management 118
6.2 PRIORITIZATION OF SECURITY ACTIVITIES 120
6.2.1 Prioritization methods 120
6.2.2 Prioritization based on Critical Path Method (CPM) 122
6.3 SECURITY MEASUREMENTS AND METRICS 127
6.4 SECURITY DOCUMENTATIONS 130
6.5 SECURITY VISUALIZATION 133
6.6 SECURITY MONITORING 134
6.6.1 Audit – common notions 135
6.6.2 Security audit 138
6.7 RACI RESPONIBILITIES CHART 139
6.8 BALANCED SCORECARD 140
6.9 1-10-100 Rule 141
6.10 LOG DATA ANALYSIS 142
6.11 CONCLUSIONS FROM THIS CHAPTER 143
7. DESCRIPTION OF PERSONAL SECURITY MODEL 145
7.1 CURRENT SITUATION 145
7.2 SECURITY CONCEPTS 146
7.3 SERIOS FRAMEWORK 153
7.4 DESCRIPTION OF SERIOS FRAMEWORK 154
7.5 CASE STUDY: EVALUATION OF A SECURITY SYSTEM 185
7.5.1 Introduction 185
7.5.2 Initial situation 187
7.5.3 Situation 1 – after risk analysis 188
7.5.4 Situation 2 – after implementation of security measures selected according to Pareto Principle 189
7.5.5 Situation 3 – after security audit 190

7.5.6 Situation 4 – after network scanning 191
7.5.7 Situation 5 – after security system testing 192
7.5.8 Situation 6 – after a security event 193
7.6 SECURITY MODEL VALIDATION AND VERIFICATION 194
7.6.1 Security model verification 194
7.6.2 Security model validation 195
7.7 CONCLUSIONS FROM THIS CHAPTER 197
CONCLUSIONS AND PERSONAL CONTRIBUTIONS 199
Personal contributions 199
Dissemination of results 201
Future work 202
REFERENCES 204

KEYWORDS: *threats, protection-price-performance analysis, informational asset, SERIOS framework, security measure, security evaluation, balanced score card, security cost calculation method, security model, maturity level, security prioritization, security program, security metrics system, security system, vulnerability*

INTRODUCTION

Every organization is interested in protecting its information assets (information and associated infrastructure). In many organizations, they are considered critical resources, whereas the existence of the organization depends on how they are protected. For this reason, to improve organizational security, large amounts of money are allocated and spent, but the results are not always as expected.

In any organization, different categories of people have interests, motives and different perceptions about what information security and the security has a different meaning for them (Brotby, 2009: XVIII). *A key element affecting the diffusion of innovations and technologies in an organization is how it is accepted individually* (Mihuţ and Tomai, 2009: 43).

In these circumstances, information security issues should be addressed from a multidisciplinary perspective and a common language of security must be created. Technical measures are not enough to ensure security of information, *many of the problems can be explained more clearly and convincingly using the language of microeconomics* (Anderson, 2001: 1). This idea is reinforced by other authors which states that *the purpose is to make information security a multidisciplinary field where technology specialists will work with experts in "sensitive issues" such as public policy, economics and sociology* (Shostack and Stewart, 2008: 103). The science that will explore the multidisciplinary field of study will be called the *Information Security Economics* and a main method will be *applying ideas from other fields* (Shostack and Stewart, 2008: 103).

The main objective of this paper is to design a security model and a framework which will implement the security system, based on the model developed.

Opportunity and motivation of thesis

The paper proposes the expanding of research in information security, by exploring common areas with other domains such as management, informatics or accounting (costs and expenses). Multidisciplinary approach is necessary because the information

security cannot be ensured only by technical means, and because in any organization should be a "common language of security" and a wide range of stake holders interests. must be harmonized.

The opportunity of the paper is given by the need to create security systems that are more effective (in terms of costs and expenses), more efficient (in terms of protection provided), which provide decision support (in terms of management) and does not affect the performance of computer systems (from technical perspective).

The starting point of this paper was established by scientific research made by the author during master studies. The choice of research topic was made as a result of the author's work concerns in the field of system administration, of the past 18 years.

Thesis objectives

In this paper we followed some concepts, issues and elements of information security domains. The objectives are:

- Designing a security model adapted to current situation and size of organizations in our country, that can be used to create a security system for the organization, or to obtain a security certification for the organization;
- Designing a framework that can be used to implement a security system, based on the proposed model and ensures security of information in a short time and as reduced consumption of resources;
- Application or adaptation of ideas and elements from other domains, creation of new working tools and using these tools in the SERIOS framework;
- Study of the security domain through a multidisciplinary approach, in order to identify areas that can be improved or changed in this domain.

