Instituto Superior de Ciências do Trabalho e da Empresa
Departamento de Ciências e Tecnologias da Informação

SECURITY CERTIFICATION FOR ORGANIZATIONS: A FRAMEWORK TO MANAGE INFORMATION SECURITY

Paulo Coelho

Dissertation presented in partial fulfilment of the Requirements for the degree of
Master in Management of Information Systems

Supervisor
Professor Doutor José Miguel Dias

November, 2007

Instituto Superior de Ciências do Trabalho e da Empresa
Departamento de Ciências e Tecnologias da Informação

CERTIFICAÇÃO DE SEGURANÇA PARA ORGANIZAÇÕES: UM MODELO PARA GERIR A SEGURANÇA DA INFORMAÇÃO

Paulo Coelho

Dissertação submetida como requisito parcial para obtenção do grau de
Mestre em Gestão de Sistemas de Informação

Orientador:
Prof. Doutor José Miguel Dias

Novembro, 2007

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.

ACKNOWLEDGEMENTS

This project could not have been accomplished without the support and encouragement of several persons, to whom I am truly indebted. Therefore, I would like to express my deepest gratitude.

Professor Miguel Dias, my supervisor and President of ADETTI, who has been a source of valuable guidance and ubiquitous encouragement during this research. His accurate insights have built bridges over the abysses, which I encountered during my endeavour of applying BS 7799 in ADETTI. His support has made this experience both rewarding and memorable.

Fernando Fevereiro Mendes, a BS 7799 certified auditor at Sinfic and an information security practitioner, has made an important contribution to enriching this investigation. His practical advice, drawn from a vast expertise in implementing security programs in organizations, helped me interpreting BS 7799.

Chris Ferrant of British Standard Institution, home of BS 7799, has helped me in showing that a security management system has to be, above all, a system that works in a particular organization. And therefore a method to implement a system like this, more than following an orthodox methodology, has to be adequate for a particular organization.

I would like to convey my deepest thanks and affection to all the personnel at ADETTI. In particular, Fátima Estevens, Sónia Ferro and Ana Rita Leitão, who have always greeted me with a smile, even though I was forced to ask them to perform many tedious tasks in order to collect data for this research. My thanks also go to Bruno Marçal and Pedro Fonseca who also guided me in the collection of data from ADETTI. My thanks also go to ADETTI´s researchers, especially Paulo Trezentos, Carlos Serrão and Manuel Gamito, for their comments, suggestions and encouragement throughout this project.

Carlos Gois, a professional auditor, who generously provided me with the opportunity to discover COBIT.

My English reviewers, Professor Sunil Gupta, John Owens and Vanesa Nicho, whose unsurpassed dedication helped in making this text more understandable.

Vanda Gonçalves Santos, for that fragile and absolute feeling that bound two strangers into lovers.

My friends - in particular Martinha Piteira and Samir Haddad - and family, neglected during this period, but never forgotten.

Lisbon, 24th September 2004

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS USED

ADETTI	Association for the Development of Telecommunications and Information Technology
ALARP	As Low As Reasonably Practicable
ALE	Annualised Loss Exposure
APCER	*Associação Portuguesa de Certificação* (Portuguese Certification Association)
ARO	Annualised Rate of Occurrence
BSCW	Basic Support for Cooperative Work
BS 7799	The same as BSI (bellow)
BSI	British Standard 7799-2:2002 - *Information Security Management Systems* - *Specification with Guidance for Use* [BSI02]
CIA	Confidentiality, Integrity, and Availability (*cf.* glossary)
COBIT	Control Objectives for Information and related Technology
CRAMM	CCTA Risk Analysis and Management Methodology
CVE	Common Vulnerability Evaluation (from the US MITRE)
DMZ	Demilitarised zone
FMECA	Failure Mode and Effect Criticality Analysis
FTA	Fault Tree Analysis
GMITS	International Organization for Standardization/International Electrotechnical Commission *Technical Report* 13335 - *Guidelines for the Management of IT Security* (GMITS) [ISO96], [ISO97], [ISO98], [ISO00b], [ISO01]
HazOp	Hazard and Operability study
IDS	Intrusion Detection System
ISMS	Information Security Management System (*cf.* glossary)
IT	Information Technology
ICT	Information and Communication Technology
ISO	International Organization for Standardization/International Electrotechnical Commission 17799 - *Code of Practice for Information Security Management* [ISO00a]
LAN	Local Area Network
NIST	National Institute of Standards and Technology (US)
NSA	National Security Agency (US)
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
SoA	Statement of Applicability
SLE	Single Loss Exposure
SM	Security Management
SMTP	Simple Mail Transfer Protocol
SWOT	Strengths, Weaknesses, Opportunities and Threats
TCP/IP	Transmission Control Protocol/Internet Protocol
TFTP	Trivial File Transfer Protocol
UK	United Kingdom
US	United States of America
TCSEC	Trusted Computer System Evaluation Criteria
WAN	Wide Area Network

GLOSSARY

Asset Anything that has value to an organization [Humphreys02b:p.13].

Availability Ensuring that authorised users have access to information and associated assets when required [BSI02:p.3].

Baseline A (security) baseline is the minimum set of assurance ensured by a group of security controls.

Confidentiality Ensuring that information is accessible only to those authorised to have access [BSI02:p.3].

Countermeasure The same as a security control (see below).

BSI´s implementation An implementation of the framework of BSI (BS 7799-2:2002) in an organization. Implementations which are audited as compliant receive the BSI certification.

Degree of assurance The level of protection required for an asset, determined by business and legal constraints.

Evaluation area The organization's area subject to the security evaluation process. This area is defined by its activities, resources, locations and types of information.

Evaluation criteria The same as risk acceptance criteria: the group of criteria used by organizations to classify risks as acceptable or unacceptable.

Impact The result of an unwanted incident [ISO96] in an organization [AS99].

Information The meaning that is currently assigned to data by means of the conventions applied to that data [Humphreys02b:p.14]. Information can be stored in an electronic format or by any means. An example is intellectual information, which is stored in people's minds.

Information security Protection of confidentiality, integrity and availability of information [BSI02:p.3].

Information security management Management activity aimed to the protection of information and its supporting infrastructure. This activity involves a continuous assessment of risks and management (selection, implementation, monitoring and readjustment) of security controls targeted to mitigate them.

Information Security Management System (ISMS) (1) Part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security. It includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources [BSI02:p.3]. (2) Area of an organization subjected to security management. (Assertion sometimes used in the text).

Integrity Safeguarding the accuracy and completeness of information and computer software [Humphreys02b:p.14].

Operational manager A manager with direct responsibilities in a unit or department included in the evaluation area.

Process A set of linked activities within an organization that has an input and an output [BSI02]. In the text, only the word "process" is sometimes used to refer to organizational processes.

Residual Risk The risk remaining after the risk treatment [Humphreys02b:p.14].

Risk Combination of probability of an event and its consequences [BSI02:p.3].

Risk acceptance criteria See "evaluation criteria" above.

Risk assessment The overall process of risk analysis (systematic use of information to identify sources and to estimate the risk) and risk evaluation (process of comparing the estimated risk against given risk criteria to determine the significance of risk [BSI02:p.3].

Risk management Coordinated activities to direct and control an organization with regard to risk [BSI02:p.3].

Risk treatment Process of selection and implementation of controls to modify risk [Humphreys02b:p.15]. In practical terms, treat the risk can be (1) reduced by security controls; (2) transferred its negative effects to another party through e.g. insurance; (3) avoid the risk by preventing the use of the asset affected by that risk.

Security control A practice, procedure or mechanism that mitigates security risk [Humphreys02b:p.14].

Security control catalogue A list of recommended security controls. Examples studied in this research are ISO [ISO00a], GMITS [ISO00b] COBIT [ISACA00] and NIST Handbook [NIST95].

Threat A potential cause of an unwanted incident [ISO96], which affects the CIA dimensions of security and results in harm to an organization.

Vulnerability A weakness of an asset, a flaw in the organizational policies or worker’s actions, that allows a threat to cause harm [ISO96], [Alberts02].

1.

INTRODUCTION

Mankind only poses for itself such tasks as it can resolve.
Karl Marx [1]

1.1 MOTIVATION FOR THE RESEARCH PROJECT

Microsoft recently suffered an attack, deemed by them as the most harmful ever, by which a part of the source code of Windows operating system was robbed from the facilities of a partner [Público04]. This security incident highlighted the issue of trust between organizations and their partners.

In our increasing networked economy, the IT applications that support the business of organizations are progressively becoming more dependent on third parties [Zuccato02]. The abandonment of the in-house development by most organizations and the need to interconnect different systems has contributed to the growing IT dependency of an organization on its partners.

This IT interdependency has lead organizations to develop the need of evaluating systems developed by others and assessing the trustworthiness of partners.

Conscious of these needs, the US Department of Defence issued a policy, in 2002, to force all acquired systems to be evaluated for its security capacities [Robinson02]. According to this requirement, all products must be tested by independent laboratories under the Common Criteria rules (see next section).

Apart from systems, also the internal operations of organizations can also be subjected to security evaluations. In this context, some organizations, compelled by regulations (as Data Privacy Laws), as well as, instigated by clients and partners, have obtained security certifications (*cf.* 3.2.4 b).

1.2 CURRENT APPROACHES TO SECURITY EVALUATIONS

The evaluation mechanisms that issue a security classification can be classified in three categories according to their scope: (1) system, (2) interface or (3) management certifications, as illustrated in Figure 1.1

[1] Karl Marx in Contribution to the Critique of Political Economy. Extracted from Baudrillard [04].

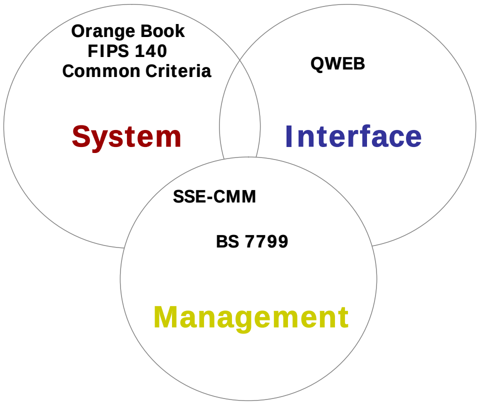


Figure 1.1: A taxonomy of security evaluations according to its scope

The pioneering security evaluation mechanisms measure the security of specific products. This is the case of Trusted Computer System Evaluation Criteria (TCSEC), also known as Orange Book and of the current Common Criteria (ISO/IEC 15408) and Federal Information Processing Standard (FIPS) 140. All of these certifications rank systems security according to a predefined scale of assurance levels.

Interface certifications attest the e-commerce interface of organizations with their clients and partners. An example is Qweb from APCER (*Associação Portuguesa de Certificação* - Portuguese Certification Association).[2]

Management certifications focus on the management of security. In this field, Systems Security Engineering Capability Maturity Model (SSE-CMM) employs a metrology of five levels to grade the maturity of the security processes conduced by an organization (*cf*. 3.8.4). However, this model addresses only the management processes associated with the security of resources (systems, products or services) and not the processes with a broader organization scope. On the contrary, BS 7799-2:2002 [BSI02], a British standard of information security, issues a certification for organizations that have developed security management mechanisms with an organizational ambit.

An organization to be granted with the BS 7799-2 certification by a certification body [3] must (1) implement security management processes according to BS 7799-2:2002 (a security management standard) and (2) select a set of security controls from ISO/IEC 17799:2000 [ISO00a], a security control catalogue.

These controls tackle technological aspects (as the requirement for applications to validate input data), requirements for the operation of e-commerce (e.g. order transactions) and management issues (as security training for users). Therefore, as seen, management certifications also incorporate concerns about systems and e-commerce platforms in addition to managerial issues.

This dissertation will focus on a management certification, which is BS 7799-2:2002 (according to a selection made in section 2.4.2).

[2] Qweb establishes the technological and commercial requirements of a proper business operation within e-commerce platforms (i.e., includes specifications to mediate conflicts between the organization and buyers). Some Portuguese websites are Qweb certified [APCER03].

[3] A certification body is an institution which is accredited to issue a specific certification. In Portugal, examples of certification bodies are APCER and Bureau Veritas Quality International (BVQI).

1.3 PROBLEM STATEMENT

1.3.1 Research objective and presumptions

The present dissertation aims to formulate a methodology capable of implementing security management in small sized organizations (up to 100 employees).

In order to delimitate the research, the dissertation adopted the assumptions that security management in organizations involves two main tasks: (1) assessing risks associated with information security and (2) implementing security controls to mitigate risks. Based on this assumption, it can be conceived that an implementation methodology of security management would be supported on a determined course of actions to identify and assess risks as well as decide a strategy to handle it, which could be, for example, adopting a countermeasure to mitigate it. The adopted protection measure could be selected from a list of recommended controls considered applicable to the organization.

In sum, this dissertation assumes that an implementation methodology of security management is sustained on (1) a risk management methodology and (2) a catalogue of countermeasures.

1.3.2 Research questions

The primary research problem of this academic endeavour is:

How management of information security can be implemented in a small sized organization?

This question, which seeks to attain the aforementioned research objective (*cf*. 1.3.1), leads to three research questions examined in the review of the available literature:

- Which risk management methodology is more suitable to handle risks affecting information security? (Answered in chapter 2)

- What procedures are employed to identify, assess and mitigate risks affecting information security? (Debated in chapter 3)

- How different catalogues of countermeasures tackle the protection of information? (Pondered in chapter 4)

Findings from this theoretical investigation are applied in the formulation of an implementation methodology of security management according to BS 7799-2:2002. This methodology is employed in a given case study (ADETTI), which enables to gain insights of the methodology’s applicability.

1.4 RESEARCH METHODOLOGY OVERVIEW

The current project was carried out adopting two methodologies: literature review and case study analysis.

Due to scarcity of academic studies about implementations of security management in organizations and especially, about BS 7799-2:2002, the researcher made extensive use of insights from information security practitioners and reports available from International User Group of BS 7799 (http://www.xisec.com), SANS Institute (http://www.sans.org), *Biblioteca do Conhecimento* Online (http://www.b-on.pt), as well as documents from the British Standard Intuition, *alma mater* of BS 7799-2:2002.

The case study of ADETTI enabled the application of the proposed methodology of security management implementation.

As a result, in ADETTI it was analysed security risks affecting the organization within the BS 7799-2:2002 framework, defined possible paths to mitigate them and planned organizational mechanism to sustain security management.

1.5 OVERVIEW OF THE DISSERTATION

The dissertation is organised into five parts, as depicted in Figure 1.2. Following the introduction, the second part - literature review - analyses the three assertions defined in section 1.3.2 throughout chapter two, three and four.

The conclusions reached about risk management methods (chapter two and three) and safeguards catalogues (chapter four) are applied to define an implementation methodology of a security management system. This proposed methodology is discussed in chapter five and in chapter six it is employed in ADETTI, an organization used as a case study for the application of the methodology.

The research culminates in chapter seven, in which the author presents a synthesis of the findings of the dissertation, taking a stock of the research undertaken and reaching conclusions in relation to the investigation hypotheses as well as proposing possible research directions.

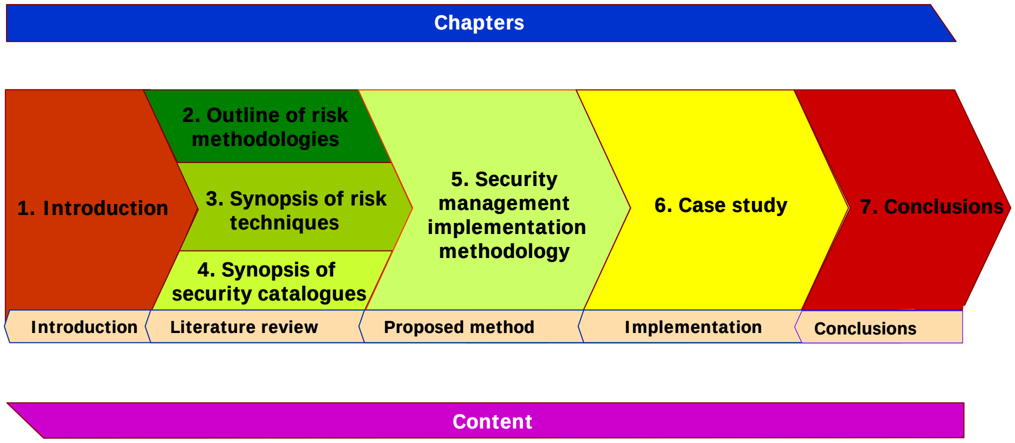

Chapters
1. Introduction
2. Outline of risk methodologies
3. Synopsis of risk techniques
4. Synopsis of security catalogues
5. Security management implementation methodology
6. Case study
7. Conclusions
Introduction
Literature review
Proposed method
Implementation
Conclusions
Content

Figure 1.1: Dissertation structure

2.

OUTLINE OF RISK MANAGEMENT METHODOLOGIES

Security is managing risks.
Marcos Sêmola [4]

2.1 INTRODUCTION

We will begin our research of security management by investigating one of its twofold dimensions: risk management (*cf.* 1.3.1). As ascertain in the preceding chapter, the management of information security is supported on the assessment and treatment of risks. This chapter provides the foundation to comprehend risks within the context of information security management.

The increasing degree of risk exposure of information systems, as inferred by the available reports on computer security breaches, suggests the need to handle risk from a managerial approach. [5] As a result of these concerns, several standard's bodies have issued risk management frameworks.

The text evaluates four risk schemes - (1) the British standard (BS 7799-2:2002 or simply BSI) [BSI02], (2) CORAS [Gran03], (3) OCTAVE [Alberts02] and (4) GMITS [ISO98] - in order to select a proper framework for implementation.

This chapter is structured as follows. First, the concept of risk is located in the information security context. Then, four risk standards are assessed based on two information security requirements. Finally, a risk management definition is reached.

2.2 WHAT IS A RISK?

Few concepts are probably as ubiquitous as risk. Risk has been defined by business management authors as being:

- "Deviations from the expected value" [Valsamakis00].

[4] Extracted from Sêmola [03].

[5] Examples of data sources are CSI/FBI [CSI04], Ernest & Young [E&Y04], CERT Coordination Centre [CERT04], PriceWaterhouseCooppers [PWC02].

- “A situation, which may present a relative variation of the actual from the expected outcome” [Skipper98].
- “Risks are uncertain future events that could influence the achievement of the organizations strategic, operational and financial objectives” [IFAC99].

In the IT field, risk has been conceptualised from several angles:

- (1) “Risk is the combination of the probability of occurrence of harm and the severity of that harm.”

  IEC standard Functional safety of electrical/electronic/programmable electronic safety-related systems *IEC61508. Cited in [Fredriksen02]*

- (2) “Risk is a function of the anticipated frequency of occurrence of an undesired event, the potential severity of resulting consequences and the uncertainties associated with the frequency and severity.”

  NASA standard STD-8719.13A Software Safety. Cited in [Goseva-Popstojanova03]

- (3) “Risk is the potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the asset (i.e. an impact).”

  ISO risk standard GMITS [ISO98]

- (4) “Risk is the possibility of something happening that will have an impact upon objectives. Risks are measured in terms of consequences and likelihood.”

  Australian risk standard, AS/ANZ 4360[AS99]

- (5) “Risk is the combination of the probability of an event and its consequences.”

  ISO Guide 73, adopted in British Standard 7799-2 [BSI02]

Based on the aforementioned definitions, the following key elements are evident:

- (A) Both business management and IT perspectives agree that risk is *something* (1) uncertain, (2) which has the potential to cause negative consequences.
- (B) All IT approaches consider that risk has a probability (which suggests, that uncertainty can be estimated) and an impact (in other words, negative consequences).
- (C) IT definitions differ in terms of the object that suffers the impact. For GMITS, the impact is suffered by the asset; for the Australian and the British standard the impact is endured by the organization.

This last point (identified as C) marks the distinction between (1) risk frameworks, with a system scope (as the citations 1, 2 and 3) and (2) risk methods that try to assess information security in organizations as the Australian standard (which was adopted by the risk method CORAS, as further explained) and the British standard (BSI).

BSI considers that information security is the protection of the properties of information, particularly its Confidentiality, Integrity and Availability (or as used in this dissertation CIA).

A risk definition consistent with this notion is provided by Sêmola [03]:

> "Risk is the probability that agents, which are *threats*, exploit *vulnerabilities*, exposing the *assets* to losses of *confidentiality*, *integrity* and *availability*, and causing *impact* on the business" [Sêmola03:pp. 55-56].

Subsequently, these risk dimensions are examined: *assets, threats, vulnerabilities* and *impacts*.

2.3 THE DIMENSIONS OF RISK IN INFORMATION SECURITY

Commonly risks are regarded as consisting of four components: assets, threats, vulnerabilities and impact [Peltier00], [Alberts01], [Sêmola03].

2.3.1 What is an asset?

An asset is *something* of value to an enterprise [Alberts02], which "may be considered valuable enough to warrant some degree of protection" [ISO01:p.4]. In light of this concept, anything (tangible or intangible) considered valuable by an organization could be regarded as an asset.

2.3.2 What is a threat?

Threats in information security have been defined by several authors [S.Pfleeger00], [Peltier00], [Maiwald04].

According to Peltier [00], a threat consists of (1) an agent, (2) a motive and (3) a result. An agent is "the catalyst of threat", which can be human, machine or natural. The motive is the cause of action, and it can be accidental or intentional. The result is "the outcome of the applied threat" [Peltier00:p.8].

A more comprehensive characterization is proposed by Maiwald [04]. This author has identified three components of threats: (1) a target, (2) an agent and (3) an event.

A target is a threatened security service (integrity, accountability, non-repudiation, etc.). An agent is an actor who has (1) access to the target, (2) knowledge to conduct the attack and (3) motivation to undertake the action. An event is the consequence of the attack (for example, information alteration).

To sum up, the author defines threat as an *agent* who takes advantage of a *vulnerability* [Visintine03], causing an incident that affects CIA dimensions of security, resulting in a business *impact* [Sêmola03].

2.3.3 What is a vulnerability?

The concept of vulnerability reveals the dissimilarities between risk methods. For GMITS (as well as other authors [6]), a vulnerability is a fault associated to an IT system [ISO98].

According to the Australian standard, OCTAVE and BSI, which consider security in an organizational scope, vulnerability might be a weakness in the actual procedures followed by employees [Alberts01].

In the information security context, vulnerabilities can be derived from [Sêmola03], [Mendes04]:

- physical vulnerabilities (e.g. a data centre without closed doors);
- natural vulnerabilities (e.g. a facility located 200 meters from a river likely to flood in winter);
- hardware vulnerabilities (e.g. server components difficult to replace, in case of failure or electromagnetic emanations [7], etc.);
- software (software *bugs*);
- media vulnerabilities (as for instance deterioration of paper);
- communication vulnerabilities (e.g. interruptions in Internet traffic);
- human vulnerabilities (i.e. the only clerical worker who knows the location of a type of documents will take a maternity leave);

The classification of vulnerability of a feature of an asset merely indicates that it has been utilised by a threat to violate the security of an organization. Vulnerability is simply a condition or set of conditions that may allow a threat to affect an asset [NIST01].

In conclusion, vulnerability for information security can be defined as a weakness associated with information systems [Sêmola03], or as a flaw in the organizational policies or workers' actions [Alberts02] that allows a threat to cause harm.

2.3.4 What is an impact?

The risk impact is measured by the extent of damage caused by a security incident in an organization [AS99].

GMITS, the Australian standard, OCTAVE and BSI concur that the impact should be evaluated in terms of CIA dimensions [ISO98], [AS99], [Alberts02], [BSI02].

[6] These authors regard vulnerabilities as a system's flaw [Albuquerque02], representing a point where the system is vulnerable to an attack [Russell92]. Peltier [00], who has the same position, reasons that the source of weaknesses can also be in the system's surroundings, in the application or at infrastructural level.

[7] A vulnerability common to electronic equipments is an emanation of electromagnetic waves. These waves permit the reconstruction of data, which is being processed and transmitted through the device. To remediate this potential leaking point, the US Department of Defense and NATO developed the program TEMPEST. TEMPEST endorses the use of fibre optics or STP cable instead of UTP cable, and the isolation of servers and terminals with copper plaques [Russell92].

Thus, the impact of a risk is determined by the level in which the damage is suffered by an organization, due to the unauthorised disclosure, modification and unavailability of information.

All these standards assume that the disclosure, modification or interruption of information (and of course, supporting systems) may cause significant negative consequences for an organization, as financial losses or harm to the organization's image. [8]

2.4 RISK MANAGEMENT FRAMEWORKS

2.4.1 Requirements of information security for risk management

The protection of valuable organizational information from the ever-changing vulnerabilities and threats has created two main challenges for risk management:

- risks affecting information processing are not the same as those of IT systems [Wadlow00], [Maiwald04];
- due to increasing exposure of organizations to information security risks, the activity of risk assessment has to be conceived as a continuous process [Braithwaite02] [Alberts02].

The first requirement involves the definition of the object according to risk frameworks. Traditionally, risk methods focused on technology assessments [Wright99]. As information overlaps the scope of systems, risk schemes have to assimilate the managerial and procedural dimensions of organizations in their evaluations. [9]

The latter requirement entails the definition of risk assessment as a continuous management process.

A turbulent business environment forces an organization's internal structure to undergo constant changes [Geus97]. The pace of these modifications fuel frequent alterations on IT platforms, and lead to the escalation of threats. As risks are swiftly changing; the assessment of them has to, therefore, be a permanent activity.

Furthermore, four risk frameworks are weighted against these two requisites. The purpose of this is to evaluate how risk methods tackle these issues:

- What is the object of assessments (it is system or it is information)?
- What is the managerial objective of risk evaluations (the purpose of risk assessment is to be a time restrict assessment or a permanent process)?

[8] The sense of *lack of security* felt by consumers towards e-commerce is regarded as one of the main obstacles for its development [Serrão02]. However, it has not been proved that the perceived overall security of an organization has the same importance for consumers to conduct *offline commerce.*

[9] Risk evaluations of information security, as seen further on, require, for instance the understanding of management instructions in the form of security policies and the examination of processes and procedures followed by workers. The object of assessment, consequently, apart of IT systems, it involves also documents, procedures and directives of the organization.

a) GMITS

The Guidelines for the Management of IT Security (GMITS), also referred as ISO 13335 is a suite of standards comprising of five documents:

- ISO/IEC TR 13335-1:1996, GMITS - *Concepts and Models for IT Security* [ISO96]; [10]
- ISO/IEC TR 13335-2:1997 GMITS - *Managing and Planning for IT Security* [ISO97]; [11]
- ISO/IEC TR 13335-3:1998 GMITS - *Techniques for the Management of IT Security* [ISO98];
- ISO/IEC TR 13335-4:2000 GMITS - *Selection of Safeguards* [ISO00b]; [12]
- ISO/IEC TR 13335-5:2001 GMITS - *Management Guidance on Network Security* [ISO01];

Part 3, ISO/IEC TR 13335-3:1998 GMITS - *Techniques for the Management of IT Security* [ISO98], addresses risk management.

GMITS defines risk management as “the total process of identifying, controlling, and eliminating or minimizing uncertain events that may affect IT system resources” [ISO98:p.I].

The GMITS presents the sequences of risk assessment phases without loop backs or without suggesting how to provide continuity to the process.

The above analysis of GMITS allows us to ascertain the two issues currently concerning risk management (defined at the beginning of this section):

- the centre of concerns of GMITS is the IT system, not information and;
- GMITS does not explicitly structures the risk process as an ongoing activity.

b) OCTAVE

Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) was released in 1999 by the Software Engineering Institute (SEI) of the US Carnegie Mellon University.

OCTAVE defines risk management as “the ongoing process of identifying risks and implementing plans to address them” [Alberts02].

In OCTAVE, risks are identified by an internal team, which in a series of workshops [Alberts02] develop qualitative evaluations of risks affecting the organization.

[10] The first Guideline provides recommendations for IT security management, and defines basic terms (threats, risks, vulnerabilities) and processes (contingency planning, risk analysis, etc.).

[11] Explains the design of IT security process and its integration into existing enterprise processes, as well as proposes an IT security organization.

[12] Part 4, *Selection of Safeguards*, gives information about which safeguards are relevant to which threats and how, for instance, a reasonable level of baseline protection can be defined for an organization.

As OCTAVE admits continuous monitoring is not addressed by the method [Alberts01]. OCTAVE is basically a qualitative assessment method, which can be integrated into a risk management framework.

Consequently, in terms of the two questions affecting risk management stated in the beginning of this section:

- OCTAVE assess the security of information (object of evaluation) and;
- although, OCTAVE emphasises the need for a continuous process, the method does not instruct how to achieve it.

c) BSI (BS 7799-2:2002)

BS 7799-2:2002 (or BSI) was originally published in 1998 by the British Standard Institution and revised in 2002 [BSI02]. [13]

This document is not, *in stricto sensu*, a risk methodology, but a guideline set for organizations, which seek to obtain an information security management certification.

BS 7799-2:2002 was designed to be an implementation guide of BS 7799-1 [AEXIS02], a countermeasures catalogue (described in chapter 4). Safeguards of BS 7799-1 had to be selected on the grounds of results on risk analysis. Consequently, risk analysis was a procedure to select adequate measures to an organization.

Risk management was subjected to hefty amendments in the last edition of BS 7799-2 [BSI02]. The most important was the adoption of the Plan, Do, Check, Act (PDCA) model, as observed in Figure 2.1. [14]

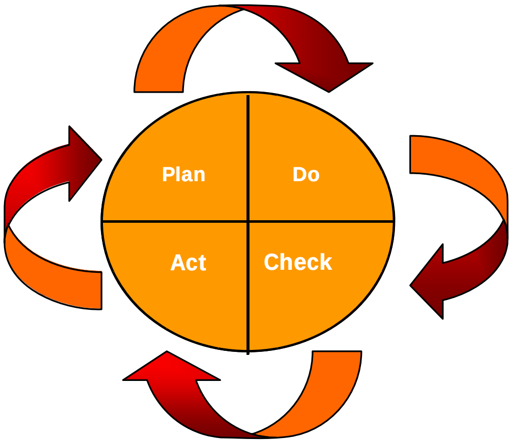


Figure 2.1: The PDCA model

[13] The actual title of BSI is BS 7799-2:2002 *Information security management systems - Specification with guidance for use* [BSI02].

[14] The Plan, Do, Check, Act methodology was inspired by the Japanese idea of Kaizen (continuous improvement process), which has popularised by total quality defenders [Capuder04]. Both the quality and environmental standards, respectively ISO 9001 and ISO 1400, employ this method, also known as Deming Wheel [IQP00].

The PDCA model solidifies the idea of a continuous risk assessment process [Gammassl02] in which managers monitor and control their security systems, thereby minimising the residual business risk and ensuring that security continues to fulfil the organizational and legal requirements.

The object of evaluation of BSI is information. Its purpose, as stated, is to "protect information assets and give confidence to customers and other interested parties" [BSI02:p.3].

In conclusion, with regard to the two questions mentioned at the outset of this section:

- risk management in BS 7799-2 is an ongoing process, supported by the PDCA model;
- BSI focuses on information protection.

d) CORAS (AS/ANZ 4360)

CORAS [Gran03] was published in 2003 by a European consortium, which was formed with the aim to produce a risk modelling toolkit [Houmb03]. [15]

CORA's framework is a comprehensive synthesis of the current state of the art of risk assessment of systems.

The evidence of the assembly made by CORAS is the source of its diverse aspects:

Risk management process: AS/ANZ 4360 [AS99], an Australian and New Zealand risk standard.

Risk assessment techniques: HAZard and OPerability study (HazOp), Fault Tree Analysis (FTA), Failure Mode and Effect Criticality Analysis (FMECA), Markov analysis methods, CCTA Risk Analysis and Management Methodology (CRAMM).

UML notation: ISO/IEC 10746 standard *Basic Reference Model for Open Distributed Processing* (RM-ODP).

As noted, CORAS adopted the AS/ANZ 4360 [AS99]. It is considered one of the first risk schemes in the world and was initially published in 1995 [Paul01].

The Australian risk standard defines risk management as "the systematic application of management policies, procedures a practice to the tasks of establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating risk" [Gran03:p.28].

As seen in Figure 2.2 the risk process involves, apart from sequential activities (establish context, etc), two vertical activities (monitor/review and communicate/consult), which interconnect the other sequential phases, ensuring a continuous loop.

[15] CORAS has been applied in the security modelling of a telemedicine application [Stamatiou03], adopted in thesis [Fredriksen02] and tackled in several papers [Raptis02], [Houmb03], [Aagedal02]. The CORAS official web site is: http://www.nr.no/coras.

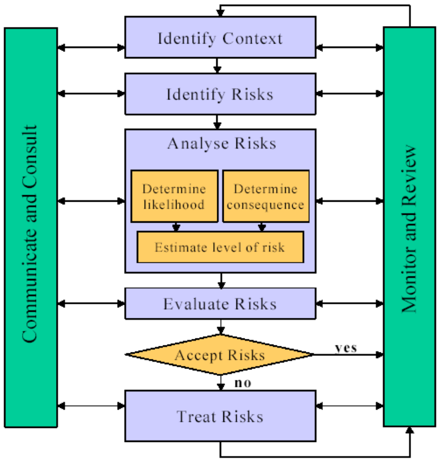


Figure 2.2: The Australian standard phases, AS/ANZ 4360 (extracted from [AS99])

CORAS assesses the Target of Evaluation (ToE), that is, IT systems and related documentation [Fredriksen02]. Accordingly, the assessment tools used by CORAS, as UML modelling and Fault Tree Analysis (FTA), are designated to address IT systems.

However, the aspects of information security - CIA dimensions - are used as requirements for the modelling security of systems.

It should be noted that the Australian risk standard, AS/ANZ 4360 [AS99], adopted as the risk management process by CORAS, is considered to have an information security and not a system security focus [Paul01].

To summarise in CORAS:

- the object of risk assessment is systems and;
- risk management is considered as a permanent process.

