ABSTRACT

Information security in organizations is more than a technological issue. To attain higher information security, organizations have to implement technological safeguards, as well as modify their internal procedures and promote the adoption of a security attitude by their employees. Therefore, organizations have to adopt a managerial approach towards security.

An increasing number of organizations aimed to demonstrate to their peers that they possess an internal model of information security management through the attainment of the BS 7799-2 certification (future ISO 27001).

The present dissertation examines the application of the requirements of this British certification of security management in a small sized organization, with the objective of presenting and discussing an implementation methodology of information security management in small and medium sized organizations.

Keywords:
Information Security Management; Security Certification; Risk Management; ISO/IEC 17799;

RESUMO

A segurança da informação nas organizações extravasa o domínio tecnológico. As organizações para proporcionarem uma maior protecção para a sua informação, além de implementar sistemas de protecção de cariz tecnológico têm de modificar os seus procedimentos internos e promover a adopção de uma atitude de segurança por parte dos seus colaboradores. Neste contexto, as organizações têm que assumir uma perspectiva de gestão face à segurança.

Um número crescente de organizações procuram demonstrar aos seus pares que possuem um modelo de gestão de segurança da informação, através da obtenção da certificação BS 7799-2 (futura ISO 27001).

A presente dissertação examina a aplicação dos requisitos desta certificação britânica de gestão de segurança numa organização de pequena dimensão, tendo como finalidade apresentar e discutir uma metodologia de implantação de gestão da segurança da informação, adequada às pequenas e médias organizações.

Palavras-chave:
Gestão de Segurança da Informação; Certificação de Segurança; Gestão do Risco; ISO 17799.

Língua:
A presente tese foi escrita em Inglês, segundo a norma linguística do Inglês Europeu.

TABLE OF CONTENTS

TABLE OF CONTENTES …………..…………………………………………………………….…. V

LIST OF TABLES ……………………………………………………….……………….......… X

LIST OF FIGURES ……..……………………...…………………………………..………......… XI

LIST OF ACRONYMS USED …………………………………………………….…...……...... XII

GLOSSARY ………………………………………………….………..………..…………..... XXI

1. INTRODUCTION …………………………...……..………….………..…………...…..….… 1

1.1 Motivation for the research project .... **Error! Bookmark not defined.**

1.2 Current approaches to security evaluations .... **Error! Bookmark not defined.**

1.3 Problem statement .... **Error! Bookmark not defined.**

1.3.1 Research objective and presumptions.. **Error! Bookmark not defined.**
1.3.2 Research questions.. **Error! Bookmark not defined.**

1.4 Overview of research methodology... **Error! Bookmark not defined.**

1.5 Overview of the dissertation.. **Error! Bookmark not defined.**

2. OUTLINE OF RISK MANAGEMENT METHODOLOGIES…………..………......…… 19

2.1 Introduction .... **Error! Bookmark not defined.**

2.2 What is a risk? .... **Error! Bookmark not defined.**

2.3 The dimensions of risk in information security .... **Error! Bookmark not defined.**

2.3.1 What is an asset?.. **Error! Bookmark not defined.**
2.3.2 What is a threat? .... **Error! Bookmark not defined.**
2.3.3 What is a vulnerability? .... **Error! Bookmark not defined.**
2.3.4 What is an impact?... **Error! Bookmark not defined.**

2.4 Risk management frameworks .... **Error! Bookmark not defined.**

2.4.1 Requirements of information security for risk management......... **Error! Bookmark not defined.**
2.4.2 Selection of a risk framework: BS 7799-2................................... **Error! Bookmark not defined.**
2.4.3 Risk management according to BS 7799-2:2002 (BSI)................ **Error! Bookmark not defined.**

2.5 Conclusions .... **Error! Bookmark not defined.**

3. SYNOPSIS OF THE RISK MANAGEMENT PROCESS…………..………......………… 30

3.1 Introduction.. **Error! Bookmark not defined.**

3.2 Phase 1: Define the scope of the ISMS .... **Error! Bookmark not defined.**

3.2.1 Overview .... **Error! Bookmark not defined.**
3.2.2 Summary of BSI requirements .... **Error! Bookmark not defined.**
3.2.3 Interpretation of BSI requirements .... **Error! Bookmark not defined.**
3.2.4 Analysis of available literature .... **Error! Bookmark not defined.**