Thesis structure

The thesis is developed over seven chapters.

In the first two chapters we examined the research field (information security), in order to identify the key conceptual and structural elements of domain and to position the security model which is the subject of the thesis. We analyzed existing security

models and systems and information security particularities in some new areas of computer science. At the end of these chapters were presented the overall findings and research directions that we followed throughout the other chapters.

In chapter three we analyzed risk management as it is the main process in security management. We have developed *Generic catalogs of threats and vulnerabilities*, in order to use them in the security model. We compared risk assessment methods, to determine how they can be used in a case study presented in the paper. For risk reduction phase of the risk management, we developed a *Generic catalog of security measures*, which was used in the framework described in chapter seven.

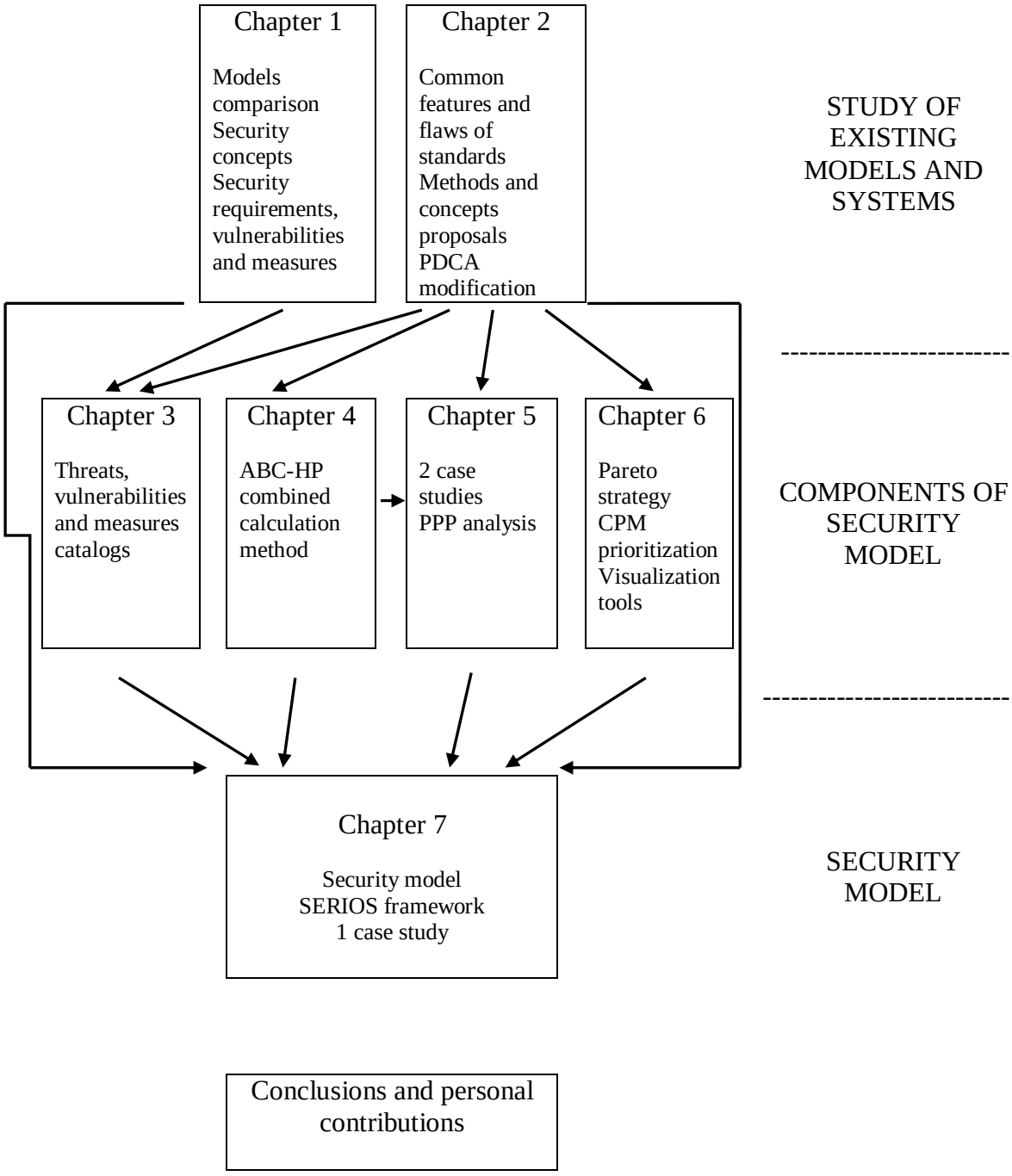
In chapter four we examined two methods for calculating indirect costs and the reasons for each of these methods is not enough to calculate precise security costs. Based on the analysis, we proposed a combined calculation method. Verification of the combined method was made through a case study.