2.4.2 Selection of a risk framework: BS 7799-2

In the previous section it was shown that BS 7799-2:2002 (BSI) is the only risk scheme that complies with both of the two exposed requirements, as shown in Table 2.1.

Risk management scheme	GMITS	OCTAVE	BSI	CORAS
Focus on information not IT systems	No	Yes	Yes	No
Risk management conceived as a continuous activity	No	No	Yes	Yes

Table 2.1: Requirements of information security for risk management frameworks

Since BSI (1) centres its assessment on information and (2) perspectives risk evaluation as a continuous management process, this dissertation has adopted this risk management as its research framework.

Consequently, the subsequent discussion of risk management is supported by the BSI perspective.

2.4.3 Risk management according to BS 7799-2:2002 (BSI)

BSI defines risk management as “coordinated activities to direct and control an organization with regard to risk” [BSI02:p.I].

Risk management consists of several tasks, as illustrated in Figure 2.3. Initially, risks are identified and then an estimation is performed on their probability and impact on the organization. As a result of the analysis phase, risks are associated with the estimated level of danger that they pose to the business.

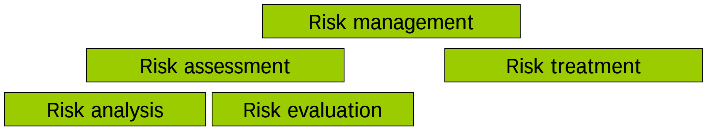
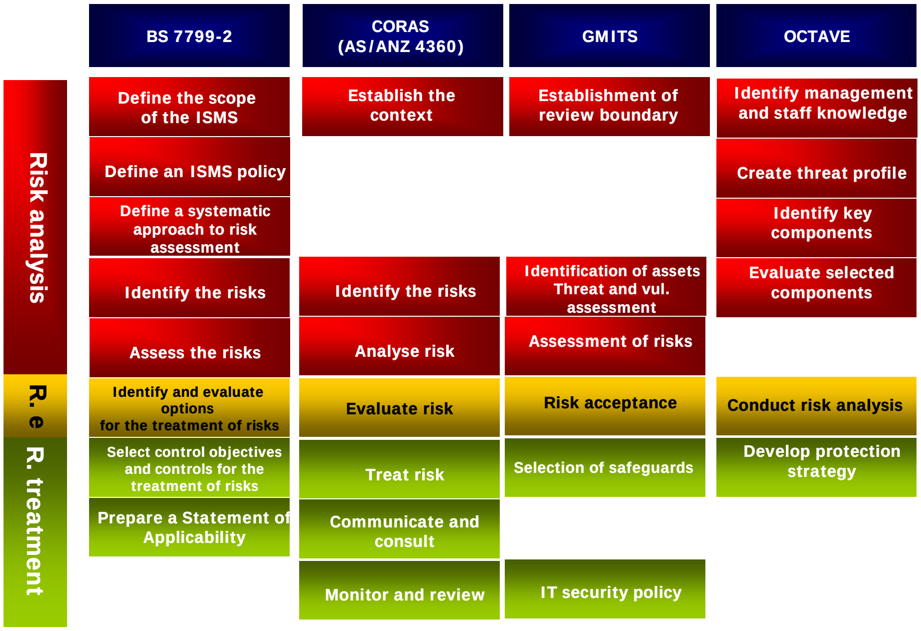


Figure 2.3: Risk management tasks according to BS 7799-2:2002

This level of danger is then compared to a given risk criteria in order to establish the significance of risk for the organization (*risk evaluation*). This evaluation determines whether or not a particular risk is beyond the tolerance level defined by the organization. All risks deemed as not acceptable have to be *treated*, that is, measures have to be implemented to modify the level of danger posed by the risk (*risk treatment*).



	BS 7799-2	CORAS (AS/ANZ 4360)	GMITS	OCTAVE
Risk analysis	Define the scope of the ISMS	Establish the context	Establishment of review boundary	Identify management and staff knowledge
	Define an ISMS policy			Create threat profile
	Define a systematic approach to risk assessment			Identify key components
	Identify the risks	Identify the risks	Identification of assets Threat and vul. assessment	Evaluate selected components
	Assess the risks	Analyse risk	Assessment of risks	
R. e	Identify and evaluate options for the treatment of risks	Evaluate risk	Risk acceptance	Conduct risk analysis
R. treatment	Select control objectives and controls for the treatment of risks	Treat risk	Selection of safeguards	Develop protection strategy
	Prepare a Statement of Applicability	Communicate and consult		
		Monitor and review	IT security policy	

Figure 2.4: Risk management phases according to several standards

All the mentioned schemes include (1) a risk analysis stage, where the risk is identified and estimated, (2) a risk evaluation step (R.E. in Figure 2.4) to decide what to do with the risk and (3) a risk treatment stage to implement the risk countermeasures previously decided.

Furthermore, it is possible to identify other similarities between the standards: (1) As shown in Figure 2.4, BSI, CORAS and GMITS start by defining the area of the organization, which will be subject to risk management. (2) For these risk schemes, identifying this area implies also establishing its context.

2.5 CONCLUSIONS

The chapter began by deconstructing risk into its underlying dimensions (asset, threat, vulnerability and impact) in the perspective of information security.

It was considered that security of information involves risks different from those of IT systems and requires a continuous management process. In the light of these considerations, four risk methodologies (BSI, CORAS, GMITS and OCTAVE) were evaluated.

This analysis revealed that:

- GMITS and CORAS assess risks associated with IT systems, while OCTAVE and BSI are targeted to risks concerning information.

- OCTAVE and GMITS do not provide guidelines to implement an on going risk process. On the contrary, BSI and CORAS included in the risk process, feedback loops between phases and instructions to constantly monitor and improve the protection level. Consequently, risk assessment, from a time limit activity, has become a continuous management process.

In conclusion, BSI is the only risk standard that (1) assesses the security of information and (2) conceptualises risk evaluation as a continuous management process. Therefore, BSI was selected as the risk management methodology reference in this research.

Furthermore, the risk methodology of BSI was divided into it three phases: analysis, evaluation and treatment of the risk. In consequence, as was shown for BSI, risk management involves the identification and estimation of risk (*risk analysis*), and then the comparison of the estimated risk to a given risk criteria in order to establish the implications of risk for the organization (*risk evaluation*). If the risk is regarded as intolerable, measures have to be taken to lower the risk level (*risk treatment*).

This chapter was able to demonstrate that the diverse risk frameworks converge with each other in the crucial steps of risk management: analysis, evaluation and treatment of risks. And that BSI, CORAS and GMITS share a preceding task of risk management: defining the organizational area subjected to evaluation (which involves establishing its context).

The following chapter will scrutinize these several tasks, investigating the procedures employed in implementations to identify, assess and mitigate risks.

3.

SYNOPSIS OF THE RISK MANAGEMENT PROCESS

> *Program* (and security) *testing can be quite effective for showing the presence of bugs, but is hopelessly inadequate for showing their absence.*
> *Dr. Dijkstra* [16]

3.1 INTRODUCTION

In the foregoing chapter, BSI was considered as the risk methodology more appropriate to assess risks affecting information resources.

The same chapter also disclosed the major phases of BSI´s risk management methodology (*cf.* 2.4.3).

The present chapter details these phases, examining how these guidelines are implemented in organizations.

Organizations to achieve the BSI´s certification must pursue the standard's methodology of putting into operation a security management system (*cf.* 1.2). According to these requirements, the implementation of a security management system, necessarily, involves the application of a risk management methodology [BSI02].

Based on this viewpoint, the current chapter scrutinizes the nine phases of BSI´s risk methodology, as illustrated in Figure 3.1, as a process to continuously identify, assess and treat risks within a framework of security management.

In each of these stages, the methodological requirements of BSI it will be summarized, interpreted and cross-referenced with the available literature concerning implementations of this methodology in organizations.

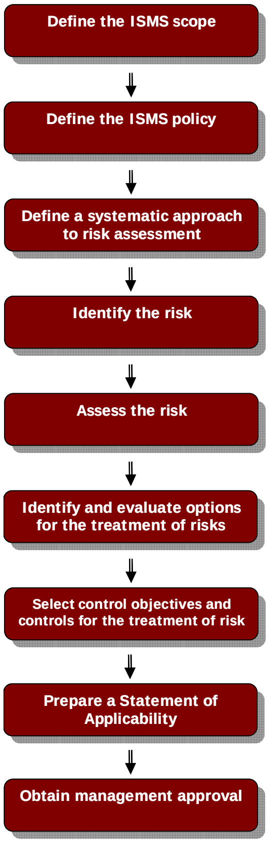

Define the ISMS scope
Define the ISMS policy
Define a systematic approach to risk assessment
Identify the risk
Assess the risk
Identify and evaluate options for the treatment of risks
Select control objectives and controls for the treatment of risk
Prepare a Statement of Applicability
Obtain management approval

Figure 3.1: BSI ´s risk management methodology

[16] Cited without bibliographic reference in Graff [03]. The author has added the word in brackets.

3.2 PHASE 1: DEFINE THE SCOPE OF THE ISMS

3.2.1 Overview

The opening task to put into practice a risk management process is to determine the boundaries of the evaluation realm (the area of the organization which will have its risks assessed).

3.2.2 Summary of BSI requirements

a) "The ISMS (*should be established)* within the context of the organization's overall business risks" (order of words was changed) [BSI02:p.3]
b) "Define the scope of the ISMS in terms of the characteristics of the business, the organization, its location, assets and technology." [BSI02:p.5]
c) "The ISMS scope documentation should cover:
   i) the processes used to establish the scope and context of the ISMS;
   ii) the strategic and organizational context(s);
   iii) identification of the information assets within the scope of the ISMS. "
   [BSI02:p.23]

3.2.3 Interpretation of BSI requirements

As observed, BSI [02] formulates three major objectives for this first phase:

a) Selection and characterization of the scope of the ISMS using a documented procedure (according to requirements *a*, *b,* and *c.i* in 3.2.2).
b) Identification of the legal constraints and business requirements for the security evaluation, which should be based on the analysis of the strategic and organizational context(s); (requirement *c.ii*).
c) Identification of the information assets within the ISMS (requirement *c.iii*).

These objectives can be materialized in the following deliverables:

a) a written description of the ISMS and its selection procedure;
b) a list of legal constraints and business requisites;
c) a list of information assets.

Next, the BSI requisites to accomplish these outputs will be examined.

a) Selection of the evaluation area scope

BSI does not provide any procedure to identify and select the ISMS (Information Security Management System, or in other words, the evaluation area). Therefore, an organization is free to choose the evaluation area as long as it:

a) justifies that the selected area pertains to its overall business security (according to requirement *a* in 3.2.2);
b) follows a documented procedure (applying requirement *c.i* in 3.2.2).

The first assertion, although not entirely explicit from the standard's text (*cf.* clause *a* in 3.2.2), is supported by the materials of the official ISMS implementation course from the British Standard Institution (referenced as [BSI03a]). The cited text course clarifies that the evaluation area should hold information and activities with a high business importance for the organization, i.e. critical to the business risk [BSI03a].

The same text course also recommends that the scope should be defined firstly in terms of information and its supporting processes [BSI03a] and then in terms of other dimensions as required by the standard (requirement *b* in 3.2.2).

The definition of the scope in terms of information and activities must be understand in the light of the information focus of BSI (instead of an IT system focus, as discussed in 2.4.2) and the process approach advocated by the British Standard Institution, *alma mater* of BSI (that is, BS 7799-2:2002). [17]

The scope can be viewed in terms of several dimensions, as defined in requisite *b* in 3.2.2 and illustrated in Figure 3.2. In fact, the evaluation area comprises of the information and its related production, transformation, storage, distribution and destruction activities.

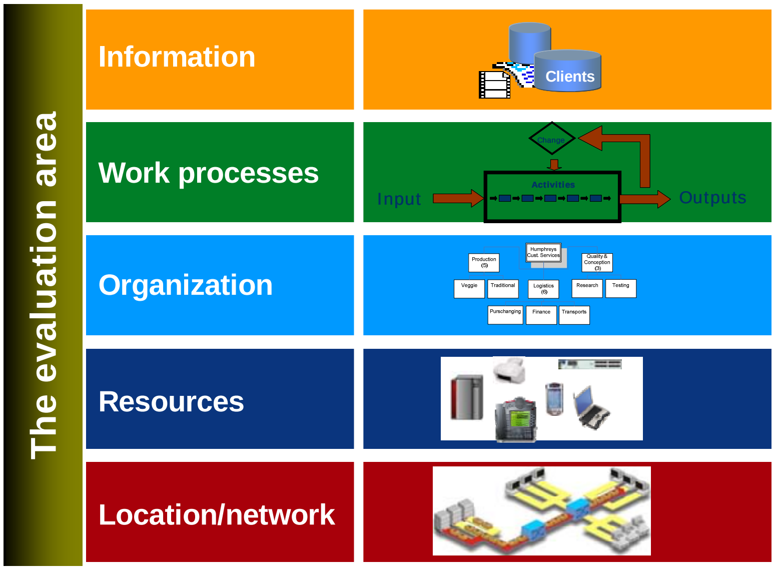


Figure 3.2: Some of the multiple subtracts of the ISMS

All these activities are presented in a process manner (i.e. identifying the input, transformation activities and deliverables). These processes require personnel (which are organized according to the organization structure), resources, all of which are located in specific physical and logical locations. Consequently, the scope should be defined in terms of the four dimensions, as depicted in Figure 3.2.

In synthesis, we may affirm that the evaluation domain can include the entire organization or be restricted to a specific part.

[17] According to a process viewpoint, all activities within the organization can be structured in a process manner that is identifying the inputs, the outputs and the transformation performed by each activity [BSI02]. An organizational process is simply an activity with an input and an output [BSI02].

In that case, the organization must sustain that this organizational area involves a specific type of information and organizational process which (1) is relevant to its overall risk level and (2) it was selected using a written procedure.

b) Identification of legal constraints and business requirements

As scrutinized, BSI requires understanding the strategy and organization structure, in order to determine the legal and business requisites for the evaluation area (*cf.* 3.2.3 b). These requisites play an important role in this process of assessing risks, since it is based on them that it is established the *amount of protection* required to defend the ISMS´s resources.

The security standard recognizes three sources of protection requirements: (1) risks, (2) legal and contractual requirements and (3) internal directives (business objectives and organizational principles) [BSI03a]. The first requisite is undertaken by the risk assessment method and reveals the *level of risks* affecting a particular asset (as seen further in 3.4). The second and last requirements are addressed by the investigation of the legal and business requisites, which are translated in the level of protection required (because of business and legal reasons) for that resource. [18]

c) Identification of information assets

As investigated (*cf.* 2.4.1), BSI aims to protect information. Consequently, the purpose of the evaluation area is to safeguard information (as well as its supporting processes). Therefore, to define the scope of security management (SM) within the organization, it is required to identify information assets, which for BSI [02] may be databases, electronic files, documents or manuals.

3.2.4 Analysis of available literature

a) Selection of the evaluation area scope

The review of literature tried to uncover the following:

a) Whether the current certified organizations had evaluated their entire structure or had restricted it to a specific part of them?
b) If so, what were the organizational areas most frequent on those corporations?
c) How the evaluation area was selected?

In order to respond to the two initial questions, the scope of the certified organization was analysed.

[18] The level of protection may be commanded by business and/or legal justifications. An outsourcing service company that is trying to attain the BSI certification to gain client confidence probably will have a soaring protection requirement for assets related to outsourcing. An illustration of a law with an impact on the level of security for a resource is the Portuguese data privacy law (*Lei de Protecção de Dados Pessoais*, law number 67/98 from 26th October) that forces a tight protection of personal data of employees and clients.

At the moment of writing (August 2004), 890 organizations in 41 countries had been certified by BS 7799-2 (BSI). [19] However, only 126 organizations have disclosed their scope. [20] Although, these scope descriptions are not absolutely clear about this issue, all of them show traces of process or area delimitation within each organization.

The examination of these scope statements showed a convergence in the areas included in the ISMS, as depicted in Figure 3.3.

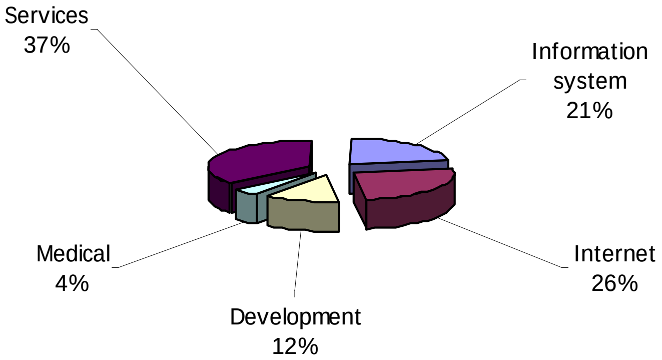


Figure 3.3: Organizational areas included in the scopes of the ISMS (analysis performed by the author)

A large number of ISMS´s (37 % of the publicly available) is related to services, either for external customers (as EDS Security & Information Assurance from the UK, which has certified security services), or internal customers as the Federal Reserve Bank of New York (US), which has certified internal services provided by the security department.

The operation of Internet platforms accounts for 26% of the ISMS´s. This involves companies, such as *Sociedade de Lotarias e Apostas Mutúas de Macau* (China), which has certified the IT operations that support an internet betting service, or *Istituto Bancario San Paolo* (Italy) that has included in the ISMS the area of Internet banking. Information systems are accountable in 21% of the ISMS´s.

An example is *Organismo Publico Descentralizado Municipal* (Mexico), which has certified the maintenance and operation of the domain server and a data base server.

An example of ISMS involving system development is Ericsson Spain, which has confined the ISMS to the development and supply of a specific software and related documentation. Implementations in medical environments (hospital, clinics) and system development are responsible together for 16%.

Most of the above examples and available ISMS descriptions reveal that a process approach was followed. The actual scopes define the ISMS in terms of activities, which are depicted in a process manner [21], instead of a department or business unit.

[19] In 2004 in Portugal there was any BSI certified organization.

[20] Those organizations revealed descriptions of their ISMS scopes. These scopes are available at http://www.xisec.com.

[21] Clear examples of these are NTT-ME Corporation (Japan), which has certified operations *processes* within the data centre and NHS Purchasing and Supply Agency (UK), which confined the ISMS to security management of the purchasing *process*.

In the light of these findings, this research found two methods to select the evaluation area. The first approach is supported by the works of BSI practitioners, such as Sêmola [03], Mendes [04], Kadam [03] and Syta [01]. The second approach is recommended by the BSI´s training course [BSI03a].

Both of them abide by a process viewpoint and documented the selection of the most important area of the organization, as required by BSI. The first method starts by delimitating the process(es) within the ISMS and then defines the information and other resources. The second approach begins by identifying the information inside the scope and afterwards the processes, as further explained in A.2.

To sum up, it seems that evaluation area is, usually, confined to a process(es) within an area of an organization. [22] The most frequent areas are services (37 % of the studied scopes), Internet platforms (26 %), information system (21 %), system development (12 %) and medical (4 %).

Not a single implementation report was found indicating the selection process followed. Nevertheless, it was compiled two selection procedures, which were advocated by security authors. The first approach to elect the evaluation starts by identifying the organizational processes, and in this context it can be designed as process-based. The second commences by identifying information and therefore may be referred as information-based (*cf.* Annex A.2.2).

b) Identification of legal constraints and business requirements

As expected, organizations do not unveil their security requirements or constraints. Therefore, analysis could only recognise external sources of security requirement with influence in a BSI implementation.

In terms of legal requirements, organizations are subjected to an increasing number of laws and regulations concerning security aspects.

Governmental bodies, as the Data Protection National Committee (*Comissão Nacional de Protecção de Dados*) in Portugal, are a prolific source of security regulations [Silva03].

Another external foundation for security requisites is regulations for specific business areas. Examples of these are (1) Health Insurance Portability and Accountability Act (HIPAA) [23] for healthcare organizations in the US; (2) CEN/ENV 12924, Medical informatics - *security categorisation and protection for health care information systems.*

[22] The author was only an exception of this trend: Plate [02] states that T-Systems CSM, a *Deutsche Telekom* Group company (Germany), had an evaluation scope that included the entire organization. The scope descriptions are not absolutely clear about this issue, but all of them show traces of process or area delimitation within each organization.

[23] The Health Insurance Portability and Accountability Act (HIPAA) is a standard for the protection of health information involving security measures in several areas. It is defined to be active by 2005 [Borkin03].

In Europe, as registered in a report from a Italian Hospital implementation [Cavalli04]; (3) Basel II for worldwide banks [24]; and (4) Graham Leach Billey Act (GBLA) and Sarbanes-Oxely Act [Mainwald04] for companies listed on the US stock exchange.

According to Brewer [04], Sarbanes-Oxely Act (SoA) and Basel II are two driving forces which are impelling organizations to security certification.

c) Identification of information assets

Alternatives understandings of the concept of information assets are available. For Ferrant [04], information assets are pieces of information involved in work processes. Therefore, any information can be classified as (1) input, (2) outputs and (3) records of a process.

Conversely, Mendes [04] classifies information asset according to its type of repository (a database, a file cabinet, a specialized worker). [25]

3.3 PHASE 2: DEFINE AN ISMS POLICY

3.3.1 Overview

Subsequent to identifying the evaluation area, it must be defined *what to protect*. Security policies establish the goals of security management (SM).

3.3.2 Summary of BSI requirements

In this subject, BSI redirects to ISO [00a], the safeguard catalogue, which is the counterpart of BSI.

In accordance with ISO, organizations ought to define (1) an information security policy and (2) its associate regulations. ISO is specific about the content of this document. Accordingly, an information security policy should include:

a) the objectives and scope of the information security for the organization;
b) a management statement in support of the information security efforts;
c) the applicable legal, regulatory and contractual requirements to the organization;
d) the overall responsibilities of information security management;
e) reference to more specific security regulations of the organization (as specific policies, internal standards, guidelines and procedures).

[24] Basel is an agreement under the Bank of International Settlement that establishes the rules for permitting funding between banks [Brewer04]. Basel II institutes a relationship between the risks assessed for a bank and the amount of working capital that needs to be set aside to cover that risk, therefore reducing the assessed risk release capital. Through this manner, Basel II provides an incentive for banks to assess and reduce the risk. As a result, banks may adopt IT risk management methodologies as BSI.

[25] Employees are viewed as information resources as they are regarded as the main holder of information in organizations [Mendes04].

3.3.3 Interpretation of BSI requirements

ISO establishes a hierarchy of security regulations (as observed in requisite *e* in the previous section) and illustrated in Figure 3.4.

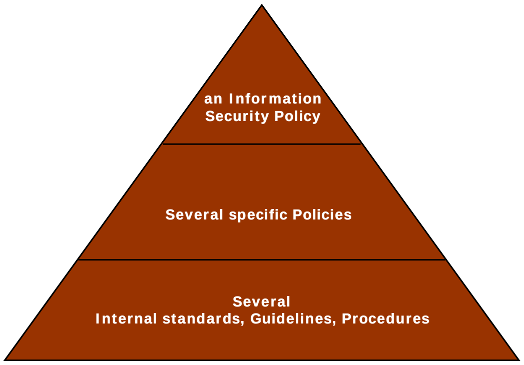

an Information Security Policy
Several specific Policies
Several Internal standards, Guidelines, Procedures

Figure 3.4: Type of security regulations according to ISO [00a]

At the top is the information security policy, which is a document that must cover the issues defined by ISO (as seen in the previous section). This overall charter is further detailed by particular policies concerning specific issues, as business continuity management. At a more operational stage, there are the internal standards, guidelines and procedures, which are addressed in Annex B.2.2.

Therefore, the outputs of this stage are (1) a top security policy document to provide overall guidance and (2) other documents as procedures to specify how to perform the required actions.

3.3.4 Analysis of available literature

As noticed, ISO does not mention the course of actions to formulate security norms. Impelled by this circumstance, the literature investigation tried to ascertain *what methods are employed to define policies and regulations*.

A number of authors provide guidelines to define security policies and procedures [Guel01], [Crabb01], [Kadam03], [Brykczynski03] and [Rees03]. However, those methods do not comply with the requirements of ISO for a policy.

A security policy under ISO has to be: (1) aligned with organizational objectives, (2) and has a strategic and not only a tactical or operational purpose [26] (*cf.* section A.4.3).

An exception is Policy Framework for Interpreting Risk in E-Business Security (PFIRES) [Rees03]. This process develops policies in line with organizational objectives, because prior to any policy definition, external requirements are assessed and a security objective is articulated [Rees03].

[26] For ISO, security policies are strategic statements that define the objectives and guidance principles of security management. Other forms of regulations, as standards and procedures are more operational.

Similarly, [Kadam03] and [Brykczynski03] advocate that policies should be based on a security objective that identifies what processes and assets are worth protection [Kadam03] and to what degree of assurance.

Brykczynski [03] distinguishes three phases in this process: (1) definition of top-level security policy; (2) identification of applicable standards, regulations, and legal requirements; (3) definition of implementation-level policies (that is, procedures).

In sum, two methods to establish security norms, with the ISO outlook, were found: PFIRES [Rees03] and Brykczynski [03]. The former approach clearly derives policies from the organization strategies and the last advocates gradual phases to define the strategic policy and then the more operational norms (based on external requirements).

3.4 PHASE 3: DEFINE A SYSTEMATIC APPROACH TO RISK ASSESSMENT

3.4.1 Overview

Prior to undertake any assessment of risks, organizations are required to define how the risks will be estimated.

3.4.2 Summary of BSI requirements

a) Risk assessment method must be “systematic” [BSI02:p.3]

b) “Identify a method of risk assessment that is suited to the (1) ISMS, and” for the “(2) business (…) legal and regulatory requirements.” [BSI02:p.23]

3.4.3 Interpretation of BSI requirements

To understand what is risk assessment method it is necessary to scrutiny the concept of risk assessment for BSI. According to this standard, all risks must be identified by a measure (a value or a qualitative attribute) indicating its degree of dangerousness. This measurement will be used to decide what to do with each risk.

BSI requires that risk be estimated using variables such as (1) impact value and (2) probability [BSI02]. Therefore, organizations must use a risk assessment formula to combine those elements in a risk measurement.

In sum, at this phase it (1) must be established a risk assessment method (an equation between probability and impact value to produce differentiate levels of risk) appropriate to the evaluation area (or ISMS) and legal and organization requirements and constraints. This scheme (2) must be applied consistently in all the assets and throughout the all process (that the interpretation of systematic).

The deliverable of this phase is, as demonstrated, the definition of the risk formula.

3.4.4 Analysis of available literature

As expectedly, BSI does not endorse any procedure to assess risks. The literature review exposed that *different types of scales where employed by the risk estimation formula to gauge risks.*

Cases were found where some risk algorithms would classify risk according to a monetary scale, while other employs a non-monetary scale, as analysed in Annex A.3.2.

BSI does not opt for a monetary or non-monetary paradigm. However, documents from the British Standard Institution subscribe the risk calculations methods from GMITS, which are an archetype of non-monetary formulas. [27]

Both approaches converge on the assertion that the dangerousness of risks depends of its likelihood and the value of the assets that it affects, or in order words, its negative consequences for the organization.

The use of a factor as subjective as probability to calculate risks is criticised by OCTAVE, which classifies risks based only on its impact.[28]

However, Mendes [04] considers that one-factor formula, as OCTAVE, can distort risks. Supposedly, for OCATVE, an earthquake and a fire can be classified as similar risks, due to causing similar impact. Nevertheless those risks have different probabilities. In continental Portugal, for example, a fire is much more probable than an earthquake.

To summarised, an organization can use monetary scales [as Exposure Factor, Single Loss Exposure (SLE) and Annualised Loss Exposure (ALE)] or non-monetary scales (as GMITS [ISO00b]) in the estimation of risks (*cf.* Annex A.3).

3.5 PHASE 4: IDENTIFY THE RISKS

3.5.1 Overview

According to an axiom, an organization can only protect itself against known threats [Wadlow00]. In this context, the importance of threat identification is high, since this task will limit the range of planned defences against threats.

3.5.2 Summary of BSI requirements

[27] The *Guide to BS 7799 Risk Assessment and Risk Management* [Humphreys02b], published by the British Standard Institution, describes the underlying concepts behind risk assessment. This document is based on GMITS [ISO00b] (*cf.* Annex A.3).

[28] OCTAVE [Alberts02] advocates that risk should only be assessed considering the impact and not on something as fluid as probabilities. Thus, this method uses a scale of low, medium and high impact to classify risks.

a) “Identify the threats to those assets.
b) Identify the vulnerabilities that might be exploited by the threats.
c) Identify the impacts that losses of confidentiality, integrity and availability may have on the assets.” [BSI02:p.5]

3.5.3 Interpretation of BSI requirements

The outcome of this phase is a list of risks. To produce this list the following sequence of practices should be followed: start discovering (1) the threats affecting resources within the ISMS, then (2) the vulnerabilities and finally (3) the impacts that losses of confidentiality, integrity and availability may have on the assets. Nevertheless, BSI [02] does not specify an operational method to perform these chores.

3.5.4 Analysis of available literature

As BSI does not provide any method to identify threats and vulnerabilities, risk practitioners are urged to import these from other areas. In this context, a number of threat identification methods may be applicable to a BSI process:

a) Threat catalogues (imported from GMITS [ISO98] - *cf.* 2.4.1 - and other sources);
b) Attack trees (popularised by Schneier [99]);
c) Threat profiles (from OCTAVE, a risk standard studied previously in 2.4.1);
d) Threat modelling methods (from CORAS, introduced in 2.4.1).

From these methods, it was found only evidence of the usage of threat catalogues, in an Italian hospital implementation [Cavalli04]. However, the remaining approaches may be helpful in identifying threats affecting IT system (specially, attack trees and modelling methods from CORAS) and general threats (using threat profiles), as further examined in Annex A.4.2.

At the same time that threats are identified, it is recommend to perform the identification of vulnerabilities [Syta01], [Yazar02]. This is due to the fact that during the detection of vulnerabilities new threats may be found as well as during the description of threats, new vulnerabilities may be discovered.

Organizations can make use of diverse tools to detect vulnerabilities, depending if they are sonly technological or general vulnerabilities, as scrutiny in Annex A.5.2.

Gap analysis - a form of general vulnerability identification (studied in Annex A.5.2.2) - has echoes of utilization. [29]

Gap analysis is the underlying principle of the questionnaires, employed by CORAS, CRAMM [30] and some other risk identification software [31], to establish vulnerabilities.

[29] GAP analysis compares prevailing controls in an organization against a safeguard catalogue [Doughty03], [Sêmola03]. The lack of a control from the catalogue reveals an unconformity and it might suggest the existence of a risk [Cavalli04].

In sum, it seems that BSI certified organizations have employed numerous risk identification methods and some organizations may even use several methods. [32]

3.6 PHASE 5: ASSESS THE RISKS

3.6.1 Overview

Subsequent to discovering risk, they must be assigned with a measure, indicating its degree of dangerousness. This phase is the application of what was defined in stage 3 (*cf*. 3.4).

3.6.2 Summary of BSI requirements

According to BSI a risk must be calculated based on its impact and probability [BSI02]. Therefore, the risk estimation is anchored in:

a) “The business harm that might result from a security failure, taking into account the potential consequences of a loss of confidentiality, integrity or availability of the assets.

b) The realistic likelihood of such a security failure occurring in the light of prevailing threats and vulnerabilities and impacts associated with these assets, and the controls currently implemented.” [BSI02:p.5]

3.6.3 Interpretation of BSI requirements

As examined in section 3.4. BSI demands that the level of menace for the organization of each risk be assessed. This implies that each risk must be measured.

Consequently, at the end of this stage, each risk must be associated with a calculated risk level (an estimation of the probability and impact of a risk).

The measurement formula, according to BSI requisites, may be sensitised as shown:

Risk = impact x probability

Risk = (breaches of C.I A.) x (threats x vulnerabilities x impact)

[30] In CTTA Risk Analysis Management Methodology (CRAMM) tables of threats are assigned to types of asset. Through a questionnaire, with questions derived from ISO, the asset owner defines how expose is the asset [Yazar02]. CRAMM method was developed by UK Security Service, a commercial CRAMM tool is available at http://www.cramm.com. CRAMM was used in several BSI implementations, such as Bank’s “Smile” Internet Bank, DTI, Serious Fraud Office, GTECH UK [Insight04] and UK National Health Service [Lillywhite02].

[31] There are more than 200 software’s packages that perform risk identification [BSI03a]. Famous examples include Automated Livermore Risk Analysis Methodology (ALRAM) and Consultive and Bi-functional Risk Analysis (COBRA) [Perltier00].

[32] This assertion is grounded on the combined use of threat catalogues (*cf.* A.3.1) and Gap analysis (*cf.* A.5.2.1) in an implementation reported by Cavalli [04].

As observed, the gravity of each risk depends of the extension of the (1) associated impact and of (2) temporal proximity degree that the risk is expected to occur.

By one side, the deeper the impact, the higher the risk is. A risk is less or more perilous depending of the level that endangers the overall organization's information security. In this circumstance, a risk is high if it seriously affects a resource relevant to the organization's business, which in consequence, can have a negative influence in the whole organization. By another side, if this risk is likely to happen soon or/and occurs often, the more hazard it represents.

The calculation of this equation encounters difficulties, especially with probability. If it is easy to foresee possible impacts of risk, it is much more challenging to predict its likelihood. For example, it is relatively easy to anticipate the consequences of a devastating fire on the organizational facilities, but is difficult to assess its probability of happen.

3.6.4 Analysis of available literature

Inspired by the complexity of assessing the probability, the literature appraisal concentrated on this question. In the end, it was establish that probability can be estimated only based on one variable or in several risk ingredients, as more granularly studied in Annex A.6.

As observed, probability, for BSI [02], it should be assessed in line with threats, vulnerabilities and impacts associated with the asset. This view (that the probability of a risk should be estimated based on a group of factors related to the asset and threat) is shared by GMITS [ISO98], OCTAVE [Alberts02] and CORAS [Gran03].