3.3 Phase 2: Define an ISMS policy.. **Error! Bookmark not defined.**

3.3.1 Overview .... **Error! Bookmark not defined.**
3.3.2 Summary of BSI requirements .... **Error! Bookmark not defined.**
3.3.3 Interpretation of BSI requirements .... **Error! Bookmark not defined.**
3.3.4 Analysis of available literature .... **Error! Bookmark not defined.**

3.4 Phase 3: Define a systematic approach to risk assessment.................. **Error! Bookmark not defined.**

3.4.1 Overview .... **Error! Bookmark not defined.**

3.4.2 Summary of BSI requirements .... **Error! Bookmark not defined.**
3.4.3 Interpretation of BSI requirements .... **Error! Bookmark not defined.**
3.4.4 Analysis of available literature .... **Error! Bookmark not defined.**

3.5 Phase 4: Identify the risks... **Error! Bookmark not defined.**

3.5.1 Overview .... **Error! Bookmark not defined.**
3.5.2 Summary of BSI requirements .... **Error! Bookmark not defined.**
3.5.3 Interpretation of BSI requirements .... **Error! Bookmark not defined.**
3.5.4 Analysis of available literature .... **Error! Bookmark not defined.**

3.6 Phase 5: Assess the risks .... **Error! Bookmark not defined.**

3.6.1 Overview .... **Error! Bookmark not defined.**
3.6.2 Summary of BSI requirements .... **Error! Bookmark not defined.**
3.6.3 Interpretation of BSI requirements .... **Error! Bookmark not defined.**
3.6.4 Analysis of available literature .... **Error! Bookmark not defined.**

3.7 Phase 6: Identify and evaluate options for the treatment of risks .... **Error! Bookmark not defined.**

3.7.1 Overview .... **Error! Bookmark not defined.**
3.7.2 Summary of BSI requirements .... **Error! Bookmark not defined.**
3.7.3 Interpretation of BSI requirements .... **Error! Bookmark not defined.**
3.7.4 Analysis of available literature .... **Error! Bookmark not defined.**

3.8 Phase 7: Select control objectives and controls for the treatment of risks........... **Error! Bookmark not defined.**

3.8.1 Overview .... **Error! Bookmark not defined.**
3.8.2 Summary of BSI requirements .... **Error! Bookmark not defined.**
3.8.3 Interpretation of BSI requirements .... **Error! Bookmark not defined.**
3.8.4 Analysis of available literature .... **Error! Bookmark not defined.**

3.9 Phase 8: Prepare a Statement of Applicability..................................... **Error! Bookmark not defined.**

3.9.1 Overview .... **Error! Bookmark not defined.**
3.9.2 Summary of BSI requirements .... **Error! Bookmark not defined.**
3.9.3 Interpretation of BSI requirements .... **Error! Bookmark not defined.**
3.9.3 Analysis of available literature .... **Error! Bookmark not defined.**

3.10 Phase 9: Obtain management approval... **Error! Bookmark not defined.**

3.10.1 Overview .... **Error! Bookmark not defined.**
3.10.2 Summary of BSI requirements .... **Error! Bookmark not defined.**
3.10.3 Interpretation of BSI requirements .... **Error! Bookmark not defined.**
3.10.3 Analysis of available literature .... **Error! Bookmark not defined.**

3.11 Conclusions .... **Error! Bookmark not defined.**

4. SYNOPSIS OF SECURITY CONTROLS CATALOGUES ………..……….....………… 55

4.1 Introduction... **Error! Bookmark not defined.**

4.2 What are security catalogues?.. **Error! Bookmark not defined.**

4.2.1 Overview of security catalogues... **Error! Bookmark not defined.**
4.2.2 Four security catalogues .... **Error! Bookmark not defined.**