In chapter five, through a case study, we present the steps necessary for using the combined calculation method proposed in chapter four. We also proposed the extensions of the cost-benefit analysis (used in decisions regarding the implementation of security measures) with a method of analysis that takes into account technical factors (performance). The presentation of this method was made in a case study. The methods presented in the two case studies will be used as working tools in the framework presented in chapter seven.

In chapter six we presented how the concepts, methods and principles from other areas, can be applied in security domain. We also presented specific working tools for security (security metrics, visual tools) and specific elements of a management system (security documentation), that will be used in the SERIOS framework.

In chapter seven we presented security model proposed in this thesis and the SERIOS framework, by which it can implement a security system based on this model. Validation of framework was done through a case study that is presented in the chapter.

The structure of thesis and personal contributions are shown in the following figure:


Chapter 1
Models comparison
Security concepts
Security requirements, vulnerabilities and measures
Chapter 2
Common features and flaws of standards
Methods and concepts proposals
PDCA modification
STUDY OF EXISTING MODELS AND SYSTEMS
Chapter 3
Threats, vulnerabilities and measures catalogs
Chapter 4
ABC-HP combined calculation method
Chapter 5
2 case studies
PPP analysis
Chapter 6
Pareto strategy
CPM prioritization
Visualization tools
COMPONENTS OF SECURITY MODEL
Chapter 7
Security model
SERIOS framework
1 case study
SECURITY MODEL
Conclusions and personal contributions

CONCLUSIONS AND PERSONAL CONTRIBUTIONS

Addressing security issues must be made from a multidisciplinary perspective, since security cannot be solved by technology, only.

The security model is adjusted to current situation, since it can be implemented on a functional information system, using only the resources of organization. SERIOS Framework, which implements this security model, does not focus on getting a security certification, but aims to develop a security system and security processes that can be integrated into organization.

The security metrics system and the management tools, that are part of the framework, provide support in decision-making, enabling efficient security activities.

The proposed metrics system allows switching from a security approach based on reactive measures to a security approach based on preventive measures.

Personal contributions

In the first chapter, we have presented theoretical models of security. Our contribution to this chapter was an analysis of these models and expressing personal opinions about them. We have also identified particularities related to security requirements, security vulnerabilities and, also, securing methods in the areas of collaborative systems, ubiquitous computing and web-services.

In the second chapter, we analyzed the management systems used for the IT governance and security management systems ISO and NIST. Our contribution in this chapter was a **multidisciplinary** analysis of structural and conceptual elements of information security systems and, also, expressing personal opinions.

In chapter three we analyzed the main elements and phases of risk management process. Our contribution in this chapter was the identification of conditions in which risk assessment methods can be used and the development of *Generic catalogs* of threats, vulnerabilities and security measures.

In chapter four we analyzed two methods for cost calculation, that can be applied to calculate the security costs: the cost model proposed by HP Laboratories and ABC method. Our contribution to this chapter was the identification of conditions under which these methods can be applied and, also, the description of *ABC-HP combined calculation method*, for accurate calculation of security costs. Checking the accuracy of the method was done by applying it to calculate the cost of an IT service and comparing the result with the result obtained by calculating the same cost using estimation model Krasner, described in section 4.5. The difference between the two results, which was less than 10%, allowed us to conclude that the combined method is accurate and can be used to calculate the security costs.

In chapter five we present two case studies, which address organizational security issues from a multidisciplinary perspective. Our contribution to this chapter was the argumentation for a multidisciplinary approach to address organizational security, the presentation of *ABC-HP combined method* steps and the development of a *Method for three-dimensional analysis of the impact of security measures on the information system of an organization*.