Oppositely, AS/ANZ 4360 [AS99] anchors probability in the resource's characteristics, not considering the threat agent. [33] The Australian standard regards the probability of a risk as a function of factors associated with assets. According to this perspective, the likelihood of risk depends upon the easiness of exploiting a vulnerability and surpassing the protective countermeasures of an asset [AS99]. This measurement will be used to decide what to do with each risk, as detailed in next section.

3.7 PHASE 6: IDENTIFY AND EVALUATE OPTIONS FOR THE TREATMENT OF RISKS

3.7.1 Overview

At this point, an organization has to decide whether the recognised risks are acceptable or not. When the risk is accepted by management, it only has to be monitored. On other hand, when the risk is considered not acceptable, the organization has to adopt a strategy to alleviate the burden that the risk poses.

[33] Factors related to the treat agent that may influence its dangerousness level are for example the motivation and skinless of the threat agent to engage the risk.

3.7.2 Summary of BSI requirements

BSI [02] stipulates four alternatives to risk treatment: (1) acceptance, (2) transference, (3) avoidance or (4) mitigation.

3.7.3 Interpretation of BSI requirements

At this stage, organizations are asked to separate the risk regarded as acceptable from those which are not, and consequently have to be subjected to treatment.

All identified risks that endanger the organization must be subjected to a management decision. The risk must be either:

a) accepted it (the potential effects of the risk is acknowledged, but it is regarded as lenient or beyond a reasonable business effort);
b) avoided it (prevent the cause and/or the effects of the risk, by for example preventing the use of the asset affected by that risk);
c) transferred (handover the negative effects to another party, frequently to insurer or suppliers);
d) reduced through the application of security controls. [34]

This decision is the deliverable of this phase.

3.7.4 Analysis of available literature

There are no reports showing *how the decision to accept or treat a risk is taken by organizations*. However, implementations guidelines of several sources can be grouped in three categories.

The decision of *what to do with a risk* can be sustained by three factors: (1) risk attributes (as impact and probability); (2) protection need or (3) a combination of both.

In the first possibility, organizations use the risk ingredients, namely impact and probability (*cf.* 3.6.2).

As illustrated in Figure 3.5, each possible value of impact and probability is associated with a risk decision. In Nordin [03], for example, a risk with a high probability and a low impact must be mitigated. Alternatively, for Cavalli [04] a risk with the same characteristics must be transferred.

[34] An example of risk acceptance is an organization considering as negligible the risk of desktops being infected with an antivirus undetected new worm. In this situation, the risk is acknowledge (i.e. identified), but it is regarded as being not technically practically or business reasonable to try to mitigate it further. In other words, the organization accepts to tolerate that risk, because it can not reduce it. Risk mitigation happens when an organization decides to apply countermeasures to reduce the effects of a risk. An example of risk avoidance is an organization preventing the risk of Internet attacks by not being connected to it. Risk transfer is, for instance, a company taking out insurance to cover eventual hackers' attacks or outsourcing its IT security management.

Impact	Likelihood	
	Low	High
Low	Accept the risk	Reduce the risk
High	Transfer the risk	Avoid the risk

Impact	Likelihood	
	Low	High
Low	Do nothing	Transfer the risk
High	Crisis management	Lower the risk level

Figure 3.5: Risk options based on its attributes, according to [Nordin03] and [Cavalli04] (right)

Following this approach, organizations simply assess whether every risk represents a serious hazardous, and if therefore, can be positioned, within an organisation’s *conformable zone* [Mendes04] or by other risks are intolerable and must be treated.

Another hypothesis to support this decision is on the protection need. Regardless of the level of danger of the risks affecting an asset, the decision is sonly based on the degree of assurance of the asset. In this ambit, a risk is tolerable or unacceptable depending on the business value of the resource affected by it.

An illustration of this tendency is Ferrant´s [04] proposition of attaching the risk acceptance criteria only on the degree of assurance.

The third decision making alternative aggregates the last two procedures. The decision is taken bearing in mind the level of risk and the degree of assurance. A paradigm of this approach is GMITS [ISO98]. This standard, endorsed by Humphreys [02b], advocates that circumstances related to the asset and to the threat should be taken into account to determine if the risk is accepted or not. These three types of risk decision are summarized in Figure 3.6.

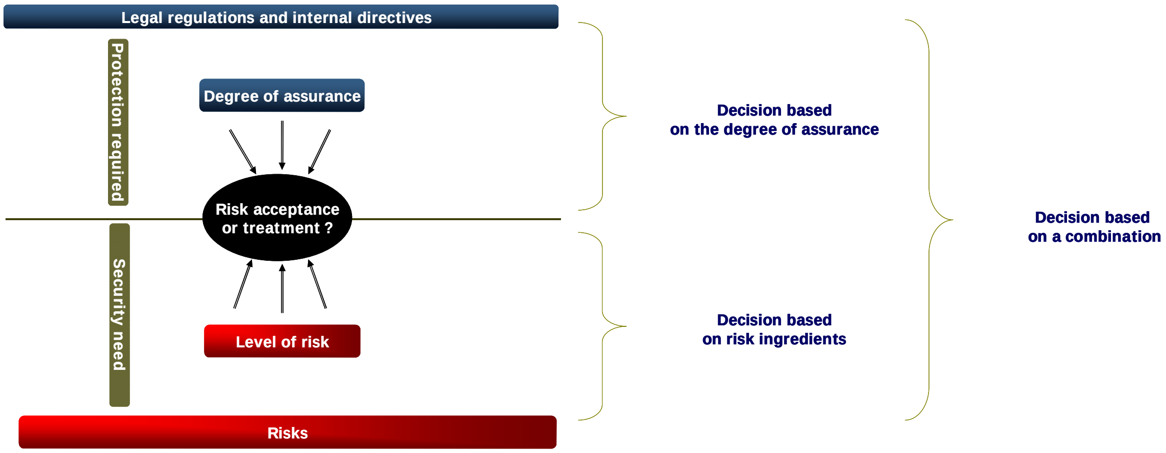

Legal regulations and internal directives
Protection required
Degree of assurance
Risk acceptance or treatment ?
Security need
Level of risk
Risks
Decision based on the degree of assurance
Decision based on risk ingredients
Decision based on a combination

Figure 3.6: Risk acceptance/treatment decision alternatives

The risk may be acceptant or subject to lessen based only on the degree of assurance or on the level of risk or finally on a combination of both.

If the risk is considered as not acceptable, it has to be subject to one of the treatment options: avoidance, transference or mitigation. In this last alternative, controls must be applied to it, as explained in next section.

3.8 PHASE 7: SELECT CONTROL OBJECTIVES AND CONTROLS FOR THE TREATMENT OF RISKS

3.8.1 Overview

At this moment, the organization is expected to define measures to *treat* the risks regarded as non acceptable, in the preceding phase.

3.8.2 Summary of BSI requirements

The output of this phase is the risk treatment plan. This document identifies for each risk: (1) a method for treating it (established in the foregoing phase); (2) the most suitable strategy to pursue the selected objective, which can be, for instance, to transfer the risk or mitigate it. In the last case, BSI requires that the strategies to reduce the identified risks be selected from a list of controls, placed at Annex A in this standard's text.

However, as this list is "not exhaustive" [BSI02:p.6], additional countermeasures can be drawn from other sources, as long as those supplementary controls "exceed the level that can be managed" [BSI02:p.24] with the BSI´s suggested measures. [35]

Nevertheless its source, each planned risk measure must have been regarded as appropriate to (1) mitigate the level of danger of a risk and to (2) the degree of protection sought by the organization.

3.8.3 Interpretation of BSI requirements

A number of possible countermeasures can be applied to the identified risks. The organization has to develop a risk treatment plan that includes:

a) *Strongly recommended safeguards* - 8 controls from BSI´s Annex A, are regarded as "guiding principles (…) for implementing information security" [ISO00a:X]. And therefore, they are deemed as applicable to all organizations.

b) *Selective safeguards* – the remaining 119 controls from Annex A may be chosen or may be excluded, if:
   - considered as not applicable to the organization;
   - regarded as applicable to the organization, but excluded, if (both conditions are meet):

[35] For instance, an organization may regard the controls for removable computer media (tapes, disks, cassettes and printed reports) on ISO insufficient for the low risk level they are attempting to implement. In this circumstance, the organization may adopt supplementary controls, which increase the assurance level beyond a point ensured by ISO. Those controls can be extracted from any standard or created by the organization.

a) deemed that their exclusion, does affect the organization's ability to provide information security in conformity with the security requirements and applicable regulations and;

b) the risks associated with the non-implementation of a control are accepted in written by the organization's senior management.

c) Measures not derived from BSI but defined by the organization as necessary because provide more assurance than the standard's controls in that particular situation.

The first group of controls is formed by 8 controls of BSI which are related to compliance with legal requirements or considered to be common best practice for information security and as a result, regarded as eligible by all organizations.

The second and third group of measures is formed by strategies to mitigate the risks identified during the assessment process, which are either based on Annex A of BSI or any other source, as long as those measures are regarded as providing a higher protection level in comparison with those mentioned controls.

The cited countermeasures from Annex A of BSI are reproductions of the controls of the 127 controls of ISO [00a], the safeguard catalogue sibling of BSI. Annex A expresses the same controls of ISO using a more normative terminology. [36]

In the last two groups, the organization has the capacity to decide which measures are necessary to reduce the identified risks, taking into account the group of potentially applicable controls of ISO (or even harsher controls).

The discriminatory power of deciding which measures (from the list of ISO) are adequate to the risk is restricted by the imposition of justifying that the selected countermeasures actually (1) reduce the risk level (2) in accordance to the assurance degree required by the organization

3.8.4 Analysis of available literature

As seen, the selection method of countermeasure adopted is based on risk analysis. The available literature uncovers two processes to select countermeasures: (1) risk analysis, or (2) application of a security baseline.

In the first approach, each safeguard is selected in conformity with the estimated level of risk that threats pose to a particular asset.

On the contrary, in a baseline approach, a predefined set of controls is selected, based on the assumption that it provides protection against most threats affecting those types of assets [ISO97].

[36] The content of the controls are the same, the difference is that BSI uses "*shall*", while ISO employs "*should*". For example, for BSI the statement is "a policy document *shall* be approved by management" [BSI02:11], and ISO conveys as "a policy document *should* be approved by management" [ISO00a:1]

BSI [BSI02], GMITS [ISO98], OCTAVE [Alberts02] and AS/ANZ 4360 [AS99] are examples of risk-oriented methodologies. All of them identify assets and their associated threats and vulnerabilities to establish the risk level. It is based on the individual assessment of risks that measures are selected.

Baseline methodologies propose incremental sets of controls that provide increasing levels of protection. An illustration is NIST SP 800-53 *Recommended Security Controls for Federal Information Systems* [NIST03], which is structured in three baseline levels, low, medium and high. Each baseline has its own specific controls.

Another example is Systems Security Engineering Capability Maturity Model (SSE-CMM) [ISSEA03], which proposes a scale with 5 security baselines, as shown in Figure 3.7 [37]

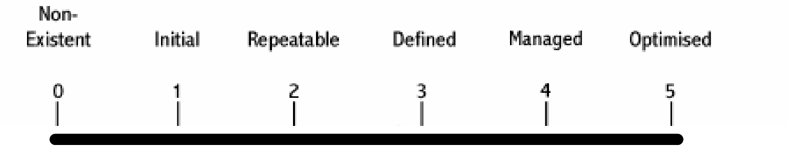


Figure 3.7: Maturity model of SSE-CMM (Extract from [ISSEA03])

SSE-CMM employs a maturity model that ranks organizations according to the level of formalisation of IT security management processes, as seen in Figure 5.9. [38]

Although BSI follows a risk analysis approach, it has been discussed the possibility of the adoption of an incremental scheme [Solms01a], [Lillywhite04].

According to cited authors, BSI requires organizations to compare their security implementations with a paradigm of 127 controls, which leads organizations to a quandary of not knowing which controls should be applied in the first place.

Contrary, to the *all-or-nothing* design of BSI, the Information Security Institute of South Africa (ISIZA) suggests a certification based on ISO controls with 5 levels [Solms01b]. Each of the levels contains a subset of ISO controls.

In this manner, an organization could gradually move from one level to another until it eventually reaches the top level, which would then be tantamount to a full BSI certification.

In the same way, the Information Governance programme in the UK has developed a set of attainment levels, scaled from 0 to 3, as a ready and relatively simple means of measuring progress towards compliance with BSI [Lillywhite04].

[37] Those levels mean: 0-Non-existent (management processes are not applied at all); 1-Initial (IT management processes are initial and ad-hoc); 2-Repeatable (IT management processes are repeatable but intuitive); 3-Defined (IT management processes are documented and communicated); 4-Managed (IT management processes are monitored and measurable); 5-Optimised (best practices are followed and automated) [ISSEA03].

[38] The idea to use scales to evaluate security implementation in organizations had echoes in Murine and Carpenter or Stacey [Siponen03]. NIST is at the moment a strong supporter of this approach, as demonstrated by the NIST Computer Security Expert Assist Team (CSEAT), an evaluation scheme for public institutions based on Capability Maturity Model (CMM) [Nash03].

In conclusion, concerning this question of safeguarding selection methods founded on risk analysis or security baseline, we may say that:

- baselines are said to be (1) easier to implement than risk analysis and [Nash03] (2) facilitating comparisons between organizations [Solms01a];
- risk analysis is more flexible than baselines, as controls are based on the organization's situation to the risk

3.9 PHASE 8: PREPARE A STATEMENT OF APPLICABILITY

3.9.1 Overview

BSI requires the composition of a document mapping the controls applied by the organization to the controls of ISO [ISO00a]. This document is entitled as Statement of Applicability (SoA).

3.9.2 Summary of BSI requirements

For BSI, the Statement of Applicability (SoA) ought to include (1) the controls of ISO previously selected [39], and (2) the reasons for its selection or exclusion.

The organization may also compose another document with the applied controls of BSI´s Annex A, designated as Summary of Controls (SoC), which can be disclosed among partners.

3.9.3 Interpretation of BSI requirements

It can be reasoned that a SoA, the clear output of this step, serves two purposes: (1) allows comparison of security efforts between organizations and (2) verifies the compliance by organizations with ISO in order to issue the BSI´s certification.

In relation to the first question, SoA enables organizations with different security management systems to be compared against a common yardstick: the 127 controls of ISO [Grammassl02]. [40]

Due to this comparative function, some certified organizations have expressed the need to document the list of controls appropriate for disclosure between clients and partners. [41]

[39] As mentioned in 3.8.3, the countermeasures of ISO are reproduced at Annex A of BSI document.

[40] As mentioned, in order for an organization to be recognised as BS 7799-2:2002 (or simply BSI) certified, it must prove its compliance with ISO (or more precisely to the Annex A of BSI - *cf.* 3.8.3).

[41] The second edition of BSI (2002) entitled this document as Summary of Controls (SoC). This document may include the controls related to the services or products offered by the organization. For marketing reasons, some corporations may wish to differentiate themselves from others certified organizations by showing clients what controls are in operation [Grammassl02].

In terms of the second issue, the SoA is a declaration that plays an important role in the certification process; since it is in this document that an organization commits itself to implementing a group of controls and it held accountable by the certification bodies for this commitment [Humphreys02b].

3.9.4 Analysis of available literature

Understandably, Statements of Applicability are not disclosed by certified organizations. This is, probably, because it would reveal what controls are in place and which are not.

In this context, the available literature deals more with the SoA role in an implementation than its actual format and writing procedures. Two expectations are Kadam [03] and Ferrant [04].

Kadam [03] suggests the addition of the risk and control reference to the other fields mentioned by BSI, as illustrated in Table 3.1. As an organization's control may address more than one BSI´s control, as well as several implemented controls may be mapped to a single control of BSI, it is important to provide the risks and control organizational references.

Controln umber	BSI number	BSI control objective	BSI control	Control implemented and reason for exclusion if any	Risk reference (from the organization)	Control reference (from the organization)
A.7 Physical and environmental security						
16	A.7.1	Secure areas	A.7.1.1 Physical security perimeter	Not applicable. Considered not relevant, due to other applied physical access controls.		
17			A.7.1.2 Physical entry controls	Applied	R6.2 Physical intrusion	C4.2 Locked door

Table 3.1: Example of a SoA according to Kadam [03]

This level of detail is not abided by Ferrant [04]. For the cited BSI´s trainer, it is sufficient to add a field of document reference of the risk assessment report that supports the need for that control.

3.10 PHASE 9: OBTAIN MANAGEMENT APPROVAL

3.10.1 Overview

The last phase of the security management system's implementation process demands the involvement of management.

3.10.2 Summary of BSI requirements

"Obtain management approval of the proposed residual risks and authorization to implement and operate the ISMS." [BSI02:p.6]

3.10.3 Interpretation of BSI requirements

The necessity of management approval can be felt at two levels: (1) approval of the outstanding risks and (2) initiation of the ISMS implementation.

The first question derives from the concept that controls are not 100% efficient, and in consequence, a fraction of the original risk will remain after the application of the risk mitigation safeguards [AS99]. BSI demands that management acknowledges these enduring risks not eliminated by security controls.

The second question is merely operational, since this process should result in an operating security management system (analysed further in 5.2).

3.10.4 Analysis of available literature

No literature was found regarding the investigated twofold questions.

3.11 CONCLUSIONS

This chapter intends to answer to an instrumental interrogation for the present dissertation's purpose: *What procedures are employed to identify, assess and mitigate risks affecting information security?*

In the last chapter, BSI was regarded as the risk methodology framework more appropriate to assess information resources.

Based on this first finding of the dissertation, this chapter examines the several phases of this method in order to establish (1) an interpretation of the standard's requisites and (2) an analytic account of the literature regarding the practical procedures employed to carry out those requirements.

The findings of this chapter are summarized in Table 3.2.

For each of the nine phases of the BSI´s risk methodology stages, this table (1) proposes an elucidation of its requirements and a number of deliverables as well as (2) reveals the procedures employed by the BSI framework implementations described in the available literature. The investigation has revealed the subsequent findings:

Phase 1: Define the ISMS scope
The first task in the methodology is to select the *evaluation area* (the organization area which will be subject to the security evaluation process). This area, following BSI requisites, should have *business relevance*.

Or in other terms, this part of the organization's structure should hold critical information and be engaged in the critical process for the overall organization. [42]

[42] For instance, a bank should not select as the scope of its ISMS the storage of the receipts of its catering section. The ISMS area should pertain to the conductance of business.

To select this area, two approaches can be followed: (1) *a process based approach*, or (2) *an information based procedure*. Both methods employ business relevance as the selection criteria of the evaluation area. Both methods attain the same outcome: a group of activities that deal with a certain type of information.

The difference between both relies merely on the starting line: the first approach starts by defining the critical organizational processes, while the second commences with the definition of the information relevant to the business.

The interpretation of the BSI requirement made by the author (and in part supported by other exegetes) founded 3 deliverables of this stage: (1) scope statement (written description the ISMS detailed *what information* and *what processes* are being evaluated and *how were those selected* – for this selection a process or an information based approach may be followed); (2) list of legal and business requisites and constraints relevant to the ISMS; (3) list of information resources (as documents or database) within the ISMS.

Phase 2: Define the ISMS policy

Subsequent to the definition of *what to protected*, protection goals should be determined. These objectives should be conveyed in a strategic document - Information Security Policy - and, if applicable, by more operational documents as procedures.

From the examined methodologies to define security policies and norms, the three-step process of Brykczynski [03] was considered appropriate.

Phase 3: Define a systematic approach to risk assessment

At this stage, it must be defined *how risk will be assessed.* Estimating a risk for BSI, means calculating its level of danger based on its (1) probability of happening and (2) value of the asset affected by it.

This calculation can be made by employing monetary values or non-monetary scales. The first approach employs formulas as Exposure Factor, Single Loss Exposure (SLE) and Annualised Loss Exposure (ALE) to estimate the financial cost of a risk. In the second approach, risks are ranked according to a qualitative scale, embodying several degrees of severity for the organization (*cf.* 3.4.4).

Phase 4: Identify the risk

As a risk is a product of the relationship between a threat and a vulnerability, both of its ingredients should be considered, in order to identify it.

A group of threat and vulnerability identification methods, compiled from literature concerning BSI implementation, were scrutinized, which unveiled the singularities of each.

Catalogues of threats and OCTAVE´s threat profiles ensure that a comprehensive range of threats are examined.

While the attack trees and the methods sanctioned by CORAS (as Fault Trees Analysis (FTA)) are more *casuistic*, exposing with great detail the relations of cause/effect of few selected threats.

Methods of vulnerability identification were categorised according to its objective by approaches aimed at technological vulnerabilities and procedures targeted to non-technological vulnerabilities.

Technological vulnerabilities are detected by comparing IT systems against a set of known vulnerabilities. Tools performing this operation can be classified according to their relationship to the scanned system as: (1) vulnerability scanners (active scanning), (2) network surveillance tools (passive scanning) and (3) software testing tools (source code exam).

Non-technological vulnerabilities are recognised through the perceived deviations of the actual actions of employees, organization's procedures or systems from an accepted practice guideline (which can be the defined security policy of the organization or a security catalogue). This comparison can be done through (1) an auditing process, known as *gap analysis*, which frequently evaluates the compliance of an organization against the controls of ISO. Another method is (2) intrusion tests, which discover weaknesses in systems and in actual worker's actions.

Phase 5: Assess the risk

As analysed, risks must be assessed through the estimation of its likelihood of occurrence and its business impact (which derives from the value of the resource affected by it).

The probability of a risk can be estimated based on a (1) single variable or (2) by a group of factors. In the first case, the likelihood of a risk occurring is regarded as a function of a single factor, either the asset's vulnerabilities or the threat agent. In the second case, the likelihood of a risk is derived from an equation that combines the asset's fragilities and the threat agent.

Phase 6: Identify and evaluate options for the treatment of risks

According to BSI, four treatment strategies can be applied to risks. A risk can be (1) accepted, (2) reduced through the application of safeguards (3) transferred to an insurer or outsourcer or (4) avoided (by preventing, for instance, the usage of the asset affected by that risk).

The *decision of what to do with the risk* may be supported on (1) only the gravity of the risk; (2) or only on the protection required by that affected resources; (3) or otherwise a combination of both (*cf.* 3.7.4).

Number	BSI phase	Major requirements	Required outputs	Examined procedures
1	Define the ISMS scope	a) Delimitation of the ISMS using a documented procedure. b) Identification of legal and business requirements c) Identification of the information assets within the ISMS	a) Scope statement b) List of legal and business requirements c) List of information assets	Scope selection procedures: a) Process based approach b) Information based approach
2	Define the ISMS policy	The document entitle of Information Security Policy should include: a) definition of objectives of information security; b) management statement in support; c) reference to other internal security regulations (e.g. procedures); d) identification of legal requirements; e) responsibilities for management; f) references to other documents.	a) Information security policy document b) Specific policies (if applicable) c) Standards, procedures, guidelines (if applicable).	Analysed phases of definition of security regulations: a) Definition of business objectives for security; b) Identification of applicable legal requirements; c) Definition of security policies and procedures
3	Define a systematic approach to risk assessment	A risk assessment method must be: a) systematic and; b) suitable to the ISMS and legal requirements.	Definition of the formula type of risk calculation	Type of formula of risk calculation: a) Monetary approaches b) Non-monetary approaches
4	Identify the risk	a) Identify the threats to assets; b) Identify the vulnerabilities that might be exploited by those threats; c) Identify the impacts that losses of CIA dimensions on assets.	List of risks	Threat identification: a) Threat catalogues b) Attack trees c) Threat profiles d) Threat modelling methods Vulnerability identification: a) Detection of only technological vulnerabilities b) Detection of general vulnerabilities
5	Assess the risk	To calculate the risk, it should be consider: a) Business impact of a security failure, taking into account the losses on CIA dimensions; b) Likelihood of it.	A calculated risk level (an estimation of the probability and impact of a risk)	Probability estimation procedures: a) Estimations supported by a single variable b) Estimations supported by a combination of variables
6	Identify and evaluate options for the treatment of risks	The risk may be: a) accept it; b) avoid it; c) transfer it to insurers or suppliers; d) reduce it.	Risk treatment decision (in terms of the 4 strategies)	Risk acceptance or treatment decision based on: a) risk attributes as impact and probability; b) protection need; c) combination of both.
7	Select control objectives and controls for the treatment of risk	The risk treatment plan should include: a) Mandatory measures from BSI´s chapters 4, 5, 6 and 7. b) Selective measures from Annex A that may be chosen or excluded. c) Measures derived from other sources, as long as they provide more assurance than the BSI`s controls.	Risk treatment plan (defines for each risk, its treatment strategy, and if this decision is to reduce, includes appropriate controls)	Type of selection of safeguards: a) risk analysis; b) security baseline.
8	Prepare a Statement of Applicability	Produce a Statement of Applicability (with the reasons for the choice of controls or its exclusion)	Statement of Applicability (SoA)	The available SoA templates in addition to the required, include also: a) risk and control reference; b) list of related documentation.
9	Obtain management approval	a) Approve residual risks b) Authorization to operate the ISMS	Residual risks approved ISMS operation authorization	Literature not found.

Table 3.2: Summary of BSI´s risk management method

Phase 7: Select control objectives and controls for the treatment of risk

After deciding the risk treatment strategy, security measures to *treat* the risk must be taken. These countermeasures should be referenced to the list of controls of ISO (copied in Annex A of BSI). [43] As each measure, intended to reduce, transfer or avoid the risk, has to correspond to, at least, one control of ISO, for matters of simplicity, it could be reasoned that the measures are *actually* selected from that catalogue. [44]

The measures to counter risks are decided on by the organization based on ISO and other sources (providing they ensure more stringent controls than ISO).

However, other measures – which are not directly related to risks - are not arbitrary. The measures required by BSI to establish and operate the Information Security Management System (ISMS) are mandatory. Those requisites involve management mechanisms, as auditing and regular reviews, which ensure that risks are continuously assessed and controls are effectively maintained.

Phase 8: Prepare a Statement of Applicability

For organizations to demonstrate compliance with the controls of ISO (these safeguards are reproduced in Annex A of the BSI text), they have to prepare a document confirming which of the catalogue's countermeasures have been applied. This document should state the reasons for the selection or exclusion of each of the safeguards of ISO (*cf.* 3.9).

Phase 9: Obtain management approval

The last stage of this methodology involves (1) the *go to live* authorization to operate the ISMS and (2) acknowledgement of the residual risks (the part of the risk remaining after the application of the control - *cf.* 3.10.3).

To sum up, this chapter examined alternative methods to carry out the nine phases of the BSI methodology to implement a management system for assessing risks and monitoring security controls. As this chapter examined methods to identify and estimate risks, the following one will examine possible security controls to mitigate risks.

[43] For example, to mitigate the risk of laptops being stolen from the organization's facilities, surveillance video cameras in the halls could be installed. This measure (surveillance video cameras) should then be referenced to ISO´s list (in this case, this safeguard may correspond to the control 7.1.3 Securing offices, rooms and facilities - *cf.* Annex B.12).

[44] Actual measures are not extracted from ISO. This catalogue, as studied in the next chapter, does not provide specific measures (e.g. install surveillance video cameras) but offers strategies (e.g. protecting working areas by proper mechanisms of surveillance).

4.

SYNOPSIS OF SECURITY CONTROLS CATALOGUES

Security models and formal methods do not establish security. Systems are hacked outside the models' assumptions.
Dorothy Denning [45]

4.1 INTRODUCTION

The last chapter discussed the various approaches to identify and estimate risks within the BSI risk management paradigm. In that chapter, it was noticed that, for BSI, all risks considered unacceptable by the organization have to be tackled by security controls (*cf.* 3.8.1). This requirement raises a question: *how to identity the appropriate security measure to diminish those risks*? [46]

Following BSI instructions, organizations have to select countermeasures - mainly (*cf.* 3.8.3) - from ISO/IEC 17799:2000 - *Code of Practice for Information Security Management* [ISO00a], a safeguard catalogue associated with BSI.

The utilization of ISO/IEC 17799:2000 as the reference guide of safeguards is supported on a number of assumptions. Organizations assume that ISO/IEC 17799:2000 (1) protects its most valuable assets, (2) provides guidelines to implement security controls and (3) has controls that address all relevant security threats.

Based on these assumptions, the current chapter examines ISO/IEC 17799:2000 [ISO00a], or simply ISO, and three other catalogues in order to validate the following hypotheses:

- (1) Does ISO aims to protect the same object of the other catalogues?
- (2) Does ISO has a detail level in its guidelines similar to other catalogues?
- (3) Does ISO has security controls similar to other catalogues?

The chapter is structured in the following sections. In section 4.2, the concept of security catalogues is expounded as well the four security frameworks covered in the investigation. Section 4.3 dissertates over the three hypothesis presented. Finally, in section 4.4 conclusions are articulated.

[45] Dorothy E. Denning. *The Limits of Formal Security Models*. National Computer Systems Security Award Acceptance Speech, October 18, 1999. Cited in Schechter [04].

[46] The text of this chapter was submitted and accepted as a poster in ICETE 2004 - International Conference on E-Business and Telecommunication Networks.

4.2 WHAT ARE SECURITY CATALOGUES?

4.2.1 Overview of security catalogues

As organizations tend to share more information with their partners, the need to evaluate the safety of the operation of the trusted partners has grown significantly [AEXIS02]. This necessity has led to the development of comparison schemes of security mechanisms among organizations.

In order to help organizations develop their security safeguards, established in a common and applicable list of control objectives, some authors and institutions started to systematise the concerns and practices of protecting IT systems. SAFE [Kraus72], AFIPS [79] and Wood [87] were famous early efforts.

Similarly, some standardisation institutions, such as the National Institute of Standards and Technology (NIST), the Information Security Forum (ISF), the British Standard Institution (BSI) and the International Organization for Standardization (ISO) began to publish control lists and promote adherence to them.

Table 4.1 shows a selection of security catalogues.

Security catalogues	Source	Observations
Baseline Security	European Telecommunications Standards Institution (ETSI)	Though designed to be the official security catalogue of the European Union, it has never received much acceptance. Mapping of controls with ISO/IEC 17799:2000 is available at [ISO00b]. Available at: http://www.etsi.org
CobiT - Control Objectives for Information and related Technology	ISACA	Analysed in this chapter. Available at: http://www.isaca.org/cobit .
GASSP – Generally Accepted System Security Principles	International Information Security Foundation (I2SF)	GASSP was intended to be a complete management framework with its general principles (Pervasive Principles), control objectives (Broad Functional Principles) and a third level with “how to" guidance (Detailed Principles). This last level has not yet been published. Available at: http://www.i2sf.org
OCTAVE - Operationally Critical Threat, Asset, and Vulnerability Evaluation	Software Engineering Institute (US)	This risk assessment methodology also includes a safeguard list [Alberts02]. Available at: http://www.cert.org/octave.htm .
The Standard for Information Security	Information Security Forum (ISF)	This control collection resulted from contributions of practitioners spread throughout the world. Available at: http://www.securityforum.org/.
ISO/IEC TR 13335 - Guidelines for the Management of IT Security (GMITS)	International Organization for Standardization (ISO)	Analysed in this chapter. Available at: http://www.iso.ch.
ISO/IEC 17799:2000 - Code of Practice for Information Security Management	International Organization for Standardization (ISO)	Analysed in this chapter. Available at: http://www.iso.ch.
IT Baseline Protection Manual	Bubdesamt fur Sicherheit in Informationstechunk - Germany	Addresses deeply technical matters (like cryptographic controls). The German Institute has plans to launch a certification program for organizations. A comparative study with ISO/IEC 17799:2000 is [GBSI01]. Available at: http://www.bsi.de.
NIST SP 800-12 - Computer Security Handbook	National Institute of Standards and Technology (NIST) - US	Analysed in this chapter. Available at: http://www.nscl.nist.gov/nistpubs .

NIST SP 800-53 Recommended Security Controls for Federal Information Systems	National Institute of Standards and Technology (NIST) - US	This standard was enacted by the Federal Information Security Management Act (FISMA) to guide safeguard selection in US government agencies. Proposes security measures predominantly in the same areas as NIST [95]. An innovation is the baseline approach. The document suggests 3 baselines levels: low, medium and high security. Each baseline has its own specific controls. Available at http://www.nscl.nist.gov/nistpubs.
Site Security Handbook (RFC 2196)	The Internet Engineering Task Force (IETF)	Covers issues such as policy content and training, system and network security and incident response procedures. The IEFT handbook conceives security as targeted to the protection of systems. Available at: http://www.ietf.org .
SSE-CMM -Systems Security Engineering Capability Maturity Model	International System Security Engineering Association (ISSEA)	SSE-CMM is an ISO standard (ISO/IEC 21827). Comparisons between ISO/IEC 17799:2000 and SSE-CMM are available from [Pattinson02] and [Hopkinson99]. Available at: http://www.sse-cmm.org.

Table 4.1: A selection of security control catalogues

Publishing bodies justify security catalogues as a selection of protection mechanisms that were developed and tested in several organizations [Solms01b], [ISO00a], [ISACA00]. As a result, they were considered applicable to other organization's protection [Campbell03].

As a consequence of this selection procedure, derived from previous security implementations in organizations, these recommendations are classified as *good practices* or *best practices* [Solms01b]. [47]

4.2.2 Four security catalogues

Security controls of ISO/IEC 17799:2000 will be compared to:

- ISO 13335-4 - *Guidelines for the Management of IT Security* (GMITS) [ISO00b]
- NIST *Computer Security Handbook* [NIST95]
- *Control Objectives for Information and related Technology* (COBIT) [ISACA00]

Further, the four catalogues will be briefly introduced as well as the reasons for their appearance in this dissertation.

a) ISO/IEC 17799:2000

The British Standard Institution nourish the concept of a security standard that would provide visibility to organizations that need for their information systems to be trustworthy by their clients and partners [Gammassl02].

[47] The main sources for these checklists are their own author' experiences and other security standards [Siponen03]. Several scholars [Baskerville93], [Dhillon01], [Siponen03] have criticised safeguard catalogues for being essentially supported by practical experiences and knowledge derived from information security cookbooks rather than based on empirical research and conceptual analysis.