4.3 Examination of the four catalogues according to hypothesis .... **Error! Bookmark not defined.**

4.3.1 Does ISO aims to protect the same object of the other catalogues?............ **Error! Bookmark not defined.**
4.3.2 Does ISO has a detail level similar to other catalogues? .... **Error! Bookmark not defined.**
4.3.3 Does ISO has security controls similar to other catalogues? .... **Error! Bookmark not defined.**

4.4 Conclusions .... **Error! Bookmark not defined.**

5. SECURITY MANAGEMENT IMPLEMENTATION METHODOLOGY……….………55

5.1 Introduction .... **Error! Bookmark not defined.**

5.2 Information security management (ISMS) concept............................. **Error! Bookmark not defined.**

5.3 Bakground context of the case study organization.............................. **Error! Bookmark not defined.**

5.4 Constraints of the project.. **Error! Bookmark not defined.**

5.5 Stage 1: Project management definiton.. **Error! Bookmark not defined.**

5.5.1 Overview .... **Error! Bookmark not defined.**
5.5.2 Rationale for the proposed procedures .... **Error! Bookmark not defined.**

5.6 stage 2: Evaluation area definition .... **Error! Bookmark not defined.**

5.6.1 Overview .... **Error! Bookmark not defined.**
5.6.2 Rationale for the proposed procedures .... **Error! Bookmark not defined.**

5.7 Stage 3: Define business and legal requirements................................. **Error! Bookmark not defined.**

5.7.1 Overview .... **Error! Bookmark not defined.**
5.7.2 Rationale for the proposed procedures .... **Error! Bookmark not defined.**

5.8 Stage 4: develop an asset register... **Error! Bookmark not defined.**

5.8.1 Overview .... **Error! Bookmark not defined.**
5.8.2 Rationale for the proposed procedures .... **Error! Bookmark not defined.**

5.9 Stage 5: Conduct risk management .... **Error! Bookmark not defined.**

5.9.1 Overview .... **Error! Bookmark not defined.**
5.9.2 Rationale for the proposed procedures .... **Error! Bookmark not defined.**

5.10 Stage 6: Define security processes and controls................................ **Error! Bookmark not defined.**

5.10.1 Overview .... **Error! Bookmark not defined.**
5.10.2 Rationale for the proposed procedures .... **Error! Bookmark not defined.**

5.11 Conclusions .... **Error! Bookmark not defined.**

6. CASE STUDY IN ADETTI …………………………………………………….…..………76

6.1 Introduction .... **Error! Bookmark not defined.**

6.2 Methodology application in ADETTI .... **Error! Bookmark not defined.**

6.2.1 Stage 1: Project management definition .... **Error! Bookmark not defined.**
6.2.2 Stage 2: Evaluation area definition.. **Error! Bookmark not defined.**
6.2.3 Stage 3: Define legal and business requirements......................... **Error! Bookmark not defined.**
6.2.4 Stage 4: Develop an asset register .... **Error! Bookmark not defined.**
6.2.5 Stage 5: Conduct risk management.. **Error! Bookmark not defined.**
6.2.6 Stage 6: Define security processes... **Error! Bookmark not defined.**

6.3 Analysis of implementetion metodology findings............................... **Error! Bookmark not defined.**

6.3.1 Resource and time consumption of an implementation project 72
6.3.2 Results of the implementation project .... **Error! Bookmark not defined.**

6.4 Sumary of findings… .... **Error! Bookmark not defined.**

7. CONCLUSIONS ………………..……………………………………………….…..………88

7.1 Objectives and structure of the Dissertation.. **Error! Bookmark not defined.**

7.2 Assumptions adopted in the project... **Error! Bookmark not defined.**

7.3 A conceptual view of the dissertation.. **Error! Bookmark not defined.**

7.4 Conclusions reached.. **Error! Bookmark not defined.**

7.5 Contributions of the Dissertation.. **Error! Bookmark not defined.**

7.6 Future directions.. **Error! Bookmark not defined.**

REFERENCES ………………………………………………………………..………….....… 82