In chapter six, we presented the methods and principles, taken from other areas, which we used in security model and in the SERIOS framework described in the thesis. Our contribution to this chapter was to determine how Pareto Principle, Critical Path Method and 1-10-100 Rule could be applied in the field of security. We have also created a visual tool - *State security graph*, which was included as a working tool in SERIOS framework.

In chapter seven, we described the security model, which is the objective of this thesis and the SERIOS framework, which is the instrument for implementing the security system based on this model. In section 7.6 we presented a case study through which we use the SERIOS framework in a certain company. Our contribution to this chapter was the *description of the model and the framework*, the presentation of their conceptual and structural elements, the specification of *PIV model* for processes, the *description and formalization of security metrics system*, the definition of *information asset* concept and the interpretation of the case study results.

Dissemination of results

The ideas presented in Chapters 1 and 6, as well as case studies in Chapters 4, 5 and 7 were disseminated in scientific papers published in journals in Bucharest and Suceava and in proceedings of national and international conferences.

Scientific papers published in proceedings of international conferences

1. Mihuţ, M., and Tomai, N. (2009) *Analysis of Collaborative Systems Security Using a Three-criteria Approach: Protection, Price and Performance*, International Technology, Education and Development Conference (INTED2009), published by International Association of Technology, Education and Development (IATED), pp. 3400-3409.
2. Mihuţ, M, Arba, R. and Tomai, N. (2009) *Using Data-Mining Solution for Diagnosing Systems*, Conferęncia Engenharia2009, Corvilha, Portugalia.
3. Mihuţ, M, Arba, R., Vereş, O and Tomai, N. (2009) *Centre-based Cost Analyze for Virtual IT Companies*, Conferęncia Engenharia2009, Corvilha, Portugalia.

Scientific papers published in proceedings of national conferences

4. Mihuţ, M. (2006) *TrustCoM – a Security Model for Collaboration Systems*, Annals of the "Tiberiu Popoviciu" Seminar, Supplement: International Workshop in Collaborative Systems, vol. 4, 2006, pp. 195-202.
5. Mihuţ, M. (2007) *Integrating Knowledge Management and e-Learning*, Proceedings of the International Conference on Knowledge Engineering, Principles and Techniques, KEPT2007, Cluj-Napoca (Romania), vol. II, pp. 73–77
6. Mihuţ, M. (2007) *TENCompetence – an Infrastructure for Knowledge Management*, Proceedings of the International Conference Competitiveness and European Integration, vol. Business Information Systems & Collaborative Support Systems in Business, pp. 227-229.
7. Mihuţ, M. (2008) *Aspects of Ubiquitous Computing Security*, Annals of the "Tiberiu Popoviciu" Seminar, Supplement: Romanian Workshop on Mobile Business, vol. 6, 2008, pp. 71-77.
8. Mihuţ, M. (2009) *Prioritization of IT Security Activities*, 16th International Economics Conference "Industrial Revolutions, From the Globalization and Post-

Globalization Perspective ”– IECS 2009, Sibiu, vol. 5, pp. 138-143.

9. Mihuţ, M., and Tomai, N. (2009) *Theoretical Aspects of Diffusion in IT Domain*, Studia Universitas “Babeş-Bolyai” Informatica series, Proceedings of the International Conference on Knowledge Engineering, Principles and Techniques - KEPT 2009, Cluj-Napoca, vol. III – Special Issue 2009, pp. 43-46.
10. Mihuţ, M. (2014) *Security Measurement and Visualization: a New Approach*, Proceedings of the 13th International Conference on Informatics in Economy IE2014, pp. 490-495.

Scientific articles published in national journals and magazines

11. Mihuţ, M. (2008) *Analyzing Log Files Using Data-Mining*, Journal of Applied Computer Science, issue 4 / 2008, pp. 32-34.
12. Mihuţ, M., Todor, L.S. (2009) *Aspecte ale Securităţii Web-services*, Calitatea – Acces la Succes magazine, Proceedings of the International Conference “Sustainable Development in Conditions of Economic Instability”, vol. 10, nr. 101 special / 2009, partea a II-a, Editura Cibernetica MC, Bucureşti, pp. 122-124.
13. Mihuţ, M., Todor, L.S. (2010) *Strategia de Aplicare a Principiului lui Pareto în Managementul Securităţii*, Quality – Access to Success magazine, Proceedings of the International Conference “Sustainable Development in Conditions of Economic Instability”, vol. 11, nr. 113 special / 2010, Editura Cibernetica MC, Bucureşti, pp. 546-560
14. Mihuţ, M., and Tomai, N. (2010) *A Cost Model for the IT Department* Journal of Applied Quantitative Methods, vol. 5, nr. 2 / 2010, pp. 358-366.