Accordantly, a safeguard catalogue, British Standard 7799 - *A Code of Practice for Information Security Management*, was released in 1995 with a twofold purpose: (1) assisting organizations in the implementation of security and (2) developing a common language to express information security management [AEXIS02].

This document was republished as a national standard by Australia and New Zealand as AS/NZS 4444 in 1995, and Holland in 1997.

The Dutch version (entitled SPE20003) introduced the idea of a certification scheme. The conformity of an organization with the BS 7799 controls would be recognised by either an entry certification or an advanced level certification, which would be supported by internal and external auditing processes [Gammassl02].

In response to the need of having a certification mechanism capable of evaluating the compliance of an organization with the catalogue of practices, BS 7799-2 - *Specification for information security management systems* was published in 1998. This document describes the internal management mechanisms of an organization which are required for a security operation (*cf.* section 2.4.1.c)

The *Code of Practice* was reviewed in 1999 essentially to (1) remove UK specific references and (2) add new controls related with developments such as e-commerce, mobile computing and outsourcing [AEXIS02].

Finally, the International Organization for Standardization published the British document in 2000 as an international standard, ISO/IEC 17799:2000 [ISO00a].

Currently, ISO/IEC 17799:2000 or simply ISO, as used in this text, is the most important security catalogue in the world. This is demonstrated by: (1) the expansion of its certification program (as explained - *cf.* 2.4.1.c - certification is addressed by the BS 7799-2:2002) and (2) the acceptance of its controls as *good practices* by organizations.

b) GMITS

Guidelines for the Management of IT Security (GMITS) is a series of ISO standards covering risk management (*cf.* section 2.4.1) and security controls.

This chapter examines the fourth part of GMITS, ISO 13335-4 [ISO00b], which is a catalogue of safeguards. ISO 13335-1 [ISO96] is also reviewed, since this document filters through security management (discussed in section Annex B.3.3). GMITS was selected for analysis, as it at the moment the most comprehensive ISO framework of security management.

c) COBIT

The Control Objectives for Information and related Technology (COBIT) was designed by Information Systems Audit and Control Association (ISACA) as an audit tool for information management [Okabe03], [Hoekstra02].

COBIT structures IT activities in 34 processes which have the purpose of guaranteeing that the information delivered to a business is (1) secure, (2) has quality and (3) is reliable [ISACA00]. [48]

As it is understood, the scope of COBIT is IT management and not only security. Nevertheless, COBIT was included in this research for two reasons: (1) due to its acceptance, especially amongst the auditors' community [Okabe03] and (2) its approach towards the measurement of security. [49]

d) NIST Handbook

The National Institute of Standards and Technology (NIST), a US government institute, published *NIST Computer Security Handbook* [NIST95] to guide the development of security programs in US governmental bodies [Hopkinson99]. [50] Due, to the substantial influence that the NIST Handbook had in the US [NIST01], it was incorporate in this comparison of frameworks.

4.3 EXAMINATION OF THE FOUR CATALOGUES ACCORDING TO HYPOTHESIS

4.3.1 Does ISO aims to protect the same object of the other catalogues?

It is assumed by organizations that safeguard standards protect their utmost resources. For ISO, the most important asset in organizations is information. This position is accompanied by COBIT, which also consider its controls target to protect information.

However, GMITS and NIST have a different security object (the resource aimed to protect). For them, the object is IT systems. This distinction is based on the declared objective of each catalogue. In fact, as it is shown in 4.3.3, the similarities between the controls of the four catalogues are vast.

4.3.2 Does ISO has a detail level similar to other catalogues?

[48] According to COBIT, information delivered to the business processes has to fulfil three main requirements: (1) quality, which depends on the utilization of resources to produce information and is measurable through the effectiveness and efficiency criteria; (2) security, which is defined by CIA dimensions and (3) fiduciary requirements, which involve adherence to legal requirements and internal and external standards (compliance) and provisions of appropriate information for management (reliability) [ISACA00].

[49] COBIT proposes for each control a number of indicators to measure its efficiency. These indicators are included in a comprehensive auditing scheme.

[50] NIST, in the security realm, is well known for two series of documents. They are the Special Publication and the Federal Information Processing Standard. The Special Publication on security is designated as "SP 800" and includes more than 50 titles, such as SP 800-12 *Computer Security Handbook* [NIST95], SP 800-14 *Generally Accepted Security Principles & Practices* [NIST96]. Another renowned series is the Federal Information Processing Standard (FIPS), which consist of standards of validation of cryptographic modules, as FIPS 140-X Security Requirements for Cryptographic Modules.

Safeguard catalogues are supposed to provide guidelines to implement security in organizations.

ISO is organized in a way that a reader should: (1) understand what controls objectives are to be applied (control objectives) and the reasons why those are supposed to be applied, and (2) how it can be implemented (particular security controls). Furthermore, ISO groups the control objectives into categories or domains.

In consequence, ISO has the following structure, as illustrated in Figure 4.1:

a) group of security objectives (domains);
b) what security objectives are to be attained (control objectives);
c) how the objective can be achieved (security strategies, which are designated in this chapter, as control practices or as measures).

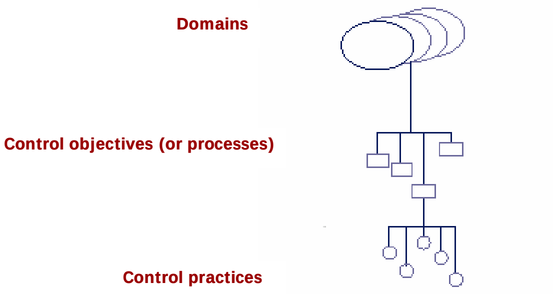


Figure 4.1: The overall structure of security catalogues (adapted from [ISACA00])

As a result, ISO is organised into 10 domains (general security areas) that group the 36 control objectives (high level objectives).

In the entire standard there are 127 specific strategies. In total, ISO is structured in 10 domains, 36 security goals and 127 security practices [ISO00a].

GMITS and COBIT abide by this three-part structure. The first one has two domains, 12 control objectives and 40 controls. COBIT is structured in 4 domains, which groups 34 critical processes of IT management, which are formed by 302 control practices. As seen, COBIT, as well as ISO, also organizes its paramount of strategies in processes.

By other hand, NIST is organized in 4 domains and 15 security objectives, and does not specify strategies. Hence, ISO, GMITS and COBIT detail paths to achieve security objectives. [51] These catalogues can establish, for example, that a security objective is protecting sensitive information and that a related feasible strategy is a policy of information classification. The cited standards (ISO, GMITS and COBIT) do not establish operational guidelines to implement security strategies. [52]

[51] NIST gives general recommendations, does not establish specific strategies.

[52] In this context, COBIT is the more detailed standard, as it provides tools - key performance indicators and key goal indicators -to measure the effectiveness of controls.

For example, a catalogue defines the need for information classification policy, but does not establish a classification scheme of information (as public and confidential). Therefore, these recommendations do not specify what tool or procedure should be implemented, leaving that for the organization. [53]

In sum, except for NIST, ISO follows the same structure of security objectives and strategies, as other catalogues.

4.3.3 Does ISO has security controls similar to other catalogues?

Control objectives sets are supposed to cover all security territory, and ensure that every important safeguard is included on the standard. To assess this assumption, a comparative appraisal of the catalogues was conducted, as documented in Annex B. As a result of this comparison, it was produced a chart of controls as illustrated in Table B.6 in Annex B.

This chart proves that ISO shares with the other standards a large group of controls. The catalogue more related to ISO is COBIT, which has 102 controls (63 %) in common with the considered 36 control objectives and 127 control of ISO. [54] The second catalogue more close to ISO is NIST with 71 shared controls (44 %), and in third place is GMITS with 66 controls (40 %).

A closer look to the safeguards of ISO and COBIT revels that most of measures of those standards are activities and not actual technological mechanisms [Aceituno04].

In sum, ISO covers all security concerns related to IT systems, represented by the controls of GMITS and NIST, as well as gathers the more management controls of COBIT. As COBIT addresses information management and not only security, it spans the scope of ISO´s controls.

4.4 CONCLUSIONS

Currently, a number of security measure catalogues compete for the preference of organizations. The reason for the profusion of these catalogues relies on their role as a security yardstick.

Catalogues establish security baseline - set of recommended security measures - which, in consequence, enable the comparison of security endeavours among organizations.

BSI forces organizations to select measures primarily from ISO, a safeguard catalogue.

[53] Those catalogues do not endorse the deployment of a certain type of technology, tool or operational procedure. For example ISO proposes the use of an authentication mechanism for nodes in terms of access control at a network level [ISO00a]. Nevertheless, it does not indicate the use of 802.1X for this purpose. 802.1X is a node authentication protocol from IEEE.

[54] The comparison considered 163 controls on ISO [ISO00a] (which, are in fact, 36 control objectives and 127 controls). This is because, in ISO, control objectives include a small text, which provides practical guidelines.

ISO, as well as other catalogues, is supposed to detail all relevant security measures necessary to protect the organization's most important resources. In other words, organizations expect catalogues to (1) be targeted to the protection of organization's resources (2) provides guidelines to implement security controls and (3) be comprehensive enough to address the security controls pertaining to that resources.

In order to scrutinize these three assumptions, it was investigated whether ISO and the three other catalogues - COBIT, NIST Handbook and GMITS - (1) were targeted to the protection of the same object (as for example, IT systems or information), (2) had the same detail level in its guidelines and (3) if covered the same security controls. This research concluded that:

- (1) ISO advocates a security object similar to COBIT and in antagonism with GIMTS and NIST. GMITS and NIST Handbook centre their concern on protecting IT systems, while ISO and COBIT focus themselves on the protection of information.
- (2) ISO has the same detail degree of GMITS and COBIT. Both of them share the same three-level structure of domains, control objectives and strategies (or control practices). In contrast, NIST does not define security strategies.
- (3) ISO addresses largely security concerns and recommends strategies similar to the other three catalogues (as examined in Annex B).

The last finding is supported on the next assertions:

- ISO, GMITS, NIST Handbook and COBIT ultimately cover the same security areas, addressing the: (1) managerial (involving aspects, such as security responsibilities), (2) operational (e.g. incident response procedure) and (3) technical dimension of security (e.g. node authentication mechanism).
- In particular, ISO shares with NIST Handbook and GMITS a group of IT technical measures, but the catalogue more closely related with ISO is COBIT.
- Although, security for COBIT, it is part of an IT management framework (and therefore its focus it is more management than only security), this catalogue share with ISO a large number of controls and has a similar concept of information security.
- Another similarity of ISO and COBIT is that they both organized their security measures according to processes. COBIT names its groups of measures as processes and ISO orders its strategies in a process manner.
- In comparison with COBIT, ISO lacks a measurement system to evaluate security efforts.

In conclusion, this chapter – whose text was submitted and accepted as a poster in ICETE 2004 - International Conference on E-Business and Telecommunication Networks - has provided the framework of the possible strategies to protect information in organizations. It has showed security objectives (the tenth domains of ISO) and strategies (its 127 security controls) to accomplish them. Based on these directives, an organization can develop its security strategy.

The following chapter discusses a methodology to assess risks and to select security strategies, from ISO, appropriate to small sized organizations.

5.

SECURITY MANAGEMENT IMPLEMENTATION METHODOLOGY

Security is a path, not a destination.
Dave Thompson [55]

5.1 INTRODUCTION

Up to this point, the present dissertation has examined methods to analyse risks and safeguard sets designed to mitigate the effects of risks in the organization.

Based on this research, the current chapter discusses and proposes a methodology appropriate for a small sized organization - as the one of the case study - to implement a group of managerial mechanisms intended to provide a continuous diagnosis of risks and ensuring that countermeasures to mitigate those are in place. Those mechanisms formed what has been labelled by BSI as a security management system.

The chapter introduces this concept (section in 5.2) and then presents the case study organization, ADETTI (in 5.3) and its security management constraints (5.4), which lead to the development of an implementation methodology, appropriate for small organizations, with similar conditions of ADETTI. This methodology is tackled from section 5.5 to 5.10. Conclusions are discussed in section 5.11.

5.2 INFORMATION SECURITY MANAGEMENT (ISMS) CONCEPT

Like ISO 9000 and ISO 14000, BS 7799-2 (referred as BSI) aims to develop a management system in organizations. [56] In the case of BSI, the management system aims to protect information resources in organizations, and is designated as an Information Security Management System (ISMS).

[55] Extracted from Microsoft [04].

[56] BSI (or BS 7799-2:2002) was developed by the same source as ISO 9001 and ISO 14001 that is the British Standard Institution.

An ISMS is defined by BSI as “that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security” [BSI02:p.4]. In this sense, an ISMS involves all activities and the supporting structures within the organization which are pertained to security management (SM). Figure 5.1 depicts the sequence of these several activities, differencing between the ones, which are mandatory (in order to obtain the BSI certification) and others which are optional.

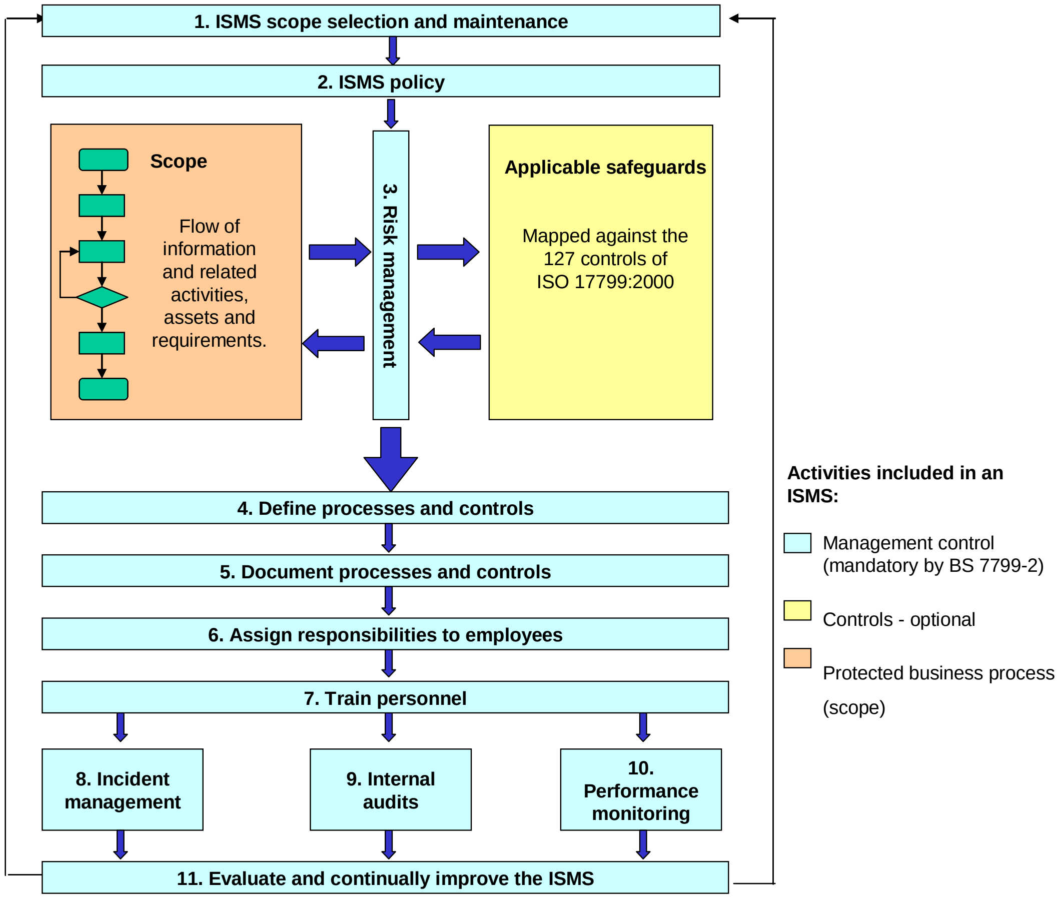

1. ISMS scope selection and maintenance
2. ISMS policy
Scope
Flow of information and related activities, assets and requirements.
3. Risk management
Applicable safeguards
Mapped against the 127 controls of ISO 17799:2000
4. Define processes and controls
5. Document processes and controls
6. Assign responsibilities to employees
7. Train personnel
8. Incident management
9. Internal audits
10. Performance monitoring
11. Evaluate and continually improve the ISMS
Activities included in an ISMS:
Management control (mandatory by BS 7799-2)
Controls - optional
Protected business process (scope)

Figure 5.1: Interpretation of the major activities of an ISMS

As seen in above figure, an ISMS is composed by three types of processes: (1) management control mechanisms, (2) safeguards taken from ISO 17799 and (3) the working processes included in the area selected as the application scope of SM in the organization.

The first type of activities - inherited from other similar management systems as ISO 9001 - are deemed as crucial enablers of a management system [BSI02] and therefore are *sine qua non* requisites to achieve the BSI certification. The activities prescribed in chapters 4, 5, 6 and 7 of the text of BSI are enfold in this category and be abridged in the 11 management controls processes illustrated in Figure 5.1 (in chapter 6, these 11 mandatory processes are detailed).

These mandatory activities are:

(1) identify a area in an organization for application of security management;
(2) define security objectives, as policies;
(3) identify and assess the risks endangering the selected scope and the defined objectives;
(4) establish procedures to support the security activities and controls norms: how to develop, monitor and revise a security norm;
(5) document the security efforts (to have records for certification purpose);
(6) organize the security responsibilities (e.g. develop a security forum);
(7) inform and train the personnel;
(8) report security incidents;
(9) perform internal audits;
(10) monitoring the performance of the ISMS;
(11) if necessary improve the ISMS through corrective and preventive action.

The second type of activities in an ISMS is formed by the controls to mitigate risks. These risk safeguards are decided by the organization, based on the list of 127 possible security strategies of ISO (*cf.* 3.8.3).

By last, the flow of the actual activities and information (the operational process), which is required to protect in the organization should also be translated into a process language.

5.3 BAKGROUND CONTEXT OF THE CASE STUDY ORGANIZATION

The case study was performed in the Associação para o Desenvolvimento das Telecomunicações e Técnicas de Informátic (ADETTI), an Information and Communication Technology (ICT) research institution associated with Instituto Superior das Ciências do Trabalho e da Empresa (ISCTE), a public University in Lisbon.

ADETTI is a non-for-profit research institution which is structured in six research units: (1) Multimedia and Virtual Environments, (2) Networking and Information Security, (3) Technologies for Business Processes, (4) Intelligent and Integrated Communication Systems, (5) Management and Strategy and (6) “We, the Body and the Mind”. [57] Administrative activities as financial control and document management are performed by a specialized unit, formed by a manager and two assistants, called Administrative Unit.

The research and development activities of ADETTI are funded by Portuguese and European Commission R&D programmes.

[57] The first research area, Multimedia and Virtual Environments, focuses on 3D computer graphics and virtual reality. Networking and Information Security area addresses computer network and security, especially secure access to multimedia information. Technologies for Business Processes studies advanced information technologies infrastructures that attain the requirements modern management methodologies. The fourth area, Intelligent and Integrated Communication, is focused on the development of new Artificial Intelligent techniques. Management and Strategy tackles industrial economics, ecology and strategic management. The “We, the Body and the Mind” area researches methods for human-computer interaction.

5.4 CONSTRAINTS OF THE PROJECT

Prior to the project inception, it was identified in ADETTI the following issues regarding the general conductance of the case study (*cf*. Annex C, chapter 2):

a) most internal resource, particularly project leaders and full-time researchers, had enormous time constraints;
b) there are was no formal security management in ADETTI and;
c) IT support activities and IT security activities are not clearly established.

As an outcome of these questions, it was defined the following objectives that an ISMS implementation methodology in ADETTI had to attain:

(1) minimize the time consummation of ADETTI personnel in the implementation process;
(2) ensuring that only the required safeguards are implemented.

To accomplish the first goal, the proposed methodology will try to moderate the time involvement of personnel.

As for the second objective, the methodology will try to ensure a "lean" security management system, formed only by the mandatory activities demanded by BSI requirements and by the risk mitigation measures, deemed as absolutely necessary. This approach attempts to avoid the overextension of controls, beyond a limit which could impair the normal working activities of ADETTI.

Based on these aforementioned constraints, on the interpretation of the processes included in an ISMS (presented in Figure 5.1) and on literature review of chapter 3, a suitable methodology was developed in ADETTI.

5.5 STAGE 1: PROJECT MANAGEMENT DEFINITON

5.5.1 Overview

Objective	Establish the management model of the implementation project and its major phases
Deliverable	Project management structure/ implementation decision structure

Inputs		**Practices and techniques**	**Outputs**
T01.1	• Manager representative with capacity to approve the project decisions • Participation of future members of security management (SM) structures • After ISMS scope selection, representatives from the selected areas may be included	• Definition of the project management model (role and participants in the project management) • Briefing of project members regarding the methodology which will be followed	• Project management model: - steering committee (with upper management and user representatives); - implementation manager (project manager). • Project team trained (team may be changed after scope selection)

5.5.2 Rationale for the proposed procedures

The central deliverable of this phase is the project's decision structure. Throughout the implementation of an ISMS, an organization will have to take decisions about implementing safeguards mechanisms, which could interfere or even modify working activities. Therefore, prior to the project inception, it must be defined how these decisions will be taken [Carlson01], [Plate02].

In literature it was found recommendations that those decisions should be nested by senior management endorsement - as advocated by BSI and ISO - and by the contributions of operational managers (or even user representatives) from the areas which will be included in the ISMS scope [Mendes04] or probable future members of SM structures [Seaver03].

5.6 STAGE 2: EVALUATION AREA DEFINITION

5.6.1 Overview

Objective	Define the boundaries of the ISMS scope in an organization
Deliverable	ISMS scope

Inputs		**Practices and techniques**	**Outputs**
T02.1	• Business objectives towards Security Management (SM) • Project constraints (time, resource and budget)	• Define criteria for the selection of the evaluation arena within the organization	• Decision criteria for scope selection
T02.2	• Decision criteria for scope selection (from T02.1) • Perception of information types and associated activities within the organization	• Process description • Process flowchart diagram • Information flow diagram • Organizational chart • Physical and network diagram	• Evaluation sphere definition
T02.3	• Evaluation sphere within the organization (from T02.2)	• Context diagram • Interfaces and dependencies list	• Interfaces and dependencies of the ISMS with other parts of the organization and other entities (as supplies and partners)

5.6.2 Rationale for the proposed procedures

The present phase, which is inspired by the first step in the BSI´s risk methodology (*cf.* 3.2) [58] establishes the area of the organization, which will be subjected to the assessment process.

The task T02.1 was originated from the case study in ADETTI and not from the literature review.

[58] Due to the complexity of the first stage of BSI risk methodology, in this proposed methodology it was only address the first outcome of BSI´s phase (scope selection), the other - identification of information assets and definition of legal and business requirements - are discussed in stage 4 and 3 of this methodology.

In spite of the recommendation - summarized in 3.2.4 - for the scope to be selected based only its business relevance, the application of the methodology in ADETTI forced the recognition that project constraints (time and resource availability) and, above all, the overall business objectives should be attained in the scope definition - as justified in Annex D 2.2.

Being BSI steered to the information protection and adopting a process viewpoint (*cf.* 3.2.3 a), it is understandable that the scope should firstly be defined in terms of information and its related activities organized in a process format [BSI03a]. Subsequently, the scope should be depicted in other dimensions (*cf.* 3.2.3 a) and justified in terms of business relevance, employing for the purpose of these tasks the techniques described in T02.2.

Ideally, the evaluation area would be an isolated area with controlled interfaces. However, as the scope is not an *island* in an organization; and furthermore, a vulnerability of a resource, outside the evaluation sphere, may be inherited by a critical asset in the scope - transitivity of vulnerabilities [Jeffcott02] - it is advisable, as shown in T02.3, to isolate the dependencies and interfaces of the ISMS with its outside environment (*cf.* Annex C, 2.2), employing context diagram [AEXIS04], [BSI03a].

5.7 STAGE 3: DEFINE BUSINESS AND LEGAL REQUIREMENTS

5.7.1 Overview

Objective	Define the objectives and external requirements for security management (SM)
Deliverable	Business and legal requirements

Inputs		**Practices and techniques**	**Output(s)**
T03.1	• Existing business requirements	• Review of documents with strategic requirements • Interviews with management • SWOT analysis • Definition of business requirements	• Index of business concerns for SM
T03.2	• Legal literature • Existing contracts	• Identify contractual and legal requirements	• Index of legal requirements for SM

5.7.2 Rationale for the proposed procedures

At this stage is established the business objectives and legal constraints which will be applied throughout the implementation process.

The placement of a phase of strategic clarification before the asset identification and the risk diagnosis was deemed as fruitful in order to accommodate the future evaluation of assets and risks into the business and legal requirement’s soil, and consequently achieve an alignment of the security process with the business objectives. This preposition is shared by Purser [04], Carlson and [02] Sêmola [03].

As discussed by Purser [04], security efforts can only be useful for the organization, if developed in relation with the overall organization requisites.

The idea of an index of requirements was drawn from Seaver [03] and Purser [04].

The present requisites will assume the input role in subsequent phases.

5.8 STAGE 4: DEVELOP AN ASSET REGISTER

5.8.1 Overview

Objective	Develop an inventory of assets
Deliverable	Asset inventory

Inputs		**Practices and techniques**	**Outputs**
T04.1	• Existing inventories in the organization • Types of records for the asset register (taken from ISO) • Asset taxonomy (taken from ISO) • Business and legal requirements (taken from T03.1)	• Records categories of the register • Taxonomy of assets • Asset evaluation formula • Asset identification criteria	• Asset inventory structure (T04.1) • Asset inventory completed (T04.2)

5.8.2 Rationale for the proposed procedures

The cornerstone of asset management is the resource registry. This concept is drawn from ISO realm “Asset Classification and Control” (*cf.* B.4) and phase 1 of BSI method (*cf.* 3.2.3.c). [59] Two challenges are posed to organizations at this stage:

a) How to identify assets?

An asset is a resource valuable for the protection of the information and processes defined as the evaluation scope (T02.2). Therefore, each identified asset must be inventoried and then subject to risk analysis [BSI02]. From this BSI requisite derives the consequence that the more or less granular is the criteria to identify assets, the more or less assets will be submitted to risk assessment. In other words, the level of detail employed to recognize assets determines the overall detail level of risk assessment.

It was found three criteria to identify assets [Mendes04]: (1) consider each particular resource in the scope as an asset. Another possibility is to regard (2) each resource’s component as a separate asset. A third hypothesis is to consider not individual assets but (3) asset categories. [60]

[59] BSI methodology only alludes to the identification of information resources (*cf.* 3.2.3.c), but ISO spans the need of register to other assets (following a taxonomy in Annex B, section 4.2).

[60] To illustrate these distinctions, a case of an ISMS based on e-mail process may be employed. Under the first perspective, assets would be resources related to the SMTP process, such as the router or mail relay

As input for asset identification, existing inventories may be employed (as their data may be useful). The inventory may follow the ISO recommendations in terms of asset taxonomy (catalogue the asset with categories as software or physical asset, for instance) and type of records, such as asset name and asset description, as discussed in Annex B.4.6.2.

b) How to valuate resources?

The asset value (i.e. the resource's business relevance - *cf.* Annex B.4.2) may be estimated using a monetary or non-monetary approach. In the first case, monetary cost of assets are employed (see SLE in Annex A.3.2.1), in the latter, scales of numbers or attributes are used to differentiate more critical assets from others (*cf.* Annex A.3.2.2).

In either approaches, it is advisable to employs the *asset owner* [61] to define the business relevance of the asset, as advocated by Insight [04].

For the definition of the asset's business relevance it should be considered the negative consequences that a breach in the confidentiality, integrity and availability of the data and/or service provided by resource, would produce in the working process and associate critical information of the ISMS scope [Insight04].

Since the value of assets tends to depreciate with time, the evaluation should have - at least - an annual frequency [AEXIS04].

5.9 STAGE 5: CONDUCT RISK MANAGEMENT

5.9.1 Overview

Objective	Assess the level of risks and compare them against what management regards as business acceptable
Deliverable	Risk treatment plan

Inputs		**Practices and techniques**	**Output(s)**
T05.1	• Asset evaluation scale (from T04.2)	• Type of formula monetary or non-monetary • Type of probability estimation	• Risk calculation formula
T05.2	• Risk calculation formula (from T05.1)	• Identify vulnerabilities • Identify threats • Estimate risks	• List of risks
T05.3	• List of identified risks	• Define the risk acceptance criteria	• Risk acceptance criteria

server. This approach ensures a closer outlook to reality, as further in the risk assessment process, the risk that affect the asset will be identified based on its characteristics (its particular position, etc.) [Mendes04]. According to the second approach, each system would be segregated in its components. The SMTP server would be divided, e.g., in hardware, and software, each of them considered as individual assets [Mendes04]. The third tactic is the less arduous, since it uses categories of assets, as desktop, servers, etc. This approach assumes that, all assets gathered in that category have a similar risk level [Kadam03]. In addition, it is suitable for organizations that desire to implement a common security level within an asset category.

[61] The *asset owner* is the employee who was nominated responsible for the asset.

T05.4	- List of identified risks - Risk acceptance criteria	- Identify the treatment strategy - Identify the applicable controls from ISO	- Risk Treatment Plan

5.9.2 Rationale for the proposed procedures

This stage comprises of the major steps of the risk methodology, examined in chapter 3. The above proposed four steps (T05.1-4) condensed BSI´s phases 3 to 7.

At this phase, risks affecting the inventoried resources (*cf*. 5.8) are identified and its probability and impact estimated in order to calculate a specific level of danger for each risk (*cf*. 3.4.2). In order to define the risk formula, it must be decided (1) type of formula (2) type of probability estimation.

In relation to the risk type formula, a number of equations are possible to compute the probability and impact value - the issues required by BSI - and asset value (*cf*. A.3.2.2). As for the probability estimation of risks, the organization may opt for an estimation supported by a single variable or by an estimation supported by a combination of variables (*cf*. 3.6.4).

In a concise outline, this stage involves:

a) Identify threats

This identification of threats can start with brainstorming sessions following instructions of (1) threat catalogues, (2) OCTAVE´s areas of concern or (3) HazOp. All these methods enable that a comprehensive range of threats be discussed, which is useful to ensure a vast coverage of possible threats. These sessions are conducted by the implementation advisor and involve members of the steering committee.

In order to reveal the relationships between threat sources, vulnerabilities and impacts, methods such as Attack trees, Event Trees Analysis (ETA), Fault Trees Analysis (FTA) and Failure Mode, Effect and Criticality Analysis (FMECA) are useful (*cf.* A.4.2.).

b) Identify vulnerabilities

The detection of vulnerabilities can be performed with auditing frameworks, as gap analysis supported on ISO (*cf.* A.5.2.2) and automated scanning tools (*cf.* A.5.2.1).

c) Estimate risks

A risk, in this context, can be regarded as a combination of a threat(s) and a vulnerability(ies), which is characterized by a particular probability and impact. As risks are constantly evolving, it is recommendable to record the reasons for the assessment of the probability and impact of each risk.

d) Risk acceptance criteria

According to BSI, it must be defined the criteria which will be employed to accept or subject the risk to a treatment option.

The criteria could be defined in relation to a number of factors, as discussed in 3.7.4.

e) Risk Treatment Plan

The last outcome of the present stage is a document - Risk Treatment Plan - which classifies the risk as acceptable or insupportable, applying the above criteria. If the risk is above the risk acceptance criteria, then it is established the suitable treatment strategy for the risk: mitigation, avoidance or transference. For the risks which have to be mitigated, it is identified the applicable control(s) of ISO (*cf.* 3.8.2).

5.10 STAGE 6: DEFINE SECURITY PROCESSES AND CONTROLS

5.10.1 Overview

Objective	Define security processes and controls
Deliverable	Documents supporting the security norms and controls

Inputs		**Practices and techniques**	**Output(s)**
T06.1	• BSI requirements of an ISMS • Existing security management practices (from T05.2) • Risk Treatment Plan (from T05.4)	• Definition of security norms and controls	• Information security policy • Organization of security management • Supporting process of security norms • Asset management • Scope management • Risk management • Human resource management • Physical and environmental management • Communications and operations management • Access control management • System development and maintenance mgment. • Business continuity management • Compliance and continual improvement mgment.

5.10.2 Rationale for the proposed procedures

In the previous phase, it was identified the practices and controls required to mitigate risks. In the present stage the security practices will be defined as security norms and the actual controls to be implemented will be decided. Consequently, the deliverables of this stage will be an assortment of documented security processes and controls.

The last stage of the methodology addresses the activities related to life cycle of the security practices and controls. In fact, it is at this phase, that security processes (as a new user registration procedure) and controls (e.g. authentication with smart token) are defined and it is planned its implementation, maintenance, evaluation and, if required, future improvements.

The first step to formalise a security process or control is to define the list of processes, derived from BSI requirements, and the list of risk controls identified in the risk treatment plan.

The next step is to analyse the existing situation, in particular the existing constraints and practices [Purser04].

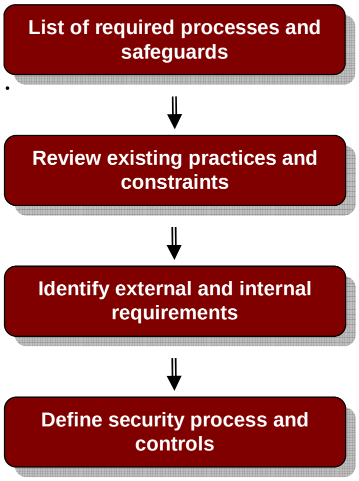

List of required processes and safeguards
Review existing practices and constraints
Identify external and internal requirements
Define security process and controls

Figure 5.2: Process and control definition

For example, before defining a backup procedure, it is necessary to analyse how backups are done and why they are done in that way (it could be that the backup software only supports a particular type of backups, e.g. full backups) [Guel01]. The current examination should focus on identifying patterns of repeatability [Scholtz04].