Future work

The SERIOS framework can be implemented by organizations that cannot afford the costs of implementing certified security management systems. It can be used both for implementing a proper security system or to prepare the organization for implementing security standards.

Some elements of the work (risk matrix, levels of maturity, levels of categorization) use a three-stage assessment scale. To increase the performance of the security system

a multi-stage scale can be used.

Framework can be extended to be used in areas such as knowledge management, collaborative systems and virtual organizations.

The multidimensional analysis of security can be extended by adding a new dimension about how security is perceived at the individual level within an organization.

REFERENCES

1. Anderson, R. (2001) *Why Information Security is Hard - An Economic Perspective*, University of Cambridge Computer Laboratory, disponibil la http://www.acsac.org/2001/papers/110.pdf, accesat la 20/10/2011.
2. Arens, A.A., Loebbecke, J.K. (2003), *Audit. O abordare integrată*, Editura ARC, Chișinău, Moldova.
3. Arnason, S.T., Willett, K.D. (2008) *How to achieve 27001 certification: an example of applied compliance management*, Auerbach Publications, Boca Raton FL, USA.
4. Bell, D.E., LaPadula, L.J. (1973) *Secure Computer Systems, Mathematical Foundation*, The Mitre Corporation, Bedford MA, USA.
5. Bell, D.E., LaPadula, L.J. (1976) *Secure computer system: unified exposition and Multics interpretation*, The Mitre Corporation, Bedford MA, USA.
6. Biba, K.J. (1977) *Integrity Considerations for Secure Computer Systems*, Technical Report MTR-3153 rev. 1, The Mitre Corporation, Bedford, MA., USA
7. Boehm, B. (1987) *Industrial Metrics Top 10 List*, *IEEE Software*, sept. 1987, pp. 84-85.
8. Boehm, B. and Basili, V.R. (2001) *Software Defect Reduction Top 10 List*, IEEE Computer, vol. 34, nr. 1, ianuarie 2001, pp. 135-137.
9. Brewer, D.F.C., Nash, M.J. (1989) *The Chinese wall security policy*, The IEEE Symposium on research in security and privacy, pp. 206-214, Oakland CA, USA.
10. Brotby, W.K. (2009) *Information security management metrics: a definitive guide to effective security monitoring and measurement*, Taylor & Francis Group, Boca Raton FL, USA.
11. Chakrabarti, A. (2007) *Grid computing security*, Springer-Verlag Berlin Heidelberg, Germania.
12. Clark, D.D., Wilson, D.R. (1987) *A Comparison of Commercial and Military Computer Security Policies*, Proceedings of the 1987 IEEE Symposium on Research in Security and Privacy (SP'87), IEEE Press, pp. 184–193, Oakland CA, USA
13. CMMI (2010) *CMMI for Development, version 1.3*, Software Engineering Institute, disponibil la http://www.sei.cmu.edu/reports/10tr033.pdf, accesat la 30/08/2013.

14. CNSS Instruction no. 4009 (2010) *National Information Assurance (IA) Glossary*, Committee on National Security Systems, disponibil la http://www.ncix.gov/publications/policy/docs/CNSSI_4009.pdf, accesat la 22/11/2011.
15. COBIT 4.1 (2007) *Framework, Control Objectives, Management Guidelines, Maturity Models*, IT Governance Institute, disponibil la http://www.isaca.org/Knowledge-Center/cobit/Pages/Downloads.aspx, accesat la 13/10/2011.
16. COBIT (2008) *Aligning CobiT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit*, IT Governance Institute, disponibil la http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Aligning-COBIT-4-1-ITIL-V3-and-ISO-IEC-27002-for-BusinessBenefit.aspx, accesat la 20/10/2011.
17. CRAMM (2005) *The Logic behind CRAMM's Assessment of Measures of Risk and Determination of Appropriate Countermeasures*, Insight Consulting, disponibil la http://www.cramm.com/files/techpapers/CRAMM%20 Counter measure%20Determination%20and%20Calculation.pdf, accesat la 15/01.2010.
18. Dorfman, M.S. (1997) *Introduction to Risk Management. and Insurance* (6th ed.). Prentice Hall Inc., Upper Saddle River NJ, USA.
19. Fătăcean, Gh. (2006) *Contabilitatea managerială şi Controlul de gestiune*, Editura Alma Mater, Cluj-Napoca, România.
20. Granof, M. H., Platt D. E. şi Vaysman, I. (2000) *Using Activity-Based Costing to Manage More Effectively*, University of Texas at Austin, disponibil la http://www.businessofgovernment.org/sites/default/files/ABC.pdf, accesat la 11/12/2007.
21. Hayat, M. Z., Reeve, J. S. şi Boutle, C. J. (2006) *Prioritisation of Network Security Services*, IEE Journal of Information Security, 153 issue 2, pp. 43-50.
22. Hayat, M. Z., Reeve, J. S. şi Boutle, C. (2006) *Dynamic Threat Assessment for Prioritising Computer Network Security*, 5th European Conference on Information Warfare and Security, Helsinki, Finland.
23. IBM Corporation și Microsoft Corporation (2001), *Security in a Web Services World: A Proposed Architecture and Roadmap*, disponibil la adresa: www.ibm.com/developerworks/library, accesat la 10/06//2009.
24. ISO/IEC 17799 (2005) *Tehnologia informaţiei – Tehnici de securitate – Cod de practică pentru managementul securităţii informaţiilor*, International Organization

for Standardization.

25. ISO/IEC 27001 (2005), *Tehnologia informaţiei – Tehnici de securitate – Sisteme de management a securităţii informaţiei – Cerinţe*, International Organization for Standardization.
26. ISO 31000 (2009) *Risk management – Principles and guidelines*, International Organization for Standardization.
27. Ivan, I. şi Toma, C. (2006) *Information Security Handbook*, Academy of Economic Studies Publishing House, Bucureşti, România.
28. Jaquith, A. (2007) *Security Metrics: replacing fear, uncertainty and doubt*, Pearson Education Inc., Upper Saddle River NJ, USA.
29. Jones, A.K. (1978) *Protection Mechanism Models: Their Usefulness*, Foundations of Secure Computing, Academic Press, New York NY, USA, pp. 237-254.
30. Juran, J.M. (1973) *Calitatea produselor,* Editura Tehnică, Bucureşti, România.
31. Kagal, L., Finn, T. și Joshi, A. (2001) *Moving from Security to Distributed Trust in Ubiquitous Computing Environments*, University of Maryland, IEEE Computer, vol. 34, no. 12 December, pp. 154-157.
32. Kaplan, R. S. şi Bruns, W. (1987) *Accounting and Management: A Field Study Perspective*, Harvard Business School Press.
33. Kaplan, R.S. şi Norton, D.P. (1992) *The Balanced Scorecard: Measures That Drive Performance*, Harvard Business Review, ianuarie-februarie 1992, pp. 71-79.
34. Karapetrovic, S. (2008*) Integrative Augmentation of Standardized Management Systems*, International Journal for Quality research, volumul 2, numărul 1, 2008, disponibil la http://www.ijqr.net/journal/v2-n1/2.pdf, accesat la 29/04/2014.
35. Krasner, J. (2003) *Total Cost of Development: A comprehensive cost estimation framework for evaluation embedded development platform*, Embedded Market Forecasters, disponibil la http://www.embeddedforecast.com/EMFTCD2003v3.pdf, accesat la 24/09/2009.
36. Landoll, J. L. (2006) *The Security Risk Assessment Handbook: a Complete Guide for Performing Security Risk Assessments*, Auerbach Publications, Boca Raton FL, USA.
37. Landoll, J. L. (2006) *The Security Risk Assessment Handbook: a Complete Guide for Performing Security Risk Assessments*, Auerbach Publications, Boca Raton FL, USA.
38. Langheinrich, M. (2001) *Privacy By Design - Principles of Privacy-Aware*

Ubiquitous Systems, UbiComp'01 Proceedings of 3rd International Conference on Ubiquitous Computing, Springer-Verlag, London, UK, pp. 273-291.