The third stage establishes "where the organization would like to go". External requirements are laws and contracts with practical consequences in the norm composition (for instance a backup procedure for electronic invoices must comply with the Portuguese law for storing this sort of data - Decreto-lei nº 256/2003 from 21th October).

Internal requisites are can described as the "amount of effort that the organization is willing to done to reduce the risk" [Guel01]. Based on business requirements, more control activities or security technology can be added to the operational activities.

The forth step is the process and control definition. This stage is a consequence of the previous steps: depending on the business requirements and constraints a process may be defined at a low or high level of detail. In the former case, it only lists the operations (e.g. backups should be done everyday) and the latter details them (e.g. full backups should be daily to a separate backup media by the system administrator).

This flexibility is also applied to technological matters: to mitigate a risk of robbery, it can be selected controls as different, and with cost implication so diverse, as installing a video camera or installing a new sophisticated lock.

5.11 CONCLUSIONS

This chapter presented a *course of actions* to deploy an Information Security Management System (ISMS) in organizations with small dimensions. The proposed path was drawn from the conjunction of the interpretation of BSI requirements, literature review and the specific project constraints in ADETTI.

According to the requisites defined by BSI, an Information Security Management System (ISMS) can be interpreted as group of managing activities. As these activities are described in a process manner and some of these processes are mandatory for an organization to achieve the BSI certification, it can be summarised that an ISMS is formed by 11 mandatory macro-processes and a group of optional processes, selected from a list of 127 possible controls in order to protect a specific operational process(es) within an organization.

In other words, an ISMS is composed by three layers of processes. In the first tier are management control activities, deemed as fundamental for any management system. The second tier is formed by the operational activity(ies) of an organization placed under the scope. An ISMS is usually, not targeted to the protection of an entire organization, but to a specific process related to particular information type.

The last tier is composed by the safeguards selected through risk assessment to protect the assets of the scope. These controls, are decided based on the BSI`s Annex A. Since most of these countermeasures prescribed more activities than actual technological mechanism (*cf.* 4.3.3), for simplicity reasons the ISO 17799 controls are described as activities.

The ADETTI´s constraints - (1) time and personnel availability and (2) low level of security practices formalization - induced the development of a methodology suitable to:

a) expend only the minimum employee’s time during the implementation process.
b) decide only the implementation of the safeguards, required by BSI or because of justifiable business requirements.

In order to alleviate the time consumption, similar activities – in particular requirements definition – were grouped together. In relation to the second issue, to facilitate the alignment of the method’s deliverables with mandatory requirements of BSI, as Figure 5.3 shows that the project’s phases, except for the first one, can be mapped against the requirements of BSI, as discussed in Chapter 3, and ISO´s safeguards, analysed in Annex B.

Proposed methodology Stage	**BSI method phase [discussed in Chapter 3]**	**ISO domain [discussed in Annex B]**	**Outcome**
1. Project management definition			Project management structure/ implementation decision structure
2. Evaluation area definition	1. Define the ISMS scope (*cf.* 3.2.3)		ISMS scope
3. Define business and legal requirements			Index of business and legal requirements
4. Develop an asset register		5. Asset Classification and Control (*cf.* Annex B.4)	Asset inventory
5. Conduct risk management	3. Define a systematic approach to risk assessment 4. Identify the risk 5. Assess the risk 6. Identify and evaluate options for the treatment of risks (from 3.4 to 3.7) 7. Select control objectives and controls for the treatment of risk (*cf.* 3.8)		Risk treatment plan
6. Define security processes and controls	2. Define an ISMS policy (*cf.* 3.3) 8. Prepare a Statement of Applicability (*cf.* 3.9.2)	All other ISO domains	Documents supporting security management processes and controls (e.g. polices, procedures)

Figure 5.3: Proposed ISMS implementation methodology

Moreover, to clarify the business alignment of the decided measures, the methodology was organized according to a process approach, placing the collection of inputs first (see stages 2 and 3), and then enabling the traceability of these requirements to the decisions made in stages 4 and 5, as detailed next:

Stage 1: Project management definition

An implementation project of a security management system involves decisions that will affect not only the management system itself, but also interfere with the working activities included in its scope. Due to this reason, the decision model of the project must be clearly defined.

Stage 2: Evaluation area definition

In this stage, the area of the organization, which will be subjected to evaluation, is defined. The selected area should have business relevance, but also be adequate to the projects constraints (time, resources and budget). Regardless of its characteristics, the selected area should include the activities related to a particular type of information: how that information is introduced in the scope, processed, accessed, stored and destroyed.

Stage 3: Define business and legal requirements

The definition of the business objectives and legal constraints was placed before the diagnostics of the security situation in order to enable that in the following assessments (asset value and risk calculation) the business and legal requirements are properly considered.

Stage 4: Develop an asset register

According to BSI, the assets of the evaluation area must be inventoried. The formulation of this register pose two issues: (1) level of detail in asset identification - the more assets, the more granular security assessment - and (2) the type of formula to calculate the asset value.

Stage 5: Conduct risk management

This stage involves the identification, assessment and treatment of risks affecting assets. Initially, threats and vulnerabilities are identified separately. Then all possible combinations between these two factors, which may represent any danger for an asset, are identified. The outcome is a risk, which is subsequently characterised by a particular probability and impact. Finally, based on these two features, the risk is evaluated as acceptable or as requiring treatment: mitigation, transference or avoidance.

Stage 6: Define security processes and controls

As a result of the risk management, it is decided the implementation of a group of controls and practices. This stage involves the necessary steps to define and plan those security norms and safeguards.

The practices and the several template documents which support this methodology are detailed in Annex C, the implementation report.

In conclusion, this chapter has proposed a SM implementation methodology, in order to answer to the primary research question:

How management of information security can be implemented in small sized organizations?

The next chapter reports the application of this methodology in ADETTI. This case study will allow the verification of the applicability of the proposed methodology.

6.

CASE STUDY IN ADETTI

"In theory, there is no difference between theory and practice. But, in practice, there is."
Jan Van de Snepscheut [62]

6.1 INTRODUCTION

The previous chapter proposed a series of structured procedures to implement an Information Security Management System (ISMS) in an organization, with heavy time and resource constraints and the requirement of a strong business alignment of security management. This chapter outlines the findings of the application of this methodology in the Associação para o Desenvolvimento das Telecomunicações e Técnicas de Informática (ADETTI). [63]

The implementation of a management system requires the production of a vast documentation, which will be used as records for the certification [Clements96]. In this context, the section 6.2 merely presents a synopsis of the case study results, focusing particular attention in the interpretation of the project's findings. Those findings are then employed in section 6.3 to ascertain the overall results of the case study.

A comprehensive report of the application of the methodology in ADETTI is offered in the Implementation Report in Annex D.

6.2 METHODOLOGY APPLICATION IN ADETTI

6.2.1 Stage 1: Project management definition

The project was supervised by a steering committee, which was formed by ADETTI´s president, the author as project manager and the administrative unit manager, as detailed in Annex C, section 2.1. Throughout the work of this committee it was found:

a) The support of the president of ADETTI was instrumental to guarantee the cooperation of ADETTI´s personnel.

[62] Citied without bibliographic reference in Zuccato [02].
[63] The meaning in English of the acronym ADETTI is Association for the Development of Telecommunications and Information Technology.

b) The participation of the administrative unit manager (as the representative of the organizational area under evaluation) was focused on the adequacy of the adopted security practices in relation to the normal working activities, ensuring that the new controls did not impair the normal working activities.

Due to the exposed findings, we may infer that:

a) It is relevant and justifiable the integration of a stage of project management on the implementation process, as proposed by the present methodology.

b) The project team should integrate possible participants in the future security management structure of the organization. As a running ISMS requires the appointment of a number of security responsibilities to a group of personnel, it is recommended to involve, from an early stage, the possible participants in the security management structure. This preposition is advocated by experts of ISO 9001 management systems [Clements96], [Pires2004], [Seaver03].

6.2.2 Stage 2: Evaluation area definition

On the contrary of the last stage, in this phase it was necessary to make some adjustments on the proposed procedures in 5.6.2. Originally, it was considered that area of the organization, which the security management system would be applied, could be selected based only on its business relevance, as discussed in 3.2.4.

However, the application of the methodology in ADETTI showed that project constraints (time and resource availability) play also a critical role in the evaluation scope selection. In fact, the area for the security evaluation was primarily selected based on the project's constrains and only collaterally on the business importance of it.

Firstly, ADETTI´s management decided to adopt a narrow scope in order to lessen the time consumption from the workers. Then, right at the beginning of the process, it was perceived that was impossible to submit to the evaluation process the production areas (the research units), due to time constraints of the researchers. Consequently, it was decided to restrict the project to the Administrative Unit (AU), in which it was found a problem with the financial reporting process.

Therefore, the financial reporting process was selected for security evaluation. This process involves all task related to the preparation, delivery and storage of the financial data of final report of the research projects (*cf.* Annex C., section 2.3.2).

In an organization with the characteristics of ADETTI, establishing the frontiers of the evaluation area presents some challenges: the Administrative Unit does not occupy a separate room neither has its own IT infrastructure and most of its resources are also used by personnel outside the ISMS (*cf.* Annex C., section 2.3.5).

In the scope definition process the following was worth of notice:

a) In scope selection, an ad-hoc approach can be more feasible than a structured method based only on business relevance concerns. This was the case of ADETTI whose evaluation area was selected, based more on the project constraints than in the business relevance of the chosen area.

b) In the discussion within the steering committee it was found a trend off between by one side, the requirement of BSI for a scope with business relevance and by another side the difficulties of impacting on the critical working activities. In ADETTI it was recognised that was not possible to interfere with the research activities and consequently the evaluation area had to be confined to a supporting process (financial process).

c) Managing the interfaces of the ISMS with other areas in the organization places some difficulties. The activities under the scope can only be performed if the input is provided in predicable conditions: if the delivery of input varies greatly it is impossible to ensure a standard process. This question in ADETTI´s scope poses in terms of the handout of invoices and financial statements by the project leader (*cf*. Annex C., section 2.3.1). This action performed by someone outside the scope, initiates the financial process. Therefore is fundamental to establish and monitor a “service level agreement” of the scope with project leaders.

Those findings steered to the prepositions that the selection of the evaluation scope:

a) must be applied to an area or process that (1) suits the organization goals for the certification process and (2) fulfils the BSI requirement of business relevance;

b) it is advisable to select areas with *relatively* stable activities. An ideally scope would be focus on a particular type of process with clear boundaries, stable resources and defined interfaces with other entities: preferably, entities to whom it is possible to define and, in case of necessity, exercise service level agreements.

6.2.3 Stage 3: Define legal and business requirements

From the definition of a group of business, legal and contractual requirements, as detailed in Annex C, chapter 3, it can be stated that:

a) The majority of these requirements can be related with security management: 3 out of 5 business requirements had direct or indirect implication in security management (SM); all ninth legal requirements demand specific actions to ensure compliance and 7 out of the 14 contractual requirements were related to SM.

b) In spite of being time consuming, the association of a reference to the requirements (e.g. “L(number)” for legal requisites) help to easily identify these requisites for the evaluation of assets, in the subsequent step of this methodology.

6.2.4 Stage 4: Develop an asset register

The development of the asset inventory tackled two issues: the criteria to identify assets and the asset value formula.

With regard to the asset identification question, it was recognised the need to define exactly what constitutes an asset. An example is the asset ServerBSCW which was deemed to include the hardware, operating system and applications that supports the BSCW database. The actual data of the BSCW database was regarded as another asset (*cf*. Annex C., section 4.3). In this context, an asset is simply a logical item worth of being individually evaluated.

Concerning asset evaluation it was employed four criteria, as detailed in Annex C, section 4.2: (1) confidentiality, (2) integrity, (3) availability and (4) business relevance.

The application of the asset evaluation in ADETTI – as reported in Annex C, chapter 4 - unveiled that:

a) In the majority of cases, the business relevance replicates the same value assigned to the confidentiality, integrity, availability of the resource. This may suggested an alignment of the CIA factors with the overall business perspective. However, in 34% of the assets, the divergence of values between the business relevance and the other criteria indicates the importance of using this business classification. In fact, in those cases, the CIA evaluation of assets did not translate the perceived business value of the resource. This fact suggests that the business relevance of an asset does not derive only from the value of the confidentiality, integrity and availability of the data and or function that the resource has or performs. [64] Moreover, the integration of business relevance in the asset evaluation is justifiable by the business alignment objective of the present methodology.

b) The types of assets regarded as more important are the human resources (two out of three were classified with the highest mark), then appear the information assets (of seven assets, four are deemed as critical) services (three of them are very important: courier, IT service and SMTP service) and finally in the physical asset categories only the BSCW server was rated as critical.

These findings lead to the present analysis:

a) The calculation of the asset value should combine the properties of information security (CIA dimensions) and business relevance.

b) As an asset, under this context, is a logical classification, it is necessary to describe it, in particular its components. An asset designated as “file server” can correspond only to the hardware or to an IT system and its stored data.

[64] For example, the Ricoh Aficio 1515 (asset PA011) was classified as relevant (4) for the business process, although its confidentiality availability and integrity is medium (3) due to holding temporarily not sensitive data, and, in case of problems, others printers could be used. The reason for this discrepancy was that the financial cost of a possible printer repair. This case shows that the business relevance, moreover to information security properties it is concerned with the actual financial value of the asset.

6.2.5 Stage 5: Conduct risk management

Risk management was performed in 4 steps: initially it was (1) defined the risk calculation formula, subsequently (2) this formula was applied to assess the identified risks. Based on the resulting value, it was (3) distinguished risks that could be deemed as acceptable and those which were not. Finally, (4) all of these risks were evaluated in terms of the most suitable risk treatment strategy that could be applied to him.

With respect to the first phase - formulation of the risk assessment equation – the Steering Committee decided to add a business variable (the asset value) to dimensions employed to gauge risk: probability and impact (as detailed in 5.2 of Annex C). This decision was inspired by the methodological goal to enable a business alignment of all security decisions.

In the second phase – risk identification – it was adopted the concept of BSI that a risk is a combination of a threat and a vulnerability. In consequence, threats and vulnerabilities were identified sequentially and then it was defined possible combinations of both factors, deemed as applicable to ADETTI by the Steering Committee.

Initially, it was identified applicable threats for the scope from the threat catalogue of Gillingham [03]. From this operation, seven threat agents as discontent student or discontent administrative unit employee were defined, as detailed in Annex C, section 5.3.1 and shown in Figure 6.1

.

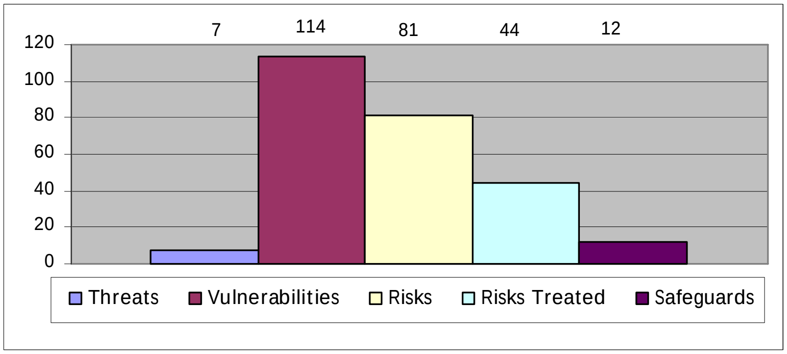


Figure 6.1: Figures from the risk management process

Concerning vulnerabilities, it was applied the preposition that any divergence of the practices and control mechanisms of ADETTI in regard to the safeguards of ISO, would represent a vulnerability. The application of this procedure guided to the recognition of a large number of possible vulnerabilities: 114, which means that 70% of the 125 controls of ISO that could be applicable in ADETTI were not actually applied, as detailed in 5.3.2 in Annex C and illustrated in Figure 6.1.

After the threats and vulnerabilities identification, for each threat it was decided the most suitable vulnerability from the list of vulnerabilities identified during the previous stages. During this process, some of the previously identified vulnerabilities were renamed: for instance, instead of using the ISO designation, it was employ names as “lack of procedures” or “inadequate procedure”.

As an outcome of the process, from the 35 assets inventoried in the previous stage, 81 risks were identified (see Figure 6.1). These risks were regarded by the employees and manager of the Administrative Unit as the most important risks affecting that particular group of assets.

For each identified combination of a threat and a vulnerability, it was assessed the probability and possible impact of such risk occurring, employing a scale of 1 to 5 (being 5 the highest value). The resulting values of probability and impact were multiplied by the asset value in order to obtain a score for each risk. This score classified risks in a scale of 1 to 125.

At this point, BSI requires that the organization decides the criteria to separate acceptable risks from others which have to be treated. To define the risk acceptance criteria, it was reviewed a series of risks and the Steering Committee decided which situations could and which could not be accepted. Based on these assessments, it was verified, that most risks regarded as non acceptable had a higher score than 32. As a result, 44 risks were deemed as unacceptable (see Figure 6.1).

To treat these risks, it was select 12 countermeasures from ISO based on the (1) estimated reduction in the risk score due to the application of the control, (2) cost and (3) time required to apply the control, as detailed in 5.5.2 in Annex C.

In total the selected countermeasures enable an estimated reduction of 17% in the sum of the risk scores of the risks deemed as not acceptable. In fact, the sum of those risks, before the application of mitigation measures, was 1243 and due to those safeguards this total decrease to 1031.

Throughout the risk management stage it was noticed:

a) The risks, classified as more harmful, are those which endanger the purpose of the security management system: protecting the financial data employed in the final financial report of research projects. This is attested by the highest risk which is information inaccurate processing of project accountability (risk score of 100). The risks with the lower scores are related to assets with low asset values, for example, risks causing the failure of the air conditioning, PBX, switch Cisco, or fax.

b) In the assessment of risks, impact was found easier to assess than probability. This opinion of the employees involved in the risk assessment is corroborated by the fact that no risk was scored with 5 (which meant that the risk was regarded as “almost certain”) while in comparison several risks were classified with the maximum impact.

c) The most applied strategy to treat the unacceptable risks in ADETTI was the mitigation approach. The preference by risk reduction measures in comparison with risk transference measures (e.g. take insurance to cover a specific risk) or risk avoidance (for instance, prevent the use of the asset affected by that risk) can be regarded as due to the financial flexibility offered by the mitigation option.

In fact, while the risk transference and risk avoidance most certainly implies some sort of financial investment, the risk reduction encompass measures, as establishing procedures, which do not imply substantial financial costs.

This predilection of the steering committee for controls related with activities is depicted by its majority in the total of measures: from the 12 selected measures, only 4 are protection mechanism which do not define security activities (in the form of procedures).

6.2.6 Stage 6: Define security processes and controls

An ISMS requires the standardisation of security activities and controls, which entails that existing practices in a organization be agreed, documented and controlled [Seaver03]. The definition of the mentioned security processes and controls will be conducted in the present phase, employing for this purpose, the interpretation of three layers of processes in an ISMS (made in section 5.2):

a) Operational process

In ADETTI, the financial reporting activities were formalized in a process, thus forming the operational process of the security management system. The existence of a description of the operational activities under the scope is a consequence of the BSI requirement of BSI "ISMS scope" (see Table 6.1).

b) Mandatory security processes

BSI requires that some activities related to management control be performed in any security management system (*cf.* 5.2). The 11 mandatory requirements of an ISMS, as described in 5.1 of the present text, are addressed in 9 developed security processes in ADETTI, as detailed in Table 6.1.

BSI mandatory requirements	**Developed procedures** (with the identification of the ISMS documentation)	
1. ISMS scope	2.1	Financial Reporting (operational process)
	2.3	Scope Management
2. ISMS policy	2.2	Security Management Planning and Review
3. Risk management	2.5	Risk Management
4. Procedures to support security norms	2.4	ISMS Documentation Control
5. Document control	2.4	ISMS Documentation Control
6. Human resource management	2.6	Human Resource Management
7. Organization of security management	2.2	Security Management Planning and Review
8. Security incidents management	2.7	Incident Report Management
9. Internal audits	2.9	ISMS Audits
10. Performance monitoring	2.2	Security Management Planning and Review
11. Corrective and preventive action	2.10	Corrective and Preventive Actions

Table 6.1: Mandatory requirements of BSI and processes developed in ADETTI

c) Selective security processes and controls

In the risk management stage 12 safeguards, selected from ISO, were regarded as necessary in order to mitigate the ADETTI´s risks. Those safeguards resulted in 4 new procedures, an amendment in an existing one and 4 new controls, as showed in Table 6.2:

BSI selective requirements [with the BSI identification]	**Applicable**	**Procedures and controls** (with the identification of the ISMS documentation)
A.5.2 Information classification	Yes	2.8 Document Classification Procedure
A.7 Physical and environmental manag.	Yes	Physical caveats integrated in "Recommended Security Practices", a supporting document of "2.6 Human Resource Manag. Procedure"
		Control: Install a surveillance camera at the office lobby
A.8 Communications and operations manag.	Yes	2.12 IT Operations Procedure
		Control: update malicious code software
A.9 Access control management	Yes	2.11 Access Control Procedure
		Control: Deploy an SMTP server for ADETTI
		Control: Reinforce firewall policies to isolate from ISCTE network
A.10 System development and maintenance manag.	No	No selected safeguard related within this domain.
A.11 Business continuity management	Yes	2.13 Business Continuity Framework Procedure

Table 6.2: Selective requirements of BSI and corresponding output

All of the mentioned processes engage in interactions between each other, as illustrated in Figure 6.2.

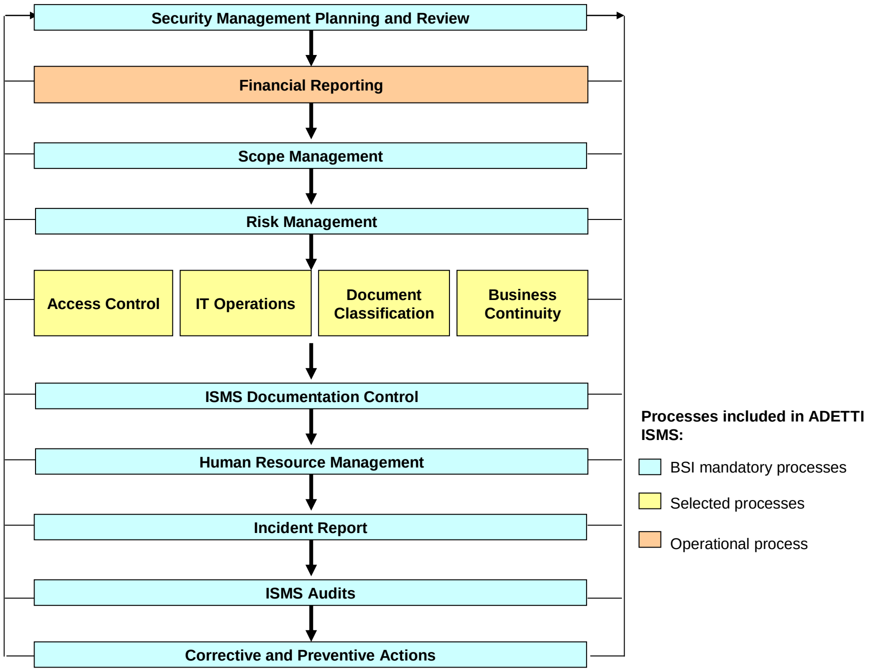


Figure 6.2: Security processes in ADETTI´s ISMS

As observed, the first process - SM Planning and Review - plays the role of two BSI requites: ISMS policy and performance monitor. By one hand, this process defines security objectives in the form of policies and by another, receives regular feedback from all other processes in order to monitor the ISMS performance (*cf.* Annex C, 6.2.14).

The modification of the ISMS policies, due, for instance, to a new business requirement, may imply a change in the operational process. Any change in the financial reporting may demand the scope documentation update (tackled by the scope management process). If this change entails new risks, they have to be assessed and registered in the Risk Treatment Plan.

If this new risk requires an adjustment of the current four procedures – in yellow in Figure 6.2 - then the related documentation must be altered (addressed by ISMS documentation control) and the employees informed (human resource management). Any incident reported or found in an audit must be investigated and corrected (corrective and preventive action).

Concisely, from the development of processes and controls arise the following findings:

a) An ISMS requires the formalization of numerous security activities: moreover to some ad-hoc practices (as e-mail usage rules, defined in terms of general security recommendations), 13 sequences of activities had to be established. From this total, 9 processes were needed to attain BSI mandatory requirements, while 4 processes were developed to mitigate the risks, as showed in the Figure 6.2.

b) Due to the few structured security activities found in ADETTI (*cf*. 6.2.5), the security norms were developed in order to:

- (1) Allow a high level of variability in the activities conductance. To enable some flexibility in the application of security regulations, making them the more immune possible to obsolesce, caused by the changes in ADETT:

    - the policies define only the general principles of security management;
    - the procedures presents only the sequence of activities and their participants, without describing, in detail, how actions are performed.

- (2) Ease the burden of document maintenance. In order to lessen the document updating, contents with different probability of being updated were placed in separate documents. For instance, the asset list of the scope is published in a separate document to avoid unnecessary changes in the scope statement.

c) The developed procedures adhere to the PDAC framework, as they prescribed, regardless of the procedure's subject, activities for (1) collecting requirements that the process must attain, and then activities for (2) planning, (3) executing, (4) controlling and (5) revaluating the results of the execution. The main activities of these processes must be auditable, in the light of BSI requirements. Consequently it was produced 23 supporting documents to enable the record of activities for auditing purpose.

d) The only security process which was put in operation during the case study was SMP05 - Risk Management. This process encompasses the activities performed during the implementation methodology: identify and assess assets based on business and legal requirements and then identify, evaluate and treat risks. This process was reviewed 3 times during the conductance of risks assessments, due to the necessity to make adjustments to ADETTI reality. Therefore, it is probable that the other security process will require amendments, when the conductance of these procedures is monitored.

6.3 RESULTS OF THE IMPLEMENTION PROJECT

To assess the results of the methodology application in ADETTI, the two objectives defined for this methodology (*cf.* 5.11) will be compared to the case study results.

a) Minimum time consumption of resources in the implementation process

The ADETTI employees have heavy time constraints, therefore the implementation methodology to alleviate their time expenditure tried to:

- optimise tasks: similar activities were grouped together – an example is the concentration of the business requirements definition in stage 3 of this method;
- employing methods with less time consumption: an illustration is the adoption of risk identification methods, as threat list and gap analysis, which are simpler than others examined (*cf.* Annex C 5.3.1).

Nevertheless, this case study required - broadly - 11 days from ADETTI personnel in a total of 56 project days, as showed in section 7.1 of Annex C.

In the mentioned period of time, the largest time slice was from the employees of the organization area under the scope (7 days), manager with decision authority (2 days) and, in third place, the support areas, a day for IT support and another for Human Resource.

This time distribution suggests that an implementation project demands a heavy involvement from the employees under the scope (to collect requirements, design processes, etc.) and with a less extend from the other areas of the organization.

b) Minimum implemented safeguards

An organization, which intends to have its security management certified by BS 7799-2 must comply with 11 mandatory requirements (*cf.* 6.2.6) and demonstrated to a certification body (as APCER) that has selected from the 127 security strategies of ISO, the controls necessary to reduce the risks of the evaluation area to a level of risk, deemed by the organization as adequate to its business and risk requirements.

To ensure that only the safeguards required by BSI or by business requirements were implemented, the present methodology (1) has its sequence of stages abiding by the order of BSI requisites and (2) has a strong alignment with the organization's objectives and constrains. This business alignment is validated by:

- the area of the organization, which will be subjected to security management is selected primarily based on organization goals and constraints;
- involve personnel from the areas under the scope in the project team, to ensure the adequacy of the future security practices to the working activities;
- the asset value and the risk scores are derived from business directives (as well was other factors);
- the definition of security processes and related documentation tried to ease the maintenance tasks.

Despite the mentioned efforts, the project lead to an ISMS, formed by a complex web of new security activities, risk countermeasures, management responsibilities and documents, as depicted in Figure 6.3:

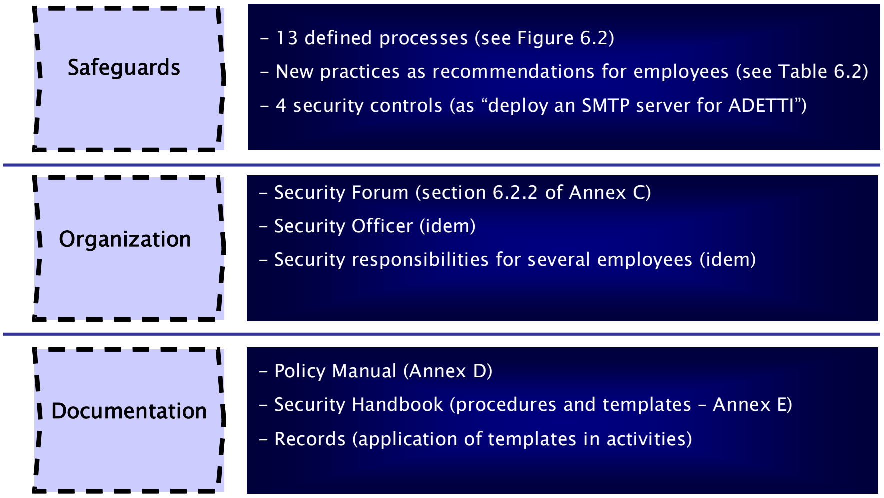

Safeguards
- 13 defined processes (see Figure 6.2)
- New practices as recommendations for employees (see Table 6.2)
- 4 security controls (as "deploy an SMTP server for ADETTI")
Organization
- Security Forum (section 6.2.2 of Annex C)
- Security Officer (idem)
- Security responsibilities for several employees (idem)
Documentation
- Policy Manual (Annex D)
- Security Handbook (procedures and templates - Annex E)
- Records (application of templates in activities)

Figure 6.3: Major outcomes of the implementation methodology

As an outcome of the definition of procedures, a number of activities were changed or introduced in ADETTI. The actual impact on ADETTI of these activities could not be determined at this project. Nevertheless, it was recognised that these activities would imply different frequencies:

- **Event driven security activities**: as some activities are impelled by specific events, the rate of occurrence of these activities will be determined by those events. For instance, every new access granted to employees, according to the access control procedure, will involve a formal authorization. Therefore, the frequency of this new security activity (access authorization) will be determined by the action of providing new access.

- **Regular security activities**: Every security process, even if not carry out (e.g. during that period of time it was not granted any access), must be reviewed regularly due to:

    - The performance monitoring requirement of BSI (*cf*. Table 6.1), which demands that evidences of the performance of each process are collected regularly to monitor them. In ADETTI, the owner of each process must provide evidences of the performance of the process every six months, the maximum period of time recommend by Humphreys [02a].

    - Procedure text review: In ADETTI it was adopted the maximum review period allowed by BSI which is one year. Therefore, each year, must exist records of a review of the procedure text.

All these activities demand a new position (security officer), a new management forum (security forum) and new responsibilities, as well as maintaining an enormous documentation (as detailed in Annex C, section 6.2.2).

6.4 SUMMARY OF FINDINGS

An implementation of a security management system posse hundreds of decision points, regarding practical issues. Nevertheless, we have tried to present, in this chapter, a summary of the most important questions, addressed in the ADETTI case study and which are pertained to answer to the primary research question:

How information security management can be implemented in small sized organizations?

To solve this challenge, it was design and applied a security management implementation methodology in ADETTI. This methodology aimed to be of (1) “fast” application – minimise the time expenditure of resources - and (2) produce a “lean” security management system, with only the minimum safeguards. To attain these two objectives, it was found in the ADETTI case study the following findings:

a) The project team should involve: (1) upper management, (2) participation of employees from the area, selected as scope for security management and (3) integrate possible future security management actors.

b) The scope should be an organizational area that (1) suits the organization requirements, (2) fulfils the BSI requisite of business relevance and (3) has stable activities and resources.

c) The assets of the scope must be inventoried with a clear description of its components and its value should reflect the information security properties (CIA dimensions) and business relevance.

d) In the assessment and treatment of risks, it was found that it is (1) easier to assess impact than probability and (2) the risk mitigation measures allow more flexibility and less financial investment than the risk transference and avoidance options.

e) An ISMS requires the formalization of numerous activities, which must be carry out within the scope. For instance, in ADETTI, it was defined 9 mandatory security processes (required by BSI requirements) and 4 selective security processes (decided to mitigate risks).

f) As policies and procedures try to crystallise evolving activities, it is necessary to make regular adjustments in the documentation that support security regulations. To alleviate this work, it is possible to define policies and procedures that combine the compliance with BSI requirements with a determined level of flexibility, allowing in consequence some variability in the performance of activities.

In sum, this chapter has summarised the case study project in ADETTI. Next, in the concluding chapter, a summary will be given of the subjects covered and the lessons learnt from this research project.

7.

CONCLUSIONS

7.1 DISSERTATION OBJECTIVES AND STRUCTURE

The primary research objective of this dissertation is to discuss and propose an implementation blueprint of security management in small sized organizations.

To attain this goal, the literature review and the subsequent research was designed to answer three questions:

- (1) Which risk management methodology is more suitable to handle risks affecting information security in organizations?

- (2) What procedures are employed to identify and assess risks affecting information security?

- (3) What catalogue of countermeasures is more appropriate to protect information security?

The first question has lead to the adoption of BS 7799 (or BSI) as the information security risk paradigm in this dissertation, as seen in chapter two. The second question has allowed the compilation and a taxonomy of risk assessment techniques used in organizations, as seen in chapter three. In order to respond to the last question, a comparison was made in chapter four between several security measures catalogues, originated from academia and industry, and ISO 17799, the catalogue of countermeasures endorsed by BSI.

The proposed methodology to assess risks concerning information security and establish security control mechanisms in organizations was discussed in chapter five. This methodology was applied to ADETTI in chapter six and the conclusions summarised in chapter seven.

7.2 ASSUMPTIONS ADOPTED IN THE PROJECT

The current dissertation is founded on a number of assumptions. The most relevant are examined next.