39. Lipton, R.J. şi Snyder, L. (1977) *A Linear Time Algorithm for Deciding Subject Security*, Journal of the Association for Cornputing Machinery (Addison-Wesley) volume 24 no. 3, pp. 455–464.
40. Magiera, J. şi Pawlak, A. (2005) *Security frameworks for virtual organizations (capitol în cartea Virtual Organizations: Systems and Practices, pp. 133 – 148)*, Springer US, Boston MA, USA.
41. Marty, R (2009) *Applied Security Visualization*, Pearson Education Inc., Boston MA, USA.
42. Mihuţ, M. (2006) *TrustCoM – a Security Model for Collaboration Systems*, Annals of the "Tiberiu Popoviciu" Seminar, Supplement: International Workshop in Collaborative Systems, vol. 4, 2006, pp. 195-202.
43. Mihuţ, M. (2007) *Integrating Knowledge Management and e-Learning*, Proceedings of the International Conference on Knowledge Engineering, Principles and Techniques, KEPT2007, Cluj-Napoca (Romania), vol. II, pp. 73–77
44. Mihuţ, M. (2007) *TENCompetence – an Infrastructure for Knowledge Management*, Proceedings of the International Conference Competitiveness and European Integration, vol. Business Information Systems & Collaborative Support Systems in Business, pp. 227-229.
45. Mihuţ, M. (2008) *Aspects of Ubiquitous Computing Security*, Annals of the "Tiberiu Popoviciu" Seminar, Supplement: Romanian Workshop on Mobile Business, vol. 6, 2008, pp. 71-77.
46. Mihuţ, M. (2008) *Analyzing Log Files Using Data-Mining*, Journal of Applied Computer Science, issue 4 / 2008, pp. 32-34.
47. Mihuţ, M., şi Tomai, N. (2009) *Analysis of Collaborative Systems Security Using a Three-criteria Approach: Protection, Price and Performance*, International Technology, Education and Development Conference (INTED2009), published by International Association of Technology, Education and Development (IATED), pp. 3400-3409.
48. Mihuţ, M. (2009) *Prioritization of IT Security Activities*, 16th International Economics Conference "Industrial Revolutions, From the Globalization and Post-Globalization Perspective "– IECS 2009, Sibiu, vol. 5, pp. 138-143
49. Mihuţ, M., Todor, L.S. (2009) *Aspecte ale Securităţii Web-services*, Calitatea –

Acces la Succes magazine, Proceedings of the International Conference "Sustainable Development in Conditions of Economic Instability", vol. 10, nr. 101 special / 2009, partea a II-a, Editura Cibernetica MC, Bucureşti, pp. 122-124.

50. Mihuţ, M., şi Tomai, N. (2009) *Theoretical Aspects of Diffusion in IT Domain*, Studia Universitas "Babeş-Bolyai" Informatica series, Proceedings of the International Conference on Knowledge Engineering, Principles and Techniques - KEPT 2009, Cluj-Napoca, vol. III – Special Issue 2009, pp. 43-46
51. Mihuţ, M, Arba, R. şi Tomai, N. (2009) *Using Data-Mining Solution for Diagnosing Systems*, Conferęncia Engenharia 2009, Corvilha, Portugalia
52. Mihuţ, M, Arba, R., Vereş, O şi Tomai, N. (2009) *Centre-based Cost Analyze for Virtual IT Companies*, Conferęncia Engenharia2009, Corvilha, Portugalia
53. Mihuţ, M., Todor, L.S. (2010) *Strategia de Aplicare a Principiului lui Pareto în Managementul Securităţii*, Quality – Access to Success magazine, Proceedings of the International Conference "Sustainable Development in Conditions of Economic Instability", vol. 11, nr. 113 special / 2010, Editura Cibernetica MC, Bucureşti, pp. 546-560
54. Mihuţ, M., şi Tomai, N. (2010) *A Cost Model for the IT Department* Journal of Applied Quantitative Methods, vol. 5, nr. 2 / 2010, pp. 358-366.
55. Mihuţ, M. (2014) *Security Measurement and Visualization: a New Approach*, Proceedings of the 13th International Conference on Informatics in Economy IE2014, pp. 490-495.
56. Mirams, M., McElheron, P. (1999) *Certificarea ISO 9000*, Editura Teora, București, România.
57. Muţiu, A.I. (2007) *Control de gestiune: suport de curs*, Editura Risoprint, Cluj-Napoca, România.
58. NIST Interagency Report (IR) 7298 Revision 2 (2013) *Glossary of Key Information Security Terms*, US Department of Commerce, disponibil la http://csrc.nist.gov/publications/PubsNISTIRs.html, accesat la 27/06/2013.
59. NIST Special Publication 800-30 Revision 1 (2002), *Risk Management Guide for Information Technology Systems*, US Department of Commerce, disponibil la http://csrc.nist.gov/publications/PubsSPs.html, accesat la 27/01/2009.
60. NIST Special Publication 800-53 Revision 3 (2009) *Recommended Security Controls for Federal Information Systems and Organizations*, US Department of Commerce, disponibil la http://csrc.nist.gov/publications/PubsSPs.html, accesat la

04/07/2010.