This research discusses a managerial approach to the protection of information. Information security is conceptualised as the safeguard of the CIA dimensions of information.

Other dimensions may be considered pertinent, as privacy for example. In the ADETTI case study, privacy of personal data was regarded as a legal requirement and not positioned at the same level as CIA. However the growing importance of this topic to public opinion can justify the placement of privacy as one of criteria to assess risks and one of the objectives for the protection of information.

The dissertation adopted the BSI framework as its reference of security management. This selection can be questioned. As observed, BSI does not provide a clear step-by-step methodology of implementing a security management system. In consequence, organizations aiming to implement a security management system are left to decide which procedures are more appropriate to achieve BSI requirements.

Furthermore, contrarily to COBIT, BSI´s list of desired security controls - ISO 17799 - lacks the measurement indicators to gauge the impact of its security measures on an organization.

By other hand, the controls of ISO 17799 were selected based on the experience of a group of experts (*cf.* 4.2.1). Therefore, it cannot be scientifically reasoned that this particular list is better than any other produced by the same method.

Nevertheless, this dissertation adopted BSI, due to its current relevance as the most implemented security certification for organizations in the world: at the moment of writing (August 2004), 890 organizations in 41 countries are certified by BS 7799-2 [XISEC04]. Furthermore, the future publication of ISO and BSI as ISO 27000 series standard should contribute to this trend [Gammassl02].

7.3 A CONCEPTUAL VIEW OF THE DISSERTATION

The research field of the present dissertation is security management (SM). This dissertation started off by showing the necessity of SM, and then discussed how existing risk management methodologies and security catalogues could be applied in a BS 7799 security management framework.

Based on the assumption that a possible mean to develop trust between organizations is for them to adopt security certifications it was presented a taxonomy of security certifications (*cf.* 1.2). This security certifications classification suggested that a particular type of certifications – the security management – can be deemed as path to develop more trust between organizations, because these certifications have a wider scope than system security certifications or e-commerce platforms security certifications.

The mentioned security management certifications imply the adoption by an organization of a (1) risk management process and a (2) set of security controls to enable comparisons of security efforts among organizations.

In order to capture the particular traits of the BSI certification regarding the two pillars of security management (SM), it was performed a comparative analysis of this framework against other risk management methodologies (in chapter 2) and other safeguard catalogues (in chapter 4).

The research about risk management concluded that BSI conceptualises this process as a continuous activity aimed to protect information. This viewpoint differentiates BSI from other risk management standards, as GMITS, OCTAVE and CORAS (*cf.* 2.5).

The approach of perceiving security management as an ongoing activity was considered more appropriate to an environment of sifting risks (*cf.* 2.4.1). As risks change at a rapid pace, organizations are forced to continuously assess their existing risks and adjust their security measures.

The comparison of BSI´s safeguard catalogue entitled as ISO 17799 with other security "best practices" lists, as COBIT, GMITS and NIST Handbook, unveiled that ISO 17799 and COBIT and with a less extent the other catalogues, ultimately (1) are targeted to the protection of the same object (information in organizations), (2) have the same detail level in its guidelines and (3) covered the same security controls (*cf.* 4.4).

All of these catalogues propose possible security strategies (for instance, classify documents according to its confidentiality), leaving to the organization the selection of the technological tools or group of activities suitable to accomplish them.

The insights gained through the examination of the two referred security management pillars were applied in the design of a methodology aimed to accommodate the BSI requirements with the time and resource constraints of a small sized organization (*cf.* 5.11). Due to the mentioned constraints of the case study organization - ADETTI, an ICT research institution - the methodology tried to attain two objectives:

- Minimum time consumption in the implementation process.
- Decide to implement only the safeguards strictly required by BSI or by justifiable business reasons.

To ensure these objectives, the methodology adopted methods (e.g. risk identification methods) which demand less time consumption and its sequence of stages was organized to enable a traceability of all decisions to its BSI and business requirements.

According to these requirements, an organization to have its security management certified by BS 7799-2 must demonstrate to a certification body, as APCER:

- compliance with the 11 mandatory requirements of BSI (*cf.* 6.2.6) and;
- that has selected from the 127 security strategies of ISO 17799, the controls necessary to reduce the identified risks to a level of risk, deemed by the organization as adequate to ensure the confidentiality, integrity and availability of an particular type of information within the evaluation area (*cf.* 3.11).

As an outcome of these concerns, the methodology, as illustrated in Figure 7.1, defines, in an early stage, the legal and business requirements, which are then tackled in the asset value, and afterwards the asset estimation is employed to calculate the risk score. Subsequently, the security activities (processes) and controls (non activity related measures, as technological tools), demanded by BSI or selected to mitigate the risks are established tacking into account the existing security practices and constraints (*cf.* 6.4).

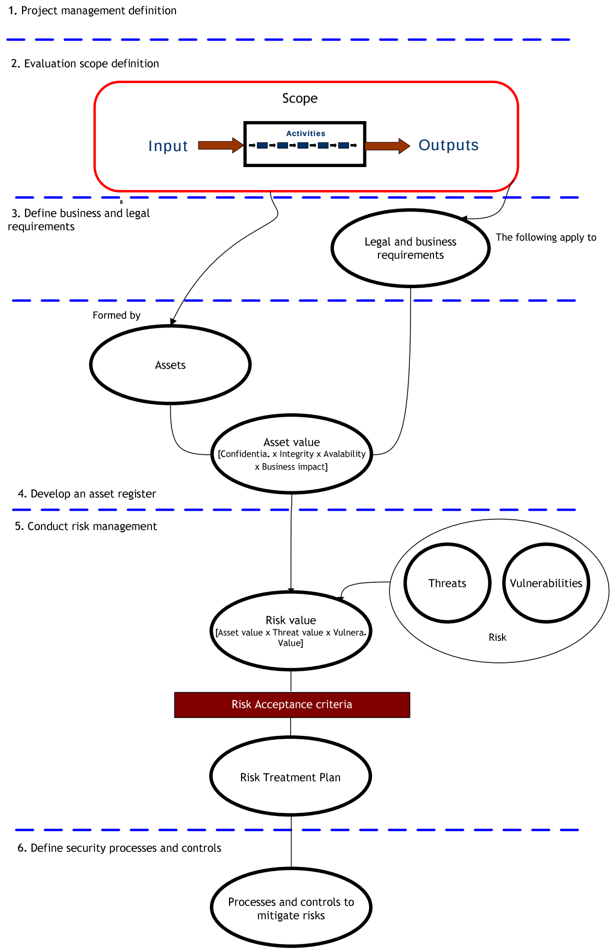

1. Project management definition
2. Evaluation scope definition
Scope
Input
Activities
Outputs
3. Define business and legal requirements
Legal and business requirements
The following apply to
Formed by
Assets
Asset value
[Confidentia. x Integrity x Avalability x Business impact]
4. Develop an asset register
5. Conduct risk management
Threats
Vulnerabilities
Risk
Risk value
[Asset value x Threat value x Vulnera. Value]
Risk Acceptance criteria
Risk Treatment Plan
6. Define security processes and controls
Processes and controls to mitigate risks

Figure 7.1: Overview of the proposed ISMS implementation methodology

The application of this methodology in ADETTI enabled some inferences, which are exposed next.

7.4 CONCLUSIONS REACHED

The case study in ADETTI leaded to the following conclusions:

a) Implementing a security management system requires a significant effort from the organization

Even with an implementation methodology designed to (1) consume the minimal time of resources and (2) ensure that only the minimum safeguards are implemented, during the implementation process, it is necessary:

- A heavy involvement from the employees under the scope - 9 days in ADETTI - and with a less extend from the other areas of the organization.
- A lengthy effort from the implementation team. In ADETTI just to design the security management system and implement a process (risk management) it was required 53 working days, in continuous effort.

b) A security management system implies a substantial adaptation of a organization

Although, the present project could not be determined the actual impact on ADETTI of a security management system - because only one process, risk management, was implemented and monitored - it was recognised that this type of system would require:

- Activities - Only to attain the BSI mandatory requirements, 9 processes are needed, while 4 processes were developed to mitigate the risks found in ADETTI.
- Organization - All these activities demand a new position (security officer), time consumption of ADETTI managers (who participate in the security forum) and employees (to perform the new security responsibilities).

In sum, a security management system may enable an estimated substantial reduction in the total of risk of an organization (almost 20% in ADETTI), but with a significant cost in terms of implementation project and incorporation of new activities and responsibilities as well as investments in security controls.

7.5 CONTRIBUTIONS OF THE DISSERTATION

This dissertation discusses a possible roadmap for the foundation of security management, according to the BSI paradigm, in small sized organizations.

The present project encompasses of:

- A security management implementation methodology, formed in each of its sequential phases, by alternative methods to attain the organization’s objectives and constraints.
- The deliverables required by BSI for certification purposes: policies, procedures and templates.
- The critical success factors - i.e. elements that are vital for a strategy to be successful [Wikipedia04a] - of an implementation project.

7.6 FUTURE DIRECTIONS

Few research of security management (SM) in organizations was found. Therefore, many investigation opportunities are still unfilled:

- applications of risk methods of other disciplines to SM (as CORAS has demonstrated this is a resourceful source - *cf.* 2.4.1);
- an comparative study of the effects of SM (focusing, for instance, in corporations with certified ISMS´s in different subsidiaries, as Vodafone);
- an meta-catalogue of safeguards, enabling the comparison of a countermeasure of a catalogue, with the related safeguards of other catalogues;
- an measurement scheme to enable a more objective performance monitoring of an security management system.

The foregoing suggestions represent a few possible areas for future research, especially in view of the fact that the research on SM still need to be refined in many ways, before it reaches the same development level as other research fields within the management and IT domains.

REFERENCES

[Aagedal02] Aagedal, J.; Braber, F.; Dimitrakos, T.; Gran, B.; Raptis, D.; Stolen, K. Model-based Risk Assessment to Improve Enterprise Security. Proceedings of the Sixth International Enterprise Distributed Object Computing Conference (EDOC'02). IEEE Computer Science. IEEE, 2002. Retrieved March 2004 from http://www.nr.no/coras

[AEXIS02] AEXIS, History of ISO 17799. 2002 Retrieved March 2002 from http://www.aexis.de/17799EPage.htm

[AEXIS04] AEXIS and XiSEC, RA2 – The Art of Risk. Help Files of software. Retrieved August 2004 from http://www.bsi-global.com/ICT/RA2/RA2_art_of_risk_%20Demo.zip

[Aceituno04] Aceituno, V. ISM3 1.0. - Information Security Management Maturity Model. Barcelona, Spain: ISECOM, 2004. Retrieved August 2004 from http://www.isecom.org/projects/ism3.shtml

[AFIPS79] AFIPS. Security: Checklist for Computer Center Self-audits. US: AFIPS, 1979

[Alberts01] Alberts, C. & Dorofee, A. Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Criteria. Pittsburgh, US: Software Engineering Institute, 2001. Retrieved January 2003 from: http://www.sei.cmu.edu/publications/documents/01.reports/01tr016/01tr016abstract.html

[Alberts02] Alberts, C. & Dorofee, A. Managing Information Security Risks: The OCTAVE Approach. Upper Saddle River, US: Addison Wesley, 2002

[Albuquerque02] Albuquerque, R. & Ribeiro, B. Segurança no Desenvolvimento de Software, Como Desenvolver Sistemas Seguros e Avaliar a Segurança de Aplicações Desenvolvidas com Base na ISO 15.408. Rio de Janeiro, Brazil: Editora Campus Ltd., 2002

[Anderson 01] Anderson, R. Security Engineering: A Guide to Building Dependable Distributed Systems. New York, US: John Wiley & Sons, Inc., 2001.

[APCER03] Associação Portuguesa de Certificação. APCER e os Sistemas de Informação in Dossier Especial *Qualidade e Certificação*, (Newspaper) Jornal Expresso, published at 25 October 2003. Retrieved December 2003 from http://www.apcer.pt/modules.php?name=Sections&sop=viewarticle&artid=21

[AS99] Australian Standard Institute and New Zealand Standard Institute. AS/NZS 4360: Risk Management. Australia: Australian Standard Institute, 1999. Retrieved August 2003 from http://www.standards.com.au.

[Atthirawong02] Atthirawong, W. & MacCarthy, B. An Application of the Analytical Hierarchy Process to International Location Decision-Making, Nottingham, UK: University of Nottingham, 2002

[Baudrillard04] Baudrillard, J. In the Shadow of the Millennium. Or the Suspense of the Year 2000. Retrieved August 2004 from http://www.simulation.dk/content.php?article.16

[Barman02] Barman, S. Writing Information Security Policies, Indianapolis, Indiana, US: New Riders Publishing, 2002

[Baskerville93] Baskerville, R. Information Systems Security Design Methods: Implications for Information Systems Development. ACM Computing Surveys no. 25, pp. 375-414 New York, US: ACM, 1993.

[Bernstein96] Bernstein, P. Against the Gods: The Remarkable Story of Risk. New York, US: John Wiley & Sons, Inc., 1996.

[Bjorck01] Bjorck, F. Security Scandinavian Style Interpreting the Practice of Managing Information Security in Organizations. Stockholm, Sweden: Stockholm University/Royal Institute of Technology, 2001. Retrieved June 2003 from http://www.bjorck.com.

[Brainthwaite02] Brainthwaite, T. Securing E-business Systems - A Guide for Managers and Executives. New York, US: John Wiley & Sons, Inc., 2002.

[Brassard96] Brassard, M. & Ritter, D. General Electrical Capital Services Memory Jogger II – A Pocket Guide of Tolls of Quality. First Edition. Methuen, MA, US: GOAL/QPC, 1996

[Brykczynski03] Brykczynski, B. & Small, B. Using ISO 17799, Code of Practice for Information Security Management to Best Advantage. Slide Show presentation at RSA 2003 Conference at April 14. Software Productivity Consortium, 2003 Retrieved January 2004 from http://www.xisec.com

[Brewer04] Brewer, D. & List, W. Measuring the Effectiveness of an Internal Control System. p. 3. Paper retrieved August 2004 from http://www.gammassl.co.uk

[Borkin03] Borkin, S. The HIPAA Final Security Standards and ISO/IEC 17799. SANS Institute, 2003. Retrieved January 2004 from http://www.sans.org.

[BSI02] British Standard Institution, British Standard 7799-2:2002 Information Security Management Systems - Specification with Guidance for Use. London, UK: BSI, 2002.

[BSI03a] British Standard Institution, Implementing BS 7799-2 Course: 2002. Delegate Workbook. London, UK: BSI, 2003.

[BSI03b] British Standard Institution, PAS 56: Guide to Business Continuity Management. London, UK: BSI, 2003.

[BSI04] British Standard Institution, Overview. Retrieved January 2004 from http://www.bsi-global.com

[Braber04] Braber, F.; Lund, M.; Lund, Stølen, K.; Vraalsen F. Reuse of Security Assessment Results under Design and Maintenance of IT Systems. Norway: SINTEF, 2004. Retrieved June 2004 from http://www.nr.no/coras

[Bravo02] Bravo R., *Criminalidade Informática, Perspectiva Actual*, presentation handout from the Security Conference, held in Lisbon, June, 2002.

[Campbell00] Campbell, P. Survivability via Control Objectives, IEEE Information Survivability Workshop. 2003. Retrieved December 2003 from http://www.cert.org/research/isw/isw2000/papers/24.pdf

[Capuder04] Capuder L., ISO-17799 - Standard for Information Security: A Welcome Boom for Security Management and Audit. The EDP Audit, Control, and Security Newsletter, May 2004 Vol. XXXI, N. 11, Boca Raton, US: Auerbach, 2004

[Carrier03] Carrier, B. Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers. In International Journal of Digital Evidence, Winter 2003, Volume 1, Issue 4. Retrieved January 2004 from http://www.ijde.org

[Carmical03] Carmical, D. Establishing a 7799 Information Security Management System. 2003. Retrieved December 2003 from http://www.sans.otg

[Carlson01] Carlson, Information Security Management: Understanding ISO 17799. US: Lucent Tecnologies, 2001. Retrieved June 2004 from www.netbotz.com/library/ISO_17799.pdf

[Carlson02] Carlson, Information Security Management: Understanding ISO 17799. US: INS, 2002. Retrieved June 2004 from www.ins.com.

[CERT04] Centre Emergency Response Team Coordination Centre (CERT-CC), Knowledge Base of vulnerabilities. Visited January 2004 at http://www.kb.cert.org/vuls/

[Clements96] Clements, R. Complete Guide to ISO 1400. Englewood Cliffs, US: Prentice Hall, 1996.

[CML04] Câmara Municipal de Lisboa, O Risco Sísmico na Cidade, Brochure from Departamento de Protecção Civil, Lisbon, Portugal: 2004

[CNPD04] Comissão Nacional de Protecção de Dados, http://www.cnpd.pt/bin/direitos/direitos.htm. Accessed on 25 July 2004.

[Cisco04] Cisco, Cisco Catalyst 2950 Series Switches with Standard Image Sw, http://www.cisco.com/en/US/products/hw/switches/ps628/products_data_sheet09186a00801cfb71.html, 2004

[CódigoCivil00] (Portuguese) Código Civil. Coimbra, Portugal: Livraria Almedina, 2000.

[CódigoTrabalho04] (Portuguese) Código do Trabalho. Coimbra, Portugal: Livraria Almedina, 2004.

[Conectiva04] Conectiva Corporation, http://www.conectiva.com.br/history. Accessed on 24 July 2004.

[Crabb01] Crabb, M. Building a Successful Security Infrastructure. Retrieved December 2003 from http://www.sans.org .

[CSI04] Computer Security Institute. Ninth annual CSI/FBI Computer Crime and Security Survey, 2003. Retrieved June, 2004 from: http://www.csi.org

[Davies89] Davies, D. & Price, W. Security for Computers Network. An Introduction to Data Security in Teleprocessing and Electronic Funds Transfer. West Sussex, UK: John Willey & Son Ltd., 1989.

[Doughty03] Doughty, K. Implementing Enterprise Security: a Case Study. Information Systems Control Journal, Vol. 2, March. London, UK: Elsevier Science Ltd, 2003. Retrieved December 2003 from http://www.b-on.pt

[Dhillon01] Dhillon G. & Backhouse, J. Current Directions in IS Security Research: Toward Socio-organizational Perspectives. Information Systems Journal, n. 11, pp. 129-156. 2001.

[DNV01] DNV, Interpretation Guide of BS 7799. London, UK: DNV, 2001. Retrieved June 2002 from http://www.dnv.com.

[DRII03] Disaster Recovery Institute, Business Continuity Plans Guidelines. St. Louis, MO, US: DRII, 2003. Retrieved June 2004 from http://www.drii.org.

[Dias04] Dias, M. ADETTI Presentation. Slide show. Lisbon, Portugal: ADETTI, 2004

[E&Y04] Ernst & Young. 2004 Information Security Survey. Available from http://www.ey.com, accessed June 2004.

[Ferrant04] Ferrant, Chris, Notes from the British Standard Institution, Implementing BS 7799-2 Course, held in Alcácer do Sal, June 2004. Further comments taken from discussions with C. Ferrant were added to these handouts.

[Fredriksen02] Fredriksen, J. Use of the Rational Unified Process for Development of Safety Related Computer Systems. 1993. Retrieved August 2003 from http://www.ia.hiof.no/~borres/mastersarchive/rune-thesis.pdf

[Freund93] Freund, J. Introduction to Probability. Minneola, US: Dover Publications, Inc., 1993.

[FCT04] Fundação para a Ciência e Tecnologia, Accessed June 2004 - http://www.fct.mctes.pt

[Gammassl02] Gammassl, BS 7799 Overview. 2002 Retrieved March 2002 from http://www.gammassl.co.uk./bs7799/history.html

[GBSI01] IT Security Criteria and IT Baseline Protection Certificate/Qualification, A Comparative Study of IT Security Criteria. p.14. Germany: BSI, 2001 Retrieved December, 2003 from http://www.bsi.bund.de/gshb/english/menue.htm

[GBSI04] IT Baseline Protection Manual: Catalogue of Threats. Germany: BSI, 2004 Retrieved December, 2004 from http://www.bsi.bund.de/english/gshb/manual/download/index.html

[Geus97] Geus, A. The Living Company. London, UK: Nicholas Brealey Publishing, 1997, pp. 24-28.

[Goseva-Popstojanova03] Goseva-Popstojanova, K.; Hassan, A.; Guedem, A; Abdelmoez, W.; Eldin D.; Ammar, H. Mili, A. IEEE Architectural-Level Risk Analysis Using UML. IEEE Transactions on Software Engineering, Vol.. 29, No. 10, October 2003. IEEE Computer Society, 2003. Retrieved March 2004 from http://www.b-on.pt

[Gordon03] Gordon, L.; Loeb, M.; Sohail, T. A Framework for Using Insurance for Cyber-Risk Management, Communications of the ACM, Vol. 46. No. 3. Nova York, US: ACM, 2003

[Govanus02] Govanus, G. & King, R. MCSE: Windows 2000 Network Security Design – Study Guide. Alameda, US: Sybex, 2002

[Gillingham03] Gillingham, J. Catalogue of Vulnerabilities, Threats and Controls, London, UK: Business Management Systems Advisor 7799.com. Handout in the BSI official course “Implementing BS 7799:2:2002” (June, 2004)

[Graff03] Graff, M. & Wyk, K. Secure Coding. Principles & Practices. Sebastopol: O´Reilly, 2003

[Gerber01] Gerber, M. & von Solms R.. From Risk Analysis to Security Requirements. Computers & Security, Vol. 20, pp. 577-584. Amsterdam, Holland: Elsevier Science, 2001

[Gran03] Gran, B. (editor) The CORAS Methodology for Model-based risk Assessment. Deliverable for project IST-2000-25031. 2003. Retrieved June 2004 from http://www.nr.no/coras.

[Guan03] Guan, B.; Lo, C.A; Wang, P., Hwang, J. Evaluation of Information Security Related Risks of an Organization – the Application of the Multi-criteria decision-making method. IEEE proceedings, 2003, pp. 168-175. Retrieved December 2003 from http://www.b-on.pt

[Guel01] Guel, M. A Short Primer For Developing Security Policies. SANS Institute, 2001. Retrieved August 2003 from http://www.sans.org.

[Herzog03] Herzog, P. OSSTMM 2.1. - Open-Source Security Testing Methodology Manual. ISECOM – The Institute for Security and Open Methodologies. Retrieved September 2003 http://www.isecom.info/mirror/osstmm.en.2.1.pdf

[Hoekstra02] Hoekstra, A & Conradie, CobiT, ITIL and ISO17799 - How to use them in to use them in conjunction. South Africa: PriceWaterhouseCoopers, 2002. Retrieved February 2004 from: http://www.isaca-calgary.ca

[Honeynet04] The Honeynet Project, Honeynet II. Edition 2004. Chapter 16 Profiling Retrieved August 2004 from http://www.honeynet.net.

[Houmb03] Houmb, S. & Jurjens, J. Developing Secure Networked Web-Based Systems Using Model-based Risk Assessment and UMLsec. Proceedings of the Tenth Asia-Pacific Software Engineering Conference (APSEC'03). IEEE Computer Science. IEEE, 2002. Retrieved March 2004 from http://www.nr.no/coras

[Hopkinson99] Hopkinson, J. The Relationship Between the SSE-CMM and the IT Security Guidance Document. 1999. Retrieved June 2003 from http://www.sse-cmm.org/lib/Papers/sse-guides.pdf

[Humphreys02a] Humphreys, T. & Plate, A. PD 3001:2002 Preparing for BS 7799-2 Certification. London, UK: British Standard Institution, 2002

[Humphreys02b] Humphreys, T. & Plate, A. PD 3002:2002 Guide to BS 7799 Risk Assessment. London, UK: British Standard Institution, 2002

[IEC97] IEC. Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems IEC61508

[I.M.P.03] Instituto de Meteorologia de Portugal, Actividade sísmica em Portugal. Lisboa, Portugal: Instituto de Meteorologia de Portugal, 2003

[Insight04] Insight Consulting. BS 7799 Compliance and Certification Datasheet. Retrieved May 2004 from http://www.insight.co.uk

[ISF03] Information Security Forum, Standard of Good Practice for Information Security. London, U.K: Information Security Forum, 2003.

[IFAC99] Financial and Management Accounting Committee. Enhancing Shareholder Wealth by Better Managing Business Risk. Director General. New York, US: International Federation of Accountants, 1999

[ISACA00] Information Systems Audit and Control Association (ISACA). Control Objectives for Information and related Technology (COBIT), ISACA, 2003. Retrieved January, 2004 from http://www.isaca.org/cobit

[ISO96] ISO/IEC TR 13335-1:1996, Guidelines for the Management of IT Security (GMITS) - Concepts and models for IT security. Geneva, Switzerland: ISO, 1996

[ISO97] ISO/IEC TR 13335-2:1997 GMITS - Managing and Planning for IT Security. Geneva, Switzerland: ISO, 1997

[ISO98] ISO/IEC TR 13335-3:1998 GMITS - Techniques for the Management of IT Security. Geneva, Switzerland: ISO, 1998

[ISO00a] ISO/IEC 17799 Information technology - Code of Practice for Information Security Management, Geneva, Switzerland: ISO, 2000

[ISO00b] ISO/IEC TR 13335-4 - Guidelines for the Management of IT Security (GMITS) - Selection of Safeguards. Geneva, Switzerland: ISO, 2000

[ISO01] ISO/IEC TR 13335-5:2001 GMITS - Management Guidance on Network Security. Geneva, Switzerland: ISO, 2001

[ISO02] ISO/IEC 19011 - Guidelines for Quality and Environmental Management Systems Auditing. Geneva, Switzerland: ISO, 2001

[ISSEA03] International Systems Security Engineering Association (ISSEA) Systems Security Engineering Capability Maturity Model Description Document, Version 3. Pittsburgh, US: ISSEA, 2003

[IUG03] The ISMS International User Group (UIG) The IMS Journal. Issue 2, February 2003. Retrieved June 2003 from http://www.xisec.com

[IQP00] Instituto Português da Qualidade, Norma Portuguesa: Sistema de Gestão da Qualidade (ISO 9001:2000), Monte da Caparica, Portugal: IPQ, 2000

[ITGI04] IT Governance Institute. COBIT Mapping pp. 10-11. ITGI, 2004. Retrieved December 2003 from http://www.itgi.org

[ITU03] International Telecommunications Union, Draft ITU-T Recommendation X.805 (Formerly X.css), Security architecture for systems providing end-to-end communications. Retrieved June 2004 from https://www.ietf.org/IESG/LIAISON/itut-sg17-ls-x805-end2end-communications.pdf

[Jeffcott02] Jeffcott, M. & Johnson, C. The Use of a Formalised Risk Model in NHS Information System Development. Cognition, Technology & Work Vol. pp.120–136 London, UK: Springer-Verlag Limited, 2002.

[Karp03] Karp, A., Enforce POLA on Processes to Control Virus, Applying the Principle of Least Authority on processes. Communications of the ACM, December 2003, Vol. 46. No. 12. New York, US: ACM, 2003

[Kauppinen09] Kauppinen, S. Modeling Internet Service Production. Dependability and Risk Assessment. Helsinki, Finland: Helsinki University of Technology, 1999.

[Korpela02] Korpela, J.; Lehmusvaara A,; Kyläheiko, K.; Tuominen M. Adjusting Safety Stock Requirements with an AHP-based Risk Analysis. Proceedings of the 36th Hawaii International Conference on System Sciences (HICSS'03). IEEE Computer Science, 2002. Retrieved January 2003 from http://www.b-on.pt

[Kraus72] Kraus, L. SAFE: Security Audit and Field Evaluation for Computer Facilities and Information Systems. New York, US: Amacom, 1972

[Labuschagne99] Labuschagne, L. A New Approach to Dynamic Internet Risk Analysis. Thesis submitted for the degree of Doctor Comercii. Johannesburg, South Africa: Rand Afrikaans University, 1999. Retrieved June 2003 from http://www.rau.za

[Lam04] Lam, K.; LeBlanc, D.; Smith B. Assessing Network Security. Redmond, US: Microsoft Press, 2004

[Lendrevie93] Lendrevie, J.; Lindon, D.; Dionísio, P.; Rodrigues, V. Mercator : Teoria e Prática do Marketing. Lisboa, Portugal: Publicações Dom Quixote, 1993

[Lillywhite04] Lillywhite, T. Implementing BS7799 in the UK National Health Service. Computers - Fraud & Security. Amsterdam, Holland: Elsevier, 2004

[Maiwald04] Maiwald, E. Fundamentals of Network Security. Burr Ridge Parkway, US: McGraw-Hill, 2004

[Marcinkowski01] Marcinkowski, S. Extranets: The Weakest Link & Security . SANS Institute. Retrieved August 2003 from http://www.sans.org

[Mendes04] Mendes, F. (In)segurança da Informação. Aplicação da ISO 17799. Handouts of the workshop held in Lisbon, June 2004. Further comments taken from discussions with F. Mendes were added to these handouts.

[Menkel-Meadon01] Menkel-Meadon, C., Mediation, Aldershot, UK: Darmount, 2001

[Mercuri03] Mercuri, R. Analyzing Security Costs, Communications of the ACM, Vol. 46. No. 6, New York, US: ACM, 2003

[Meta02] Meta Group. Ignoring Business Impact Analysis Invites Disaster. Stamford, US: Meta Group, 2002. Retrieved June 2004 from http://www.metagroup.com

[Meta04] Meta Group. Designing Security Domains to Manage Outbreak Risk. Stamford, US: Meta Group, 2004. Retrieved June 2004 from http://www.metagroup.com

[Microsoft04] Microsoft Consulting Services, Secure Corporate LANs - Security Framework. Presentation handout of Security Workshop, held in Tagus Park, Portugal, March 2004.

[Moberg01] Moberg, F. Security Analysis of an Information System Using an Attack Tree-based Methodology. Göteborg, Sweden: Chalmers University of Technology, 2001

[Morakis03] Morakis E., Vidalis, S. Blyth, A. Measuring Vulnerabilities and their Exploitation Cycle. Information Security Technical Report. Vol. 8, No. 4. Amsterdam, Holland: Elsevier Ltd, 2003

[Moore01] Moore, A.; Ellison, R.; Linger, R. Attack Modelling for Information Security and Survivability. Pittsburgh, US: Software Engineering Institute, 2001. Retrieved July 2002 from http://www.sei.org

[Nadel04] Nadel, B. (editor) Building Security Handbook for Architectural Planning and Design, New York, US: McGram-Hill, 2004

[Nash03] Nash J., Computer Security Expert Assist Team (CSEAT). 2003 Retrieved August 12, 2003 from National Institute of Standards and Technology site: http://cseat.nist.gov

[McNab04] McNab, C. Network Security Assessment. Sebastopol, US: O'Reilly Media, Inc, 2004.

[Neves03] Neves, D. Análise da Estrutura Organizacional. ADETTI internal report. Lisbon, Portugal: ADETTI, 2003

[NHSWales04] National Health Service of Wales, Risk Assessment Guidance Notes, Wales, UK, 2004

[NIST95] NIST Special Publication 800-12: An Introduction to Computer Security: The NIST Handbook. Washington, US: US Government Printing Office, 2001. Available at http://www.nist.gov

[NIST01] NIST Special Publication 800-30: Risk Management Guide. Washington, US: US Government Printing Office, 2001. Available June 2003 at http://www.nist.gov

[NIST03] NIST Special Publication 800-53: Recommended Security Controls for Federal Information Systems. Washington, US: US Government Printing Office, 2003. Available at http://www.nist.gov

[NIST04] Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories. Gaithersburg, US: National Institute of Standards and Technology, 2004. Available at http://www.nist.gov

[Nordin03] Nordin, I. Information Security Management System (ISMS) Introduction. SWEDAC, slide show presentation in security conference in Lithuania: 2003

[Noberg01] Norberg, S. Securing Windows NT/2000 Servers for the Internet. Sebastopol: O´Reilly, 2001

[NSA02] National Security Agency. Information Assurance Technical Framework. Fort Meade, US: National Security Agency, 2002

[Okabe03] Okabe, K. IT Performance Management - Maximizing IT Value. Canada: PriceWaterhouseCoopers, 2003. Retrieved February 2004 from: http://www.isaca-calgary.ca

[Oxford89] Cowie, A. (Chief editor) Oxford Advanced Learner's Dictionary of Current English. Oxford, UK: Oxford University Press, 1989.

[Pattinson02] Pattinson, F. Comparing ISO 17799:2000 with SSE CMM. 2002. Retrieved June 2003 from http://www.phi-solutions.com/documents/ISO17799_SSE_CMM_comparison.pdf

[Paul01] Paul, B. Evaluation of Security Risk associated with Networked Information Systems. Melbourne, Australia: Royal Melbourne Institute of Technology, 2001.

[Peltier00] Peltier, T. R. Information Security Risk Analysis. Boca Raton, US: Auerbach Publications, 2000.

[Pfleeger00] Pfleeger, C. Security in Computing. Second edition. Upper Saddle River, US: Prentice-Hall, 1997.

[Plate01] Plate, A. ISO/IEC 17799 Risk Assessment. Slide show presentation at SAF Conference at 8 May 2001. Sweden: Stockholm. 2001. Available at http://www.aexis.de in June 2003.

[Plate02] Plate, A. BS 7799 Certification - a European Case Study. Slide show presentation at Conference 7799 Goes Global. 2002. Available at http://www.aexis.de in June 2003.

[Pires2004] Pires, R. A. Qualidade – Sistemas de Gestão da Qualidade Lisboa, Portugal: Edições Sílabo Lda. 2004

[Porter85] Porter, M. Competitive Advantage. New York, US: Free Press, 1985

[Público04] Público (Portuguese Newspaper). Short news on Computadores n. 3 of May 2004, p.3

[Purser04] Purser, S. A Practical Guide to Managing Information Security. Norwood, MA, US: Artech House, 2004

[PWC02] PricewaterhouseCoopers UK. Information Security Breaches Survey 2002. Retrieved May 2003 from http://www.pwc.com

[Raptis02] Raptis, D.; Dimitrakos, T.; Gran, B.; Stolen, K. The CORAS Approach for Model-based Risk Management applied to e-Commerce Domain. Retrieved March 2004 from http://www.nr.no/coras

[Rees03] Rees, J.; Bandyopadhyay, S.; Spafford, E., PFIRES: A Policy Framework for Information Security, Communications of the ACM, Vol. 46. No. 7 July 2003, New York, US: ACM

[Russell92] Russell, D. and Gemi, Sr.,G. T. Computer Security Basics. Sebastopol, US: O'Reilly & Associates, Inc., 1992.

[Robinson02] Robinson, C. DoD Information Assurance. Info-Security Magazine, Vol. XX 2002. pp. 79-80.

[Kadam03] Kadam, A. Implementation Methodology for Information Security Management System (to comply with BS 7799 Requirements). 2003 Retrieved March 2004 from http://www.sans.org.

[Sawma02] Sawma, V. A New Methodology for Deriving Effective Countermeasures Design Models. Ottawa, Canada: Ottawa-Charleton Institute for Computer Science, 2002

[Schein85] Schein, E. Organizational Culture and Leadership. Sao Francisco, US: Jossey-Bass, 1985

[Schechter04] Schechter, S. Computer Security Strength & Risk: A Quantitative Approach. Cambridge, US: Harvard University, 2004

[Schneier99] Schneier B. Attack trees: Modelling security threats. Dr. Dobb’s Journal. December 1999. Retrieved from http://www.cert.org/archive/pdf/01tn001.pdf

[Scholtz04] Scholtz, T. Information Security Architecture Basics, Gartner Briefing Presentation. 2004

[Seaver03] Seaver, M., O´Mahony L. Gestão dos Sistemas de Segurança, Higiene e Saúde no Trabalho, Lisboa, Portugal: Monitor, 2003

[Stamatiou03] Stamatiou, Y., Henroksen, E,, Lund, M. , Mantzouranis, E., Psarros, M., Skipenes, E., Stathiakis, N., Stolen, K. Experiences from Using Model-based Risk Assessment to Evaluate the Security of a Telemedicine Application. 2003. Retrieved January 2004 from http://www.nr.no/coras .

[Skipper98] Skipper, H. International Risk and Insurance. First edition. New York, US: Irvwin/McGraw-Hill, 1998

[Spinellis99] Spinellis, D.; Kokolakis, S.; Gritzalis, S. Security requirements, risks and recommendations for small enterprise and home-office environments. Information Management & Computer Security N. 7/3. Retrieved from http://www.emerald-library.com at June, 2004.

[Siponen03] Siponen, M. Designing Secure Information System and Software. 2003. Retrieved June 2004 from http://herkules.oulu.fi/isbn9514267907/

[Sêmola03] Sêmola, M. Gestão da Segurança da Informação. Rio de Janeiro, Brazil: Editora Campus Ltd., 2003

[Serrão02] Serrão, C. A Importância das Infra-estruturas de Chave Pública no Comércio Electrónico de Conteúdos Digitais. Lisboa, Portugal: Instituto Superior de Ciências do Trabalho e da Empresa, 2002

[Silva03] Silva, P.; Carvalho, H.; Torres, C. Segurança dos Sistemas de Informação. Gestão Estratégica da Segurança Empresarial. Vila Nova de Famalicão, Portugal: Centro Atlântico, 2003

[Smith02] Smith, E & Eloff, J. A Prototype for Assessing Information Technology Risks in Health Care. Computers & Security. Vol 21, No 3. U.K: Elsevier Science Ltd, 2002

[Suh03] Suh, B. & Han, I. The IS risk analysis based on a business model. Information & Management 41, pp. 149–158 Amsterdam, Holland: Elsevier Science, 2003

[SullivanE03] Sullivan, E. Security Policy Models - The Bell- La Padula Mode. 2003. Retrieved January 2004 from http://www.cse.ogi.edu/~crispin/527/cse527%20Policy%20and%20BLP2.ppt

[Sullivan04] Sullivan, D. The Definitive Guide to Security Management. Retrieved from http://www.realtimepublishers.com at August 2004. US: Realtimepublishers.com, 2004

[Symantec04] Symantec Security Team, Handout of Security Trends. Slide show presentation, held in Lisbon, Portugal June 17 of 2004. Symantec, 2004.

[S.Pfleeger00] Pfleeger, S. Risky business: what we have yet to learn about risk management. The Journal of Systems and Software n. 53, pp. 265-273. Amsterdam, Holland: Elsevier Science, 2000

[Solms01a] Solms, B. & Solms, R. Incremental Information Security Certification. Computers & Security, n. 20, pp. 308-310. Amsterdam, Holland: Elsevier Science: 2001

[Solms01b] Solms, E. & Eloff, J. Information Security Development Trends. 2001. Retrieved December 2003 from: http://osprey.unisa.ac.za/saicsit2001/Electronic/paper52.PDF.

[Stabell98] Stabell, C., Fjeldstad, O. Configuring Value for Competitive Advantage: on Chains, Shops and Networks. 2004. Strategic Management Journal, Vol. 19, 413–437. London , UK: John Wiley & Son, 1998. Retrieved June 2004 from: http://www.business.uiuc.edu/gebauer/Courses/Readings/StabellFjeldstad_ValueConfiguration.pdf

[Stefaniu04] Stefaniu, M. ISO 17799 project at BMO Financial Group. Slide show presentation to ISO 17799 User Group. 2004. Retrieved June 2003 from: http://www.xisex.com

[Syta01] Syta, J. The Project of Information Security System based on ISO 17799 regulations for AVET INS. Warsaw, Poland: 2001 Retrieved June 2003 from: http://www.wip.edu.pl/index.php?d=3&s=55&rok_ukon=2002&id_abs=2856

[Swiderski04] Swiderski, F., Snyder, W. Threat Modelling. Redmond, US: Microsoft Press, 2004

[Tasker99] Tasker, P. Common Vulnerabilities and Exposures (CVE). MITRE Organization, 1999. Retrieved June 2001 from http://www.cve.mitre.org

[Tood02] Todd M., Colwill C. & Allen D., Benchmarking for Critical Infrastructure Protection Information Security Technical Report, Vol 7, No. 2 37-49. Amsterdam, Holland: Elsevier Science Ltd, 2002

[Trick04] Trick, M. Analytic Hierarchy Process. Retrieved August 2004 from http://mat.gsia.cmu.edu/mstc/multiple/node4.html

[Trivedi03] Trivedi, N. Disaster Recovery Planning, Stevens – Institute of Technology, 2002. Retrieved January 2004 from http://www.idugdb2-l.org/adminscripts/wa.exe?A1=ind0004a&L=db2-l

[UE04] European Commission – Information Society and Technology - Sixth Framework Programme (FP6) 2002-2006. Accessed March 2004 at http://ec.europa.eu/information_society/research/eu_research/index_en.htm

[Vaughan03] Implementing BS7799 Part 2 in an IT organization. A Case Study. Retrieved January 2004 from http://www.sans.org

[Visintine03] Visintine, V. An Introduction to Information Risk Assessment. SANS Institute, 2003. Retrieved from http://www.sans.org in January of 2004

[Valsamakis00] Valsamakis, A.; Vivian, R.; Troit, G.; Risk Management. Second Edition. Johannesburg, South Africa: Heinemann Higher and Further Education.

[M.Whitman04] Whitman, M. & Mattord, H. Management of Information Security. Boston, US: Thompson Course Technology, 2004

[Wadlow00] Wadlon, T. Segurança de Redes, Brazil: Editora Campus, 2000

[Wiechman03] Wiechman, G. 2003 Minnesota HIPAA 2003 Minnesota HIPAA - Implementation Summit Implementation Summit. Minnesota, US: Guidant Corporation, 2003

[Wikipedia04] Wikipedia, the free encyclopedia, Article "Earthquake" Retrieve July 2004 from http://en.wikipedia.org/wiki/Earthquake

[Wright99] Wright, M. Third Generation Risk Management Practices. Computer Fraud & Security. February 1999. Amsterdam, Holland: Elsevier B.V., 1999. Retrieved January 2004 from http://www.b-on.pt

[Wood87] Wood, C. (editor) Computer Security: a Comprehensive Controls Checklist. Chichester, UK: John Wiley and Sons, 1987.

[Wood02] Wood, C. Information Security Policies Made Easy Version 9. NetIQ Corporation, 2002. Retrieved June 2003 from http://www.netiq.com

[Yazar02] Yazar, Z. A Qualitative Risk Analysis and Management Tool - CRAMM. Retrieved from http://www.sans.org in September of 2003.

[Yurdakul03] Yurdakula, M, Tansel Y. AHP Approach in the Credit Evaluation of the Manufacturing Firms in Turkey. International Journal of Production

Economics No. 88, pp. 269–289 Amsterdam, Holland: Elsevier B.V., 2003. Retrieved January 2004 from http://www.b-on.pt

[XISEC04] Xisec Consulting, ISMS Scopes. 2004. Retrieved August 2004 from www.xisec.com

[Zuccato02] Zuccato, A. Towards a Systemic Holistic Security. Karlstad, Sweden: Karlstad University, 2002. Retrieved June 2003 from http://www.cs.kau.se/~albin.

ANNEXES

LIST OF ANNEXES

ANNEX A

A PROPOSED TAXONOMY OF RISK MANAGEMENT TECHNIQUES

If everyone pulled in the same direction, the whole world would topple over.
Yiddish proverb [1]

A.1 INTRODUCTION

This annex provides supplementary information to sustain the assertions made in chapter 3 of the dissertation text.

The cited chapter discusses the *actual procedures employed to conduct a risk management process* in accordance to BSI requirements. For the benefit of the chapter's length, some of these risk management practices were not described in detail. To remedy this situation, this annex presents for four of the nine methodological stages of BSI - as shown in Figure A.1 - a more comprehensive account of these procedures.

Figure A.1 depicts which of the phases of BSI risk management methodology, are discussed in this Annex. This figure illustrates also the correspondence between these phases and the sections of this Annex.

In each of these stages, techniques from several risk schemes are categorised in a proposed classification.

The examination of the assessment techniques is illustrated with an actual example: a document repository software called BSCW [2], which is operating in ADETTI, an IT research centre which is object of the case study.

.

.

[1] Cited in [Menkel-Meadon01].

[2] BSCW is a commercial product from Orbiteam (http://www.orbiteam.de).

Number	BSI method phase	Procedures examined in chapter 3	Procedures detailed in this annex
1	Define the ISMS scope	Scope selection procedures: a) Process based approach b) Information based approach	A.2 How to select the evaluation area? A.2.2.1 Process based approach A.2.2.2 Information based approach
2	Define the ISMS policy	Analysed phases of definition of security regulations: a) Definition of top-level security policy; b) Identification of applicable legal requirements; c) Definition of implementation-level policies (that is, procedures)	
3	Define a systematic approach to risk assessment	Type of formula of risk calculation: a) Monetary approaches b) Non-monetary approaches	A.3 How to calculate risk calculation? A.3.2.1 Monetary approaches A.3.2.2 Non-monetary approaches
4	Identify the risk	Threat identification: a) Threat catalogues b) Attack trees c) Threat profiles d) Threat modelling methods Vulnerability identification: a) Detection of only technological vulnerabilities b) Detection of technological vulnerabilities	A.4 How to identity threat? A.4.2.1 Threat catalogues A.4.2.2 Attack trees A.4.2.3 Threat profiles A.4.2.4 Threat modelling methods A.5 How to identity vulnerability? A.5.2.1 Detection of only technological vulnerabilities A.5.2.2 Detection of general vulnerabilities
5	Assess the risk	Probability estimation procedures: a) Estimations supported by a single variable b) Estimations supported by a combination of variables	A.6 How to estimate the probability of risks? A.6.2.1 Estimations supported by a single variable A.6.2.2 Estimations supported by a combination of variables
6	Identify and evaluate options for the treatment of risks	Risk acceptance or treatment decision based on: a) risk attributes as impact and probability; b) protection need; c) combination of both.	
7	Select control objectives and controls for the treatment of risk	Safeguard selection processes: a) risk analysis; b) security baseline.	
8	Prepare a Statement of Applicability	The available SoA templates in addition to the required, include also: a) risk and control reference; b) list of applicable legislation.	
9	Obtain management approval	Literature not found.	

Figure A.1: Structure of Annex A

A.2 HOW TO SELECT THE EVALUATION AREA

A.2.1 Outline

Due to the impossibility of finding a report revealing *what selection procedure was followed in an actual BSI´s implementation* [3] , the two presented methods were based on the literature regarding recommend guidelines to implement BSI´s risk management.

Two methods are proposed: the first uses a stating point the identification of process viewpoint and is supported by the works of BSI practitioners, such as Sêmola [03], Mendes [04], Kadam [03] and Syta [01]. The second approach is build upon the identification of information types and is the recommended technique by BSI training course [BSI03a].

A.2.2 Approaches for the selection of the evaluation area

A.2.2.1 A process based approach

a) Identification of organizational processes

In ADETTI, as in other organizations, it is possible to distinguish two types of processes: primary and support [Porter85].

Primary processes (or business processes) target the fulfilment of the organization's ultimate goal: to obtain profit for its stakeholders, in case of a company, or to generate knowledge and advances on science and technology, in case of ADETTI [Dias04]. Support processes cater to the conditions for the organization to function.

In ADETTI, an internal document [Neves03] has defined a group of organizational processes. According to this document, primary processes in ADETTI are activities associated with receiving inputs (finding research opportunities and preparing proposals), transforming them into the final product (research development) and then store and communicate the research results to the community (storage and dissemination of knowledge).

Support activities are the remaining activities not included in the primary activity categories [Stabell98], such as human resource management, administrative support or financial management, as illustrated in Figure A.2.

[3] Despite the large number of organizations certified as BSI compliant (890 in August 2004 [XISEC04]), a report showing the selection procedure of the evaluation area was not found.

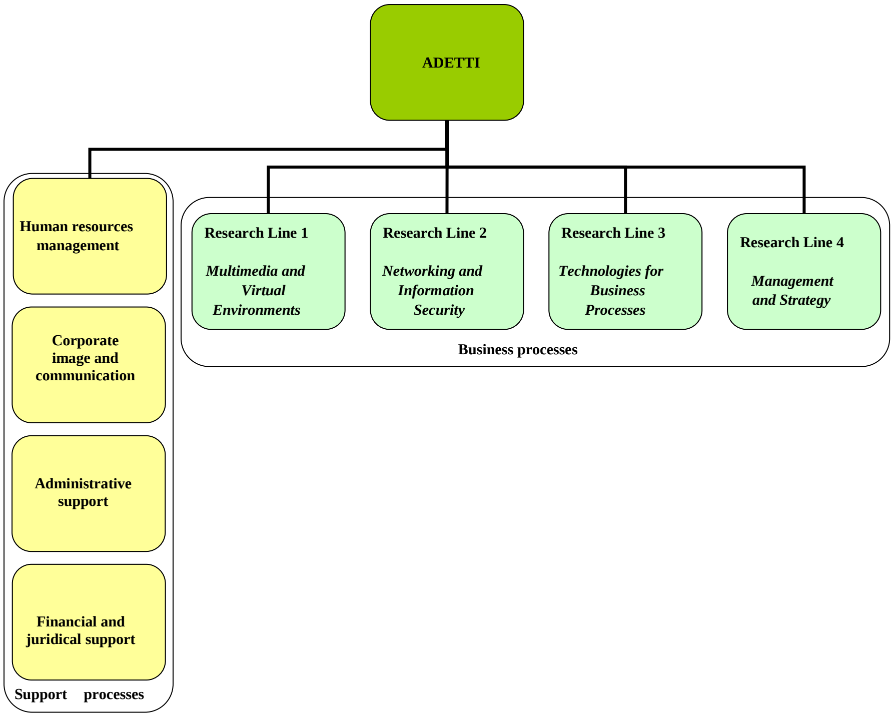

ADETTI
Human resources management
Corporate image and communication
Administrative support
Financial and juridical support
Support processes
Research Line 1
Multimedia and Virtual Environments
Research Line 2
Networking and Information Security
Research Line 3
Technologies for Business Processes
Research Line 4
Management and Strategy
Business processes

Figure A.2: Some of the processes in ADETTI

The identification of organizational processes should be done with input provided by internal documents and opinions from the actual managers and personnel of the organization. Their perception can be collected by techniques as structured interviews, brainstorming [Sêmola03] and Delphi approach [Syta01]. [4]

b) Classification of relevance of organizational processes

At this moment, the risk analyst has a number of processes. Nevertheless, not all of them have the same importance for an organization. The more relevant processes, as expected, should benefit from a tighter security than others. This is the purpose of relevance classification.

The business (or primary) processes may be classified with the assistance of business criteria, such as revenue, number of clients, strategic weight [Mendes04], as seen in Table A.1.

[4] Delphi approach is a structured method of group discussion [Syta01].

	Number of clients	Revenue	Strategic weight	Market share
Business Process 1				
Business Process 2				
Business Process 3				

Table A.1: Classification of relevance of business process (based on [Sêmola03]) [5]

Support processes may be ranked according to their recognized importance by an organization. For this purpose, a scale may be used. Table A.2 shows a model scale with scenarios to help evaluation of processes.

Scale	Scenario (if the process paralyse for a week, it would…)
1 - Not considerable	Means a low difficulty for the organization; may cause irrelevant impacts.
2 – Relevant	Means a difficulty for the organization; may cause partially relevant impacts.
3 – Important	Implies the paralysis of the organization; may cause partially significant impacts.
4 – Critical	Implies the paralysis of the organization; may cause highly significant impacts.
5 – Vital	Compromises the organization; may cause uncalculated impacts in terms of recuperation and business continuity.

Table A.2: Scale of importance of support processes (based on [Sêmola03])

As for the ADETTI example, *research lines*, the business processes for ADETTI, could be classified according to the strategic importance or the number of current projects in course. Support processes could be structured using the scale in Table A.2.

For the sake of simplicity, only support processes, shown in Figure A.2, were subjected to classification. The management staff of ADETTI concluded that (1) administrative support and (2) preparation of proposals (to apply for research funds) were the more significant support processes.

Accordingly, this approach concluded that document management process is the most suitable process to be subjected to evaluation.

After this process selection, the evaluation area (which can be designated as ISMS) will be characterized in terms of several aspects, including the information that holds inside.

[5] For ADETTI, relevance criteria could be number of spin-offs, number of registered patents, number of licenses of software developed, etc.

A.2.2.2 A information based approach

As stated, the purpose of the BSI is to protect information. Consequently, the evaluation territory could be defined using information [BSI03a]. This could be done by:

a) Gather a group of managers from sensitive departments of the organization.
b) Ask them to identify individually (1) the information that competitors will like most and (2) what is the information they need most for their work.
c) Collect the answer and discuss in group what the most important information in the organization is. This will be the basis for the ISMS.

As information is simply data which has meaning in a context (see *glossary*). Therefore, it is not sufficient to guard the information stored, if the activities that support it are not protected.

Therefore, after identifying the most important type of information (e.g. the client database), the activities that handle this information should be identified and then defended. These activities are described in a process manner that is identifying inputs, the transformation and outputs.

At the end, the ISMS will be the activities that deal with a certain type of information.

A.3 HOW TO CALCULATE RISKS

A.3.1 Outline

BSI demands a definition of the risk assessment approach prior to any assessment (*cf.* 3.4.1). As risks must be assessed using an equation between probability and impact value (*cf.* 3.4.3), the organization has to decide which risk equation should be employed. The several risk formulas founded in the literature may be classified in terms of monetary or non-monetary.

A.3.2 Risk calculation approaches

A.3.2.1 Monetary approaches

Some risk analysts calculate risk in order to determine its monetary costs [Sullivan04].

In the literature concerning this subject, three algorithms are often mentioned [Peltier00], [Suh03], [Sullivan04]: Exposure Factor, Single Loss Exposure (SLE) and Annualised Loss Exposure (ALE).

The Exposure Factor estimates the magnitude of impact on the asset that would arise from a threat occurrence. This term is expressed within a range from 0 to 100 percentage loss.

For example, suppose that the BSCW database has been valued at € 10,000. The risk analyst may estimate that in case of a hard disk failure, as weekly backups are being made; only 10% of the database information could not be restored from backups. Therefore, the Exposure Factor of BSCW would be 10%.

The Single Loss Exposure (SLE) is simply a financial calculation of the expected monetary effect of a specific threat. In SLE the asset value is multiplied by the loss exposure. In the BSCW example, the calculation is € 10,000 × 10%, which equals € 1,000.

The Annualised Loss Exposure (ALE) is also a financial evaluation, but in an annualised time frame [Peltier00]. To facilitate annual financial planning, the cost of a risk is exposed in an annualised format.

The formula of the Annualised Loss Exposure (ALE) is: [6]

Single Loss Exposure (SLE) **x** **Annualised Rate of Occurrence (ARO)** **=** **Annualised Loss Exposure (ALE)**

The Single Loss Exposure (SLE) has been described above.

The Annualised Rate of Occurrence (ARO) is the number of times a threat will occur in one year. This value is expressed in a decimal format.

Consequently, assuming that a hard disk failure affecting the BSCW server may occur once in 10 years, the Annualised Rate of Occurrence (ARO) would be 0.1. The ALE of a disk collapse in BSCW server is 0.1 × € 1,000, which equals € 100.

The ALE value is supposed to represent the maximum amount an organization should rationally spend to protect itself against a threat in a year. In this circumstance, ADETTI should not spend more than € 100 a year protecting the BSCW server against a disk malfunction.

The accuracy of these values is illusive. All of them are dependent on subjective estimation. The Exposure Factor and the Single Loss Exposure (SLE) are estimation of the financial cost of a risk. The Annualised Loss Exposure (ALE) combines in its formula an economical conjecture (SLE) and a speculation of the frequency of an event (ARO).

These formulas are often used to calculate the cost of implementing a new measure. The effective cost of a measure is the outcome of the subtraction of its implementation costs by any reduction in ALE from using the control [Pleeger00]. [7]

[6] Authors as Suh & Han [Suh03] have proposed amendments in the ALE formula.

[7] In this area, some efforts are accountable, as the Incident Cost Analysis Modelling Project (I-CAMP), developed by a group of US universities, or the guidelines for Cost-Benefit Analysis (CBA) from the US National Institute of Health [Mercuri03].

A.3.2.2 Non-monetary approaches

A group of authors calculate risk using scales of attributes [Alberts02], which can be numerical or non-numerical. [8]

Next, four qualitative formulas are described. These are entitled according to the number of inputs and type of output produced. The first one (which is the simplest) computes two inputs to produce a non-numerical output. The second and third one uses two variables and result, respectively, in an arithmetical and in a verbal output. The fourth is the most complex and uses 3 variables to provide a numerical output.

The second equation is from AS/ANZ 4360 [AS99], while all others are extracted from GMITS [ISO98] and reproduced in BSI`s training course [BSI03a]. All of these formulas assume that impact value is equal to the asset value. An illustration of the assumption is, for example, if a certain database has a value of 5, on a scale of 1 to 6, any security breach affecting this asset would result in an impact of 5. A risk causing total destruction of the asset and another risk resulting in unavailability for 2 minutes would be graded with the same impact.

As impact value is the same for all threats affecting the same asset. Impact could be deemed as a *neutral* element for risk calculation. Consequently, the determining factors of risk calculation are the ease of exploiting a vulnerability and the probability of a threat occurring.

a) A risk equation with 2 variables and a simple non-numerical output (GMITS)

This risk metric furnished by GMITS [98] merely qualifies the risk as tolerable (T) or intolerable (I), as shown in Table A.3. This two-factor equation (impact x probability) provides a binary classification, which, although simple, is not a risk decision support aid. The qualitative output does not indicate the most dangerous risks that need to be treated first.

As with other GMITS formulas, impact means asset value and frequency is the probability of threat.

Damage value Frequency value	0	1	2	3	4
0	T	T	T	T	I
1	T	T	T	T	I
2	T	T	T	T	I
3	T	T	T	T	I
4	I	I	I	I	I

Table A.3: Matrix of intolerable and tolerable risks

[8] These scales can be designed as *qualitative* in comparison to the monetary formulas which are *quantitative*. Qualitative approaches evaluate risks using relative values of their dangerousness to the organization. Quantitative approaches employ actual monetary values.

b) A risk equation with 2 variables and a numerical output (GMITS)

This is a classical formula to calculate risk that considers risk as a product of impact and probability. This formula, with two variables, results in three different situations: (1) if both factors, probability and impact, are low, there is no risk at all, (2) if one factor is high and another is low, there is a moderate risk and (3) if both factors are high, there is a high risk.

Initially, the risk analyst evaluates each asset, for example, with a predefined scale from 1 to 5, as shown in column *b* of Table A.4. This classification will reveal the impact of any threat in a particular asset. The second step is inserting the probability of threat in the matrix (in column *c*), using the same scale as employed for asset valuation. Subsequently, probability and impact are multiplied, as shown in column *d*.

Finally, threats are ranked in order of their *exposure* level, as seen in column *e* of Table A.4, from the most dangerous threat (which has the number 1 in column *e*) to the least hazardous.

Threat descriptor	Impact value of assets	Likelihood of threat occurrence	Measure of risk	Threat ranking
(a)	(b)	(c)	(d)	(e)
Threat A	5	2	10	2
Threat B	2	4	8	3
Threat C	3	5	15	1

Table A.4: Ranking of threats affecting several assets by measures of risk

If the BSCW server is estimated with an asset value of 5, and the threat of fire receives a probability of 2, the measure of risk is 10.

c) A risk equation with 2 variables and a non-numerical output (AS/ANZ 4360)

The Australian Standard - AS/NZS 4360 [AS99] - combines impact and probability. [9]

The first task is to define the significance of each grade of impact and probability scales. For each level of these scales, an organization positions the events that threaten specific assets.

For example, in ADETTI, in the consequence scale, a minor consequence was ascribed to unavailability of desktop1, but the disclosure of research output stored in the BSCW server was regarded as a major consequence. The remaining values were also exemplified with similar cases.

The frequency scale is ranked in accordance to the persistent level of threats, established by an organization. In this scale, for example, rare frequency can be defined as typical of incidents that occur less often than once every twentieth year.

[9] CORAS, a risk methodology studied in 2.4.1, adopts this formula.

After the frequency and consequence are estimated, these two values are combined in the subsequent matrix to produce a risk level.

Frequency value Consequence value	Rare	Unlikely	Possible	Likely	Certain
Insignificant	No Risk	No Risk	Low R.	Low R.	Medium R.
Minor	No Risk	Low Risk	Low Risk	Medium R.	Medium R.
Moderate	Low Risk	Low Risk	Medium R.	Medium R.	High R.
Major	Low Risk	Medium R.	Medium R.	High R.	High R.
Catastrophic	Medium R.	Medium R.	High Risk	High Risk	Extreme R.

Table A.5: Matrix of qualitative classification of risks

d) A risk equation with 3 variables and a numerical output (GMITS)

This risk algorithm correlates three factors: (1) the probability of threat, (2) the easiness of exploring vulnerability and (3) the asset value. The calculation is made in two steps. Initially the threat and vulnerability are combined in a value, which are designated as a frequency indicator. Afterwards, the frequency value is combined with asset value to produce the risk indicator.

The process starts with the assignment of a value to the asset. This value characterises the impact.

Furthermore, the threat level (indicates the likelihood of threat) and the vulnerability level (expresses the easiness of exploring vulnerability) are combined to produce the frequency value. [10]

For illustration proposes, we may suppose that BSCW has an asset value of 4 and that it is affected by only two threats: fire (Threat1) and hardware failure (Threat2). We may presume that Threat1 over BSCW has a low likelihood and a medium vulnerability easiness level. The subsequent frequency value would be 1, as seen in Table A.6. If Threat 2 over BSCW has a low probability, a high level of vulnerability, the frequency value would be 2.

Levels of threat (probability)	Low			Medium			High		
Levels of vulnerability	L	M	H	L	M	H	L	M	H
Frequency value	0	1	2	1	2	3	2	3	4

Table A.6: Calculation of frequency value

At this moment, the risk analyst intersects the frequency value with the asset value. The correlation of frequency with asset value results in a specific value, indicating the risk score.

[10] The term *frequency* is used with other meanings in risk literature. For OCTAVE, frequency is a synonym for objective probability [Alberts02].

As an asset suffers from various threats, we have to sum up all the threat/assets values to find a total asset score. This value represents all the applicable threats that an asset has.

Analysing Table A.7, the asset/threat score of BSCW/Threat1 is found. As BSCW has a value of 4 and the frequency value is 1, the intersection of both values provides us with score of 5. From this example, it is observed that a valuable asset (with an asset value of 4), with medium level vulnerabilities, even in the presence of a minor threat, reach a medium score.

Equally, for Threat2 over the BSCW, the frequency value is 2 and the asset value is 3, which results in asset/threat score of 5. In summary, the total asset/threat score for BSCW is 10 (we have added the score of both threats for this asset).

Asset value Frequency value	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	5
2	2	3	4	5	6
3	3	4	5	6	7
4	4	5	6	7	8

Table A.7: Asset/threat score

A.4 HOW TO IDENTIFY THREATS

A.4.1 Outline

The British Standard does not specify any requisite for the threat identification method. In literature four methods were founded: (1) catalogues of threats, (2) attack trees, (3) threat profiles using OCTAVE and (4) threat modelling using CORAS.

A.4.2 Threat identification approaches

A.4.2.1 Catalogues of threats

Organizations that follow this technique assume that their assets face similar threats to the ones gathered in those lists.

Lists of threats can be formulated on (1) the experience of practitioners, as the list of Peltier [00] or Gillingham [03], shown in Table A.8, (2) other lists are issued by international organizations, as German Federal Office for Information Security [GBSI04] or GMITS [ISO98]. GMITS is particular interesting as shows the mapping between each type of asset and its possible threats. Another source is (3) statistical data indicating the existing and most frequent threats, as reports from the Computer Security Institute or the Portuguese Criminal Police (*Polícia Judiciária*).

Natural threats	Accidental threats	Intentional threats
Acid rain	Disclosure	Disclosure
Air pollution	Operator/user error	Alteration of data
Cyclone	Software error	Alteration of software
Earthquake	Telecommunications interruption	Bomb threat
Flood	Electrical disturbance	Employee or external sabotage
Haze	Electrical interruption	Fraud
Humidity	Emanation	Riot/Civil disorder
Tornado	Environment failure	Strike
Tsunami	Fire	Theft
	Hardware failure	Unauthorised use
	Liquid leakage	Vandalism

Table A.8: List of threats classified according to intention (extracted from [Peltier00])

The annual survey of Computer Security Institute/Federal Bureau of Investigation (CSI/FBI) presents a ranking of the most frequent threats detected by the American organizations which have responded. According to the 2004 edition, threats considered most dangerous and frequent were [CSI04]:

Most frequent threats detected	Percentage
Virus	78%
Insider abuse of Net access	59%
Laptop/mobile theft	49%
System penetration	39%
Unauthorised access to information	37%
Denial of service	17%
Theft of proprietary information	10%
Sabotage	5%

Table A.9: Frequent threats according to 2004 CSI/FBI survey [CSI04]

As this set of threats reflects the experience of hundreds of organizations (481 respondents in the cited edition), may be regarded as a valid source of possible threats that might be applicable to other organizations.

In Portugal, the Criminal Police (*Polícia Judiciária*) has released a report that reveals that the 5 most frequent attacks from 2001 to 2002 were [Bravo03]: (1) illegitimate access; (2) paedophilia; (3) unauthorised use of proxies; (4) defamation and; (5) spam/mail bomb.

A.4.2.2 Attack trees

Attack trees were popularised by Schneier [99] and have been adopted in a number of studies [Slate99], [Moberg01], [Moore01] and [Schechter04].[11] Attack trees were described as a formal and practical method to uncover possible attacks paths [Moore01], [Swiderki04].

[11] Attack trees are a variation of tree-based methods as Fault Tree Analysis (FTA) and threat tree [Swiderski04].

To develop an attack tree, the first step is to identify possible goals of an attack. Each plausible goal of an attack will be the root node of a single tree. The attacker's approach to achieve this goal will be represented as lower level nodes of the tree. This newly created leaves can be thought of as sub-goals. Thus, for an attack to be successful, it has to attain these sub-goals in order to accomplish its main goal, the root node of a tree.

The relationship between sub-goal nodes pertains to the structure of an attack tree. Some set of sub-goals will need that all nodes be achieved for an attack to succeed. This relationship is represented as AND-decomposition, as illustrated in Figure A.3.

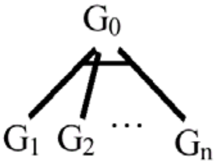


Figure A.3: Graphical representation of an AND-decomposition

Another set of attack sub-goals requires that only one of the nodes be achieved for an attack to be successful. This is symbolized as an OR-decomposition, as shown in Figure A.4:

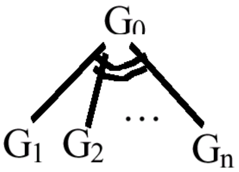


Figure A.4: Graphical representation of an OR-decomposition

For example, an attacker, who intends to gain a privileged access to BCSW Web Server, will need to achieve 5 sub-goals (as 1. Identify ADETTI Domain name and others). Each of these is attainable if one of the strategies described as OR is realized. To determine ADETTI firewall access control policy (the third sub-goal), the attacker will have to either search for specific default listening ports or otherwise scan ports broadly for any listening port.