61. NIST Special Publication 800-37 Revision 1 (2010) *Guide for Applying the Risk Management Framework to Federal Information Systems*, US Department of Commerce , disponibil la http://csrc.nist.gov/publications/PubsSPs.html, accesat la 12/04/2011.
62. Olaru, M., Isaic-Maniu, A., Lefter, V., Pop, N.A., Popescu, S., Drăgulănescu, N., Roncea, L., Roncea, C. (2000) *Tehnici şi instrumente utilizate în managementul calităţii,* Editura Economică, Bucureşti, România.
63. Oprea, D. (2007) *Protecţia şi securitatea informaţiilor*, Editura Polirom, Iaşi, România.
64. Patel, C.D. şi Shah, A.J. (2005) *Cost Model for Planning, Development and Operation of a Data Center*, HP Laboratories Palo Alto, Technical Report HPL-2005-107(R.1), disponibil la http://www.hpl.hp.com/techreports/2005/HPL-2005-107R1.html?jumpid=reg_R1002_USEN, accesat la 10/12/2006.
65. PITAC President's Information Technology Advisory Committee (2005) *Cyber Security: A Crisis of Prioritization*, disponibil la http://www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf, accesat la 03/01/2012.
66. Pattinson, F. (2011) *Security assurance: contrasting FISMA and ISO/IEC 27001*, disponibil la http://www.atsec.com/downloads/documents/FISMA_27001.pdf, accesat la 10/04/2012.
67. Pfleeger, C.P., Pfleeger, S.L. (2003) *Security in Computing*, Prentice Hall, Upper Saddle River NJ, USA.
68. Ritter, T. (2007) *Reaching Out to Protect Within: Comparing and Contrasting ISO 27002/27002 and NIST Special Publication 800-Series information security standard*, IT Compliance Journal, volumul 2, numărul 2, 2007, disponibil la http://download.101com.com/pub/itci/Files/ITCi_Journal_V2N2_07Q3_Web_Final_a.pdf, accesat la 10/04/2012.
69. Rooney, P. (2002) *Microsoft's CEO: 80-20 Rule Applies to Bugs, Not Just Features*, disponibil la http://www.crn.com/news/security/18821726/microsofts-ceo-80-20-rule-applies-to-bugs-not-just-features.htm, accesat la 14/06/2010.
70. Schneier, B. (2008) *Security ROI*, disponibil la http://www.schneier.com/blog/archives/2008/09/security_roi_1.html, accesat la 01/02/2009.

71. Seigneur, J.M., Farrell, S. şi Damsgaard J.C. (2003) *Distributed Systems Group*, Department of Computer Science, Trinity College, Dublin 2, Ireland.
72. Shostack, A. şi Stewart, A. (2008) *The New School of Information Security*, Pearson Education Inc., Boston MA, USA.
73. Smith, M. L., Erwin, J, (2005) *Role & Responsibility Charting (RACI)*, disponibil la http://myclass.peelschools.org/sec/12/4268/Resources/RACI_R_Web3_1.pdf, accesat la 10/06/2012.
74. Stajano, F. (2002) *Security for Ubiquitous Computing*, John Wiley & Sons Ltd., West Sussex, England.
75. Vişan, A., Ionescu, N., (2009) *Managementul Calităţii – Pentru uzul studenţilor,* partea a doua, capitolul 8, Universitatea Politehnica din Bucureşti, Catedra TCM, Bucureşti, România, disponibil la http://www.aurelvisan.ro/attachments/098_MC_Rez_Cap.%2008_Guru%20Calit.pdf, accesat la 12/06/2010.
76. Wagealla, W., English, C., Terzis, S., Nixon Paddy, L.H. şi McGettrick, A. (2004) *A Trust-based Collaboration Model for Ubiquitous Computing*, Department of Computer and Information Sciences University of Strathclyde, Glasgow, Scotland, 2004.
77. Weiser, M. (1991) *The Computer for the 21st Century*, Scientific American Magazine, September 1991, pp. 94-104.
78. http://www.opnet.com/university_program/itguru_academic_edition/
79. http://hadm.sph.sc.edu/Courses/J716/CPM/CPM.html
80. http://hspm.sph.sc.edu/Courses/J716/CPM/Pathfind.html