This attack tree is represented graphically in Figure A.5:

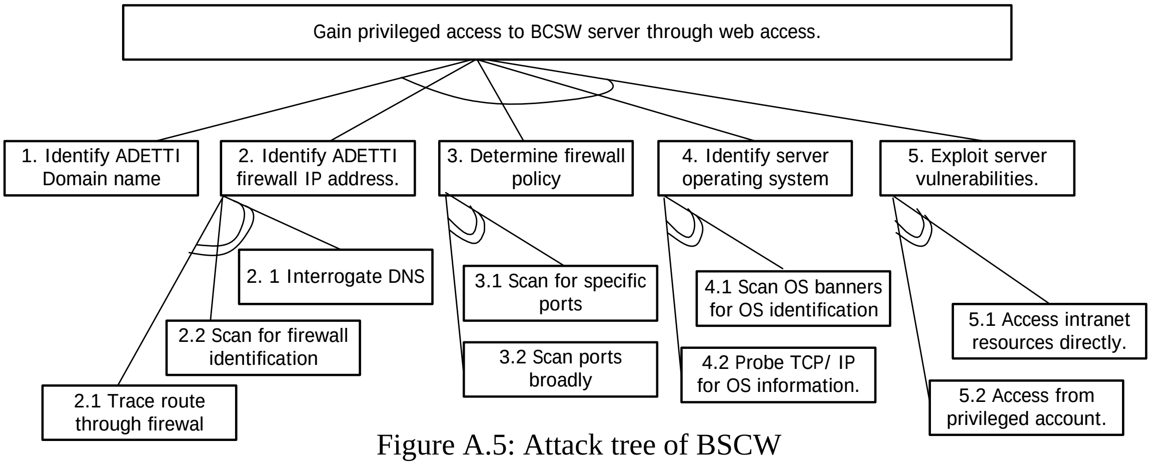

Gain privileged access to BCSW server through web access.
1. Identify ADETTI Domain name
2. Identify ADETTI firewall IP address.
3. Determine firewall policy
4. Identify server operating system
5. Exploit server vulnerabilities.
2. 1 Interrogate DNS
2.2 Scan for firewall identification
2.1 Trace route through firewal
3.1 Scan for specific ports
3.2 Scan ports broadly
4.1 Scan OS banners for OS identification
4.2 Probe TCP/ IP for OS information.
5.1 Access intranet resources directly.
5.2 Access from privileged account.

Figure A.5: Attack tree of BSCW

In conclusion, the attack tree approach requires broad security knowledge by the security auditor to identify the different attack methods that could be used by attackers. As this method places the adversary's goals at the centre of threat analysis, it is very suitable to examine human instigated threats. [12]

The method is in particular applicable to systems not very large or complex and which are not susceptible to suffer changes constantly [Morakis03].

The reason behind this restricted scope is the manner in which attack trees are constructed. As every possible path for an attack must be considered, an intricate system would require an extremely lengthy tree.

A.4.2.3 Threat profiles: the OCTAVE approach

OCTAVE, the risk assessment method of the Software Engineering Institute, recommends that threats be identified through the assistance of *areas of concern* and *threat profiles* [Alberts02].

A group of users and managers is asked to identify threatening events for the most important assets. These events are portrayed in sentences, establishing the threat source (the threat agent) and their outcome (the violation of a security property, as confidentiality). These phrases are designated as *areas of concern*.

To maintain consistency in assessments, OCTAVE advocates that the definition of areas of concern be founded on a predefined set of threat source categories and outcomes, as illustrated in Figure A.6.

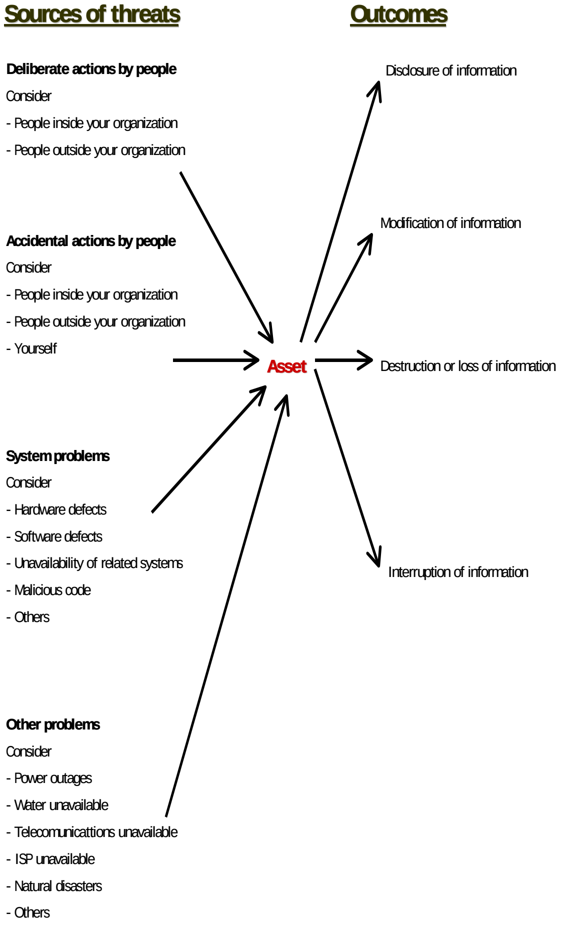

Sources of threats
Outcomes
Deliberate actions by people
Consider
- People inside your organization
- People outside your organization
Accidental actions by people
Consider
- People inside your organization
- People outside your organization
- Yourself
System problems
Consider
- Hardware defects
- Software defects
- Unavailability of related systems
- Malicious code
- Others
Other problems
Consider
- Power outages
- Water unavailable
- Telecomunicattions unavailable
- ISP unavailable
- Natural disasters
- Others
Asset
Disclosure of information
Modification of information
Destruction or loss of information
Interruption of information

Figure A.6: Categories of threats according to OCTAVE

[12] Some authors use attack tree to investigate all possible threats, including natural threats [Moberg01].

As an example, Table A.10 shows some areas of concern about the BCSW server.

Areas of concern	Threat source	Outcome
The risk of an outside intrusion into BSCW is much higher than other systems because of its public exposure.	Deliberate actions by people	Disclosure, Modification
A user modifies inadvertently important files.	Accidental actions by people	Modification
Inherent flaws and vulnerabilities in supporting applications could be exploited.	Deliberate actions by people	Modification, Destruction Disclosure

Table A.10: Areas of concern for an information system (BSCW) in ADETTI.

Each area of concern represents a distinctive threat. OCTAVE characterises threats using the following features [Alberts02]:

- asset any property valuable for the enterprise
- access which is the mode how the asset will be accessed by the actor (network access or physical access)
- actor who is someone (inside or outside to an organization) that may violate the security requirements (CIA) of an asset
- motive the human actions that may be deliberate or accidental
- outcome the disclosure, modification, destruction, loss or interruption of the security requirements of an asset

Consequently, each area of concern is depicted by this set of attributes, as shown in Table A.11.

Areas of concern	Threat properties
1. The risk of an outside intrusion into BSCW is much higher than other systems because of its public exposure.	- asset: BCSW - access: network - actor: outside - motive: deliberate - outcome: disclosure, modification
2. A user modifies inadvertently important files.	- asset: BCSW - access: network - actor: outside or inside - motive: accidental - outcome: modification
3. Inherent flaws and vulnerabilities in supporting applications could be exploited.	- asset: BCSW - access: network - actor: outside or inside - motive: deliberate - outcome: modification, destruction, disclosure

Table A.11: Areas of concern for an information system (BSCW) in ADETTI.

The threats resulting from this analysis are subsequently positioned in a catalogue of threats, which structures threats according to their source. Thus, OCTAVE considers four threat categories:

- human actors using network access (threats performed by a person via network access to the system)

- human actors using physical access
- system problems (e.g. hardware defects, software defects, etc.)
- other problems (threats beyond the control of an organization, e.g. natural disasters, etc)

Each of the four categories is represented in a tree format.

As the three areas of concern identified in ADETTI are related to human actions and network attacks, these threats are represented by a single threat tree, which addresses human actions using network access, as shown in Figure A.7.

A tree involving human actors is characterized by asset, access mode, actor, motive and outcome. [13]

Figure A.7 shows the threat tree of BCSW. The numbers in parentheses refer to the areas of concern. An area of concern could be mapped into multiple branches. Note that a solid line denotes the existence of a threat, while a dashed line indicates no threat to the asset. These unmarked threats (dashed lines) will be checked once again to confirm the inexistence of threats. [14]

In conclusion, OCTAVE builds threats from an organization's perception and then consolidates them with a predefined threat catalogue in a tree format; thereby, forcing the organization to examine a range of possible threats.

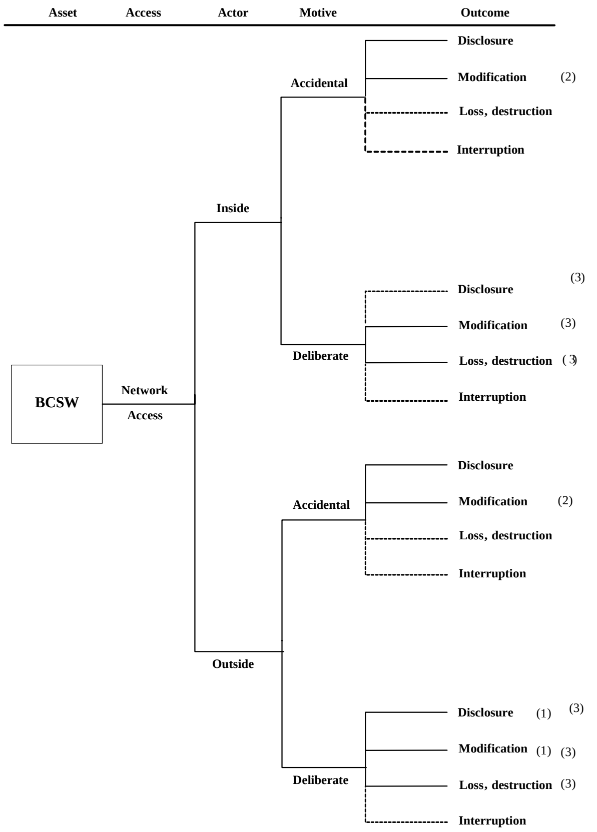


Figure A.7: Threat profile of areas of concern of BSCW

A.4.2.4 Threat modelling: the CORAS approach

[13] The threats derived from no-human actors are only represented by the concepts of asset, actor and outcome. As understandable, a natural threat does not have a motive or a privileged form of access.

[14] OCTAVE suggests that an organization should check these unmarked threats, in order to examine whether these threats were overlooked during the assessment.

As expected, CORAS, a system risk methodology (*cf.* 2.4.1), identifies threats associated with systems and those, which are related to the system maintenance and development process [Aagedal02].

CORAS makes use of a number of methods, like Hazard and Operability (HazOp), Fault Trees Analysis (FTA), Event Trees Analysis (ETA) and Failure Mode, Effect and Criticality Analysis (FMECA) [Gran03]. These methods are considered to be by a large extent complementary, as they focus on different types of risks or different areas of concern [Stamatiou03], [Stathiakis03].

Hazard and Operability (HazOp) is basically a structured brainstorming technique, designed to recognise in a system how deviations from the design specifications could result in hazards [Khan97], [Stamatiou03], [Houmb03].

HazOp enables the grouping of several threat scenarios, which may be further detailed by Fault Trees Analysis (FTA) and Failure Mode, Effect and Criticality Analysis (FMECA).

Fault Tree Analysis (FTA) employs deductive logic [Houmb03]. First, an unwanted event is defined, and then causal relationships of the failures leading to that event are identified. [15]

Instead of this top-down approach starting from unwanted outcomes, Failure Mode Effect and Criticality Analysis (FMECA) uses a bottom-up analysis for critical components. For each component of a system, all possible failures and their effects are identified, and then they are classified according to their criticality.

To sum up, CORAS employs techniques to elicit unwanted events (as HazOp) to analyse its causes (as FTA) and its consequences and criticality (using FMECA and ETA).

A.5 HOW TO IDENTIFY VULNERABILITIES

A.5.1 Outline

Similar to the previous stages, BSI does not provide guidelines to identify vulnerability. However, ISO (which is the countermeasures catalogue, sibling of BSI) endorses the utilization of vulnerability scanners and advises performing penetration tests to verify the infrastructure security [BSI02].

The classification of an asset's feature as a security flaw may be not as simple as recognising a Boolean value. Some vulnerability may depend on not only of a single aspect, but a group of them [Morakis03]. [16]

[15] A method related with Fault Tree Analysis (FTA) is Event Tree Analysis (ETA). Whereas Fault Tree determines the underlying causes of faults, Event Tree identifies the consequences of them [Aagedal02].

[16] Some weaknesses are not so straightforward to classify. Suppose that a server had the Trivial FTP (tftp) port open? Concerning this issue, CERT advises to [CERT04]: (1) create a separate partition to store the files; (2) ensure that those files are not writable. Therefore, the tftp port can be a vulnerability, if certain

A.5.2 Approaches for the identification of vulnerabilities

A.5.2.1 Detection of only technological vulnerabilities

Technological faults, especially if exploited by computer programs, [17] can be detected through automated tools, which can be categorised into 3 varieties: (1) vulnerability scanners (active scanning); (2) network surveillance tools (passive scanning) and; (3) software testing tools (source code exam).

Vulnerability scanners discover computers and applications, identify security mistakes (as weak passwords of user accounts), search for known vulnerabilities and even test exposure to common attacks [Stalling98], [Lam04]. [18]

Some scanners are tailored to evaluate only a particular type of systems as Whisker [19], which examines only flaws in web applications [Graff03], while other scanners are able to verify a number of different systems, examining in detail the network layer of systems. Examples of these scanners are COPS (developed by Dan Farmer), SATAN (written by Dan Farmer and Wietse Venema) and Nessus, originally developed by Renuad Deraison [McNab04].

All of the above scanners perform, basically, an active scanning of vulnerabilities. In other words, they attempt to illicit a response from a server by placing packets "on the wire" [Honeynet04].

Network scanners, as Nessus, interrogate the network for available services. Applications scanners, as Whisker, apply techniques known as black box testing or fault injection. These techniques try to make the application fail by deliberately providing fault inputs or parameters. This mutated input code is used to uncover buffer overflow or SQL injection problems [Graff03].

Another method to stumble upon vulnerabilities is to use network surveillance tools, which act as monitors of existing traffic (passive scanning). Network protocol analysers (as NAI Sniffer), and Intrusion Detection Systems (as Snort), are able to "sniff" packets in search of traces of vestiges of vulnerabilities, such as abnormal traffic in hosts or lapses in the application of firewall rules [Honeynet04]. [20]

precautions were not taking care of. This case illustrates a vulnerability that depends on not only a single aspect of configuration, but a group of aspects of configuration.

[17] An exploit is a computer program designed to take advantage of a vulnerability. CERT uses the term *exposure* to designated vulnerabilities, which are exploited [Honeynet04].

[18] These databases can be anchored in a vulnerabilities lexicon. Common Vulnerability Evaluation (http://www.cve.mitre.org/) maintains a dictionary of vulnerabilities that identifies known weaknesses. For example the CGI phf in Unix vulnerability is listed as *CVE-1999-0067* with the description *CGI phf program allows remote command execution through shell metacharacters*. As deduced, this was the 67th vulnerability published in 1999. Most important vulnerability catalogues, as the Centre Emergency Response Team Coordination Centre (CERT-CC) at http://www.kb.cert.org/vuls/, or SysAdmin, Audit, Network, Security (SANS) Top vulnerabilities (http://www.sans.org) comply with the CVE format.

[19] Whisker, a CGI scanner, is available at http://www.securiteam.com/tools/3R5QHQAPPY.html.

[20] The NAI Sniffer is available at http://www.sniffer.com. Snort is an open source application that can be retrieved from http://www.sourceforge.net .

A third approach in the identification of vulnerabilities is testing tools for software. These tools assess the security robustness of applications at the several stages of their life cycle [Graff03].

During the implementation stage of software, flaws may be revealed by static code checkers, such as RATS or Splint, that parse through and scan the source code for potential security pitfalls. [21] After the deployment of software in a production environment, it may be monitored with profiling tools, as Papillon or Janus. [22]

These software profilers attempt to define a standard behaviour of a program (what calls does the program make, what files need to be read or written) and subsequently watch for anomalies [Graff03].

To sum up, technological vulnerabilities can be identified by tools performing active, passive or source code scanning.

Active scanning tools are well accepted by organisations [Sawma02]. Passive scanning is regarded as time cumbersome due to the time needed to analyse alarms produced by IDS [McNab04]. Finally, software testing is used in restraint since it requires access to the source code of software [Graff03].

Other technological vulnerabilities, which are related to IT system but not detected by automated tools, as physical and natural vulnerabilities (*cf.* 2.3.3), are identified by auditing frameworks, usually applied to non-technological vulnerabilities, as seen further.

A.5.2.2 Identification of general vulnerabilities

As examined, technical weaknesses are detected with the assistance of predefined lists of vulnerabilities. Similarly, non-technical vulnerabilities also need to be identified through the support of a set of rules accepted as a security guideline by an organization.

The comparison between the actual actions of the workers of an organization with the procedures recommended by a security catalogues or established by the organization’s own policies may unveil discrepancies. For instance, some control mechanisms defined in an organization policy may not be in place, or may not be sufficiently robust enough [Sawma02]. [23]

The process of tracking down lapses between an ideal list of controls and the existing situation is designated as *gap analysis* [Sêmola03].

[21] RATS scans C, C++, Perl and PHP and is available at http://www.securesoftware.com/download_rats.html. Splint (http://www.splint.org) examines C source code.

[22] Papillon (http://www.roqe.org/papillion) screens possible attacks of system users. Janus safeguards system calls made by not trusted applications; can be retrieved from http://www.cs.berkeley.edu/~daw/janus/.

[23] As defined in 2.3.3, vulnerabilities are indications of missing or inadequate security practices.

Frequently, this form of security auditing employs questionnaires to collect the perception of the human actors. [24]

A more intrusive examination is penetration tests. This type of analysis reveals how technical and non-technical vulnerabilities may be exploited [Lam04]. In this way, a team of hired professionals try to break into the logical and physical defences of an organization. [25] The results of the attack are documented and the protection strength of the network is estimated based on their relative success [Govanus02].

A.6 HOW TO ESTIMATE THE PROBABILITY OF RISKS

A.6.1 Outline

The probability of any event can be estimated by two general approaches, known as objective and subjective probability [Bernstein96].

The probability is objective when the likelihood is expressed as a real number associated with an event. [26] For example, if someone flips a coin, he has a 50% chance of getting heads. This estimation is drawn from knowledge derived from past events. Once a coin is flipped, a person knows there are only two possible outcomes. The past experience enables a person to assess the frequency of a particular event. In the current case, heads and tails each have a 50% possibility. [27]

On the other hand, if a person ascertains the probability based on what he believes to be the likely occurrence of a risk, this probability is labelled as subjective [Alberts02].

Probability, for BSI [02], should be assessed in line with threats, vulnerabilities and impacts associated with the asset.

In an ideal situation, an organization would have enough data about past events to reasonably predict future occurrences [Sullivan04]. For example, historical audit logs from network monitors could unveil the frequency of hacker’s attacks in the past.

[24] OCTAVE and CORAS are among the risk methods that use questionnaires [Alberts01]. CORAS recommends the use of a set of questions based on the controls of ISO [ISO00a].

[25] These tests, usually, follow ad-hoc methodologies. An exception is Open Source Security Testing Methodology Manual (OSSTMM), which proposes a structured security test methodology [Herzog03].

[26] In objective probability, the likelihood of the occurrence of an event is the proportion of the time that similar events will occur over a long period of time [Bernstein96]. In order words, the probability (P) of an event (e) results from the proportion between the number of favourable results to the event (m) and the number of possible and likely results.

[27] According to the law of large numbers [Freund93], as the number of times a situation is repeated becomes larger, the proportion of successes tends toward the actual probability of success.

Assuming that both the exposure of an organization and the hacker activity has maintained the same level, the risk analyst could try to elicit the probability of hacker's risk from the audit records. [28]

However, most organizations have not collected sufficient data on risks to determine an estimation of probability based on frequency of occurrences [Alberts02]. When no frequency data is available, as frequently for risks perpetrated by human actors, an objective calculation of probability is not feasible.

The remaining probability approach relies upon the experience of persons to make educated guess about the likelihood of attack occurrence [Alberts02].

Estimation of subjective probability is based on the risk's variables. As risk is defined as the relationship between a vulnerability of an asset and a threat posed by an agent (*cf.* 2.2), consequently, the probability of a risk can be seen as derived from these elements. This estimation can be derived from a single or a combination of factors, as seen bellow.

A.6.2 Approaches for the estimation of risk

A.6.2.1 Estimations supported by a single variable

The probability of a risk, for some, is explained by a single variable: either the vulnerability or the threat agent.

An example of the first case is AS/ANZ 4360 [AS99]. The Australian standard regards the probability of a risk as a function of factors associated with assets. According to this perspective, the likelihood of risk depends upon the easiness of exploiting a vulnerability and surpassing the protective countermeasures of an asset [AS99].

In the same path, Suh & Han [03] argue that vulnerabilities are deficiencies in the security scheme of an organization. Therefore, likelihood of risks should be determined by the inspection of effectiveness and weakness of their security system, regardless of any threat consideration [Suh03].

The second theoretical pattern of subjective probability may be labelled as the protagonist model [Tood02].

Contrary to the first subjective probability approach, which estimate the risk likelihood based only on vulnerabilities, the protagonist model employs threat related factors. The primary aim of this model is to assess the likelihood of risks by considering the motivation, capability and access level of a threat agent towards the asset [Maiwald04].

Scholars as Maiwald [04] advocate that as vulnerabilities are passive elements, the probability of a risks occurring depends on the threat agent.

[28] The deployment of honeypots, as sensor devices gathering data on known and new exploits, may be able to assist in the quantification of risk. Honeypots are exposed systems placed on the Internet to lure hackers [Honeynet04].

In the preceding section A.7.2.2 it was analysed an approach endorsed by GMITS [ISO98], which follows the protagonist pattern. [29]

A.6.2.2 Estimations supported by a combination of variables

The most accepted probabilistic model considers both vulnerabilities and threats, crucial to predict risks [Peltier00].

The likelihood of a risk, according to BSI, depends not only of the ease of exploitation of vulnerabilities, but also of the existence of a genuine threat agent and the attractiveness of the asset for the attacker [Braithwaite02].

[29] The GMITS example was the only one found in terms of risk frameworks. Nevertheless, the protagonist model is endorsed by authors as Tood & alt. [Tood02] and Maiwald [04]. Tood & alt. [Tood02] contends, for instance, that by identifying and profiling different group of attackers - as dissatisfied employees, commercial competitors or terrorists - it is possible to recognised diverse likelihood between each protagonist profile.

ANNEX B

DETAILED COMPARSION OF COUNTERMEASURES CATALOGUES

B.1 INTRODUCTION

This annex compares the security measures of ISO with those from GMITS, NIST and COBIT, supporting the assertions made in chapter four about the similarities between the four countermeasures catalogues.

The annex is organised according to the 10 domains of ISO, as seen in Figure B.1. Each section first introduces general considerations about the domain, then presents ISO requirements and lastly discusses communalities between the standards.

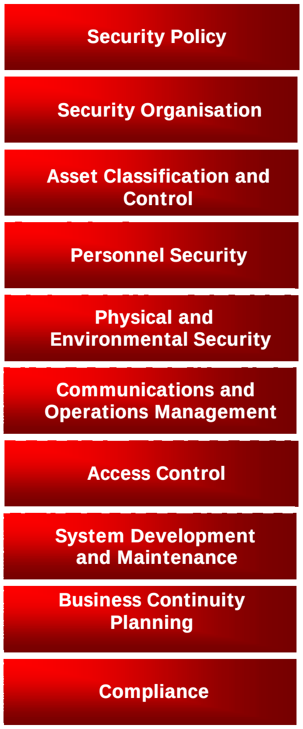

Security Policy
Security Organisation
Asset Classification and Control
Personnel Security
Physical and Environmental Security
Communications and Operations Management
Access Control
System Development and Maintenance
Business Continuity Planning
Compliance

Figure B.1: The 10 domains of ISO 17799

B.2 SECURITY POLICY

B.2.1 Background context

The larger the organization the more difficult it is to control the behaviour of its employees. Therefore, organizations need to introduce rules to reduce variations in behaviour of its workers and to guide their actions and attitudes [Marcinkowski01].

Security policies are aimed at defining appropriate behaviour, that is, actions aligned with the organization’s goals. As a consequence, it is expected that security policies mitigate risks associated with the *humanware* (i.e. personnel).

B.2.2 ISO requirements

Security policies must be developed, approved, communicated, reviewed and evaluated according to a defined documentation process. The *Code of Practice* addresses essentially two issues concerning security policy documents: (1) their content and (2) the revision and evaluation mechanism.

A security policy must include:

a) definition of the objectives, scope and importance of information security;
b) management statement demonstrating their support for security;
c) explanation of the security policies and compliance requirements followed by the organization;
d) definition of responsibilities for information security management;
e) references to documentation which support the policy.

A revision of policies is initiated by “any changes affecting the basis of the original risk assessment” [ISO00a:p2]. Significant modifications of the organization’s structure, a transformation of its technical infrastructure or a dangerous security incident are all qualified events that might trigger the revision process.

The effectiveness of security policies must be assessed by the organization. The *Code of Practice* recommends the preservation of records of security incidents in order to demonstrate the policy success ratio.

B.2.3 Comparisons with other models

ISO, NIST Handbook, COBIT and GMITS share a number of common security policies:

- security norms may be established in several forms, as policies, standards and written procedures;
- the primary source of security instructions is provided by policies;
- policies are supported by the organizational objectives and strategy.

The four catalogues structure security norms in a hierarchical order. Policies are positioned at the top of the hierarchy, while standards and procedures remain at the bottom.

Policies are conceived as strategic statements, which are detailed by operational specifications, in the form of standards and procedures. In this context, policies define objectives [Rees03], standards stipulate a uniform use of specific technologies, or parameters [NIST95] and procedures specify tasks for a particular system or users [ISO00a].

Accordingly, a policy might define that the organization has to have access to the source code of the operating systems in an office environment. A standard might describe how to harden a Linux workstation in an office environment. A possible procedure could be to create new user accounts and assign appropriate privileges.

In addition to these security norms, NIST Handbook (and other references as [Rees03]) proposes an additional security source: guidelines. Guidelines are positioned between standards and procedures. Standards, if adopted by an organization, [Rees03] assume a compulsory role, while guidelines are not compliant to follow, mere suggestions for *best practice*.

In cases where it is not possible to impose a uniform use, due to either variability of systems or high costs involved, [NIST95] a standard may not be established. In these circumstances, security recommendations may assume the figure of guidelines. An example of a guideline would be a document describing possible ways to harden a Linux workstation. Therefore, the role of guidelines is to ensure that security measures are not overlooked, but addressed by some means [NIST95].

Figure B.2 presents the hierarchy of security norms from NIST Handbook, which is the most comprehensive of the catalogues studied. Notice that ISO uses the term *guidelines* in a different context. [30]

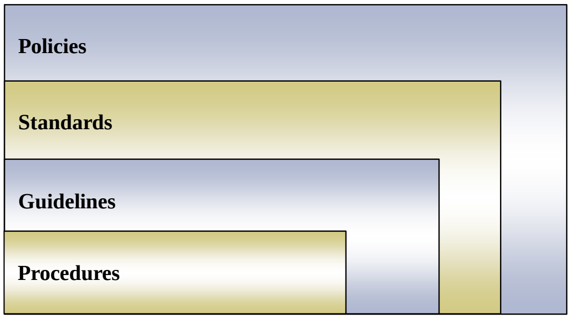


Figure B.2: Hierarchy of security norms according to NIST

The third similarity found in these catalogues is the relationship between the organization strategy and policies.

[30] ISO recommends organizations to regard the *Code of Practice*s as "a starting point for developing organization specific guidance" [ISO00a:p.IX]. Those guidelines may overlap or add new controls, not included in the safeguard catalogue. It is advisable, "to retain cross-references which will facilitate compliance checking by auditors and business partners" [ISO00a:p.IX].

According to GMITS, policies are an outcome of the security objectives of an organization (what is to be achieved) and its strategies (how to achieve these objectives) [ISO02]. Thus, security policies define the rules to be observed in implementing the protection strategies.

Whereas GMITS has an IT system approach, COBIT has an IT management perspective. Hence, security policies are integrated in the IT organizational policies. As seen in Table B.6 (*c.f.* B.12), security policies are addressed by the process responsible for the definition of the information architecture.

In conclusion, as far as ISO is concerned:

- Security norms consist of policies, standards and procedures. There is a clear distinction between strategic and operational norms. COBIT shares this view. Conversely, GMITS and NIST Handbook include operational elements in policies, as observed from theirs taxonomies of policy. [31]
- Security norms must be supported by a revision and evaluation mechanism, as seen in Table B.6 (*cf.* section B.12). COBIT also shares this concern.
- Policies are untimely focused on the protection of information. [32] The object of policies diverges between catalogues. Policies of COBIT are concerned not only with security but with all aspects of IT management (as the effectiveness and efficiency of data). NIST Handbook and GMITS are aimed at the regulation of IT systems.

B.3 ORGANIZATIONAL SECURITY

B.3.1 Background context

This section focuses on security management (SM). ISO as a SM model defines not only a portfolio of controls, but also determines the creation of structures committed to the enforcement of those safeguards in organizations.

Information security has to be, according to the *Code of Practice*, assumed as a mission by the entire organization. Nevertheless, a specific structure in the organization has to be responsible for the implementation and maintenance of the information security measures.

[31] NIST Handbook and GMITS expose taxonomies of policies according to the policie´s scope. NIST Handbook proposes three categories of security policies: (1) program policies (organization wide); (2) issue-specific policies (as E-mail Privacy Policy or the Internet Use Policy) and (3) system-specific policies (for instance, the accounting or the payroll system). GMITS suggests a classification in two classes: (1) corporate IT security policies (IT security principles and directives applicable to an organization) and (2) IT system security policies (specify for each IT system adequate safeguards).

[32] ISO enumerates a number of specific policies concerned with other matters than information (e.g. the policy of servers operation). But the aim of all policies is to protect - in some cases indirectly - data.

B.3.2 ISO requirements

ISO establishes three issues in the realm of security management. Firstly, ISO advises how to organize the management of security in organizations. Secondly, the access management of third parties to the organization is addressed. The third aspect is the management of outsourcings contracts. The analysis follows this order:

a) Structure of security management

ISO specifies two organizational pillars, which are responsible for the enforcement of security: (1) the security forum and (2) the security officer.

The security forum is a committee accountable to all security activities in the organization. It has the following assignments: (1) review and approve security policy, (2) monitor changes in the exposure of information assets to major threats, (3) review and monitor information security incidents and (4) approve initiatives to enhance information security.

Operational responsibility should be entrusted to a single manager. Although, ISO never formally labelled this manager as *security officer*, this title is commonly used in related documents [Humphreys02a], [ISO98], [IUG03]. [33]

In large organizations, which might have decentralised security duty structures (for instance, a security manager for each business unit or project), there can be an additional structure: the cross-functional forum.

This forum brings together managers with security roles within specific departments of the organization. Therefore, the cross-functional forum should have an interdisciplinary approach including, obviously, the IT department.

Furthermore, the *Code of Practice* advocates that security management deals with the following issues:

- Allocation of responsibilities for both assets and security processes (for instance, the business continuity process).
- The authorisation to implement new IT systems in the infrastructure.
- The use of external experts to enhance the security knowledge of the organization.
- Co-operation with external organizations to combat threats.
- The independent review of the systems operation.

In conclusion, it may be concluded that for ISO 17799, security management is supported by the principles of (1) collective supervision and (2) individual responsibility.

[33] In fact, ISO only employs the expression *officer* in the position of *data protection officer* [ISO00a]. In contrast, GMITS uses the concept of *security officer* to designate the manager responsible for security activities [ISO98]. In some US corporations this position is known as *Chief Information Security Officer* (CISO) [Mainwald04].

Collective supervision is performed through organizational committees. Individual responsibility is achieved because everyone in the organization knows their own responsibilities in terms of assets and security functions. It must be noted that an asset can only have a single worker responsible who, even if s/he delegates part of his/her responsibility, is always accountable to it.

b) Access of third parties to the organization

ISO determines that "access to the organization's information processing facilities by third parties should be controlled" [ISO00a:p.5]. This control assumes two forms [DNV01]: (1) identifying and counteracting of the risks arising from such access and (2) establishing contractual clauses to regulate this access.

Whenever, an external entity needs to have access to the organization's systems, (a database or any other asset on its technical infrastructure) ISO advises to perform a risk assessment. This evaluation aims to identify the security implications of the access and decide on the controls that are required.

ISO recommends the formalisation of security agreements (or the inclusion of security clauses in existing contracts) with the organizations that have physical or logical access to the organization.

Security arrangements concerning external access should reflect the different access conditions: access during or outside normal working hours, physical areas visited, types of data accessed, etc. For example, an organization could have a standard non-disclosure agreement for all external personnel that enter its facilities, as well as detailed security agreement for subcontracted personnel.

c) Management of outsourcing contracts

The access of outsourcing partners has to be based on formal arrangements. These agreements should address these matters:

a) legal requirements (e.g. data protection legislation);
b) arrangements to ensure that parties involved in the outsourcing are aware of their responsibilities;
c) controls to protect the CIA of the organization's business assets;
d) controls to ensure the availability of services in the event of a disaster;
e) establish the right of audit.

B.3.3 Comparisons with other models

The comparison of ISO with other catalogues has revealed that:

- The security management model, most related to ISO is GMITS. COBIT describes management structures orientated towards management of IT and not merely security. As NIST Handbook was designed for US governmental agencies, its management model is not appropriate for a different type of organization, as it recognises [NIST95].

- The other issues addressed by ISO - third party access and outsourcing - are also discussed by COBIT, as illustrated in Table B.6 (in section B.12).

GMITS and ISO agree, with slight differences, on the basic management supporters: (1) the security forum and (2) the security officer.

The security forum or committee has the ability to approve security policies and measures. The security officer is assigned the responsibility of implementing and controlling these decisions.

The formation of this committee is dealt with differently by both security paradigms. For the *Code of Practice*, the security forum is formed by managers and it may be part of an existing management body. As for GMITS, the security committee is a specific structure that gathers management representatives from the relevant sectors of the organization and includes representatives of users.

Similarly, the allocation of responsibilities differs in both standards. ISO assigns the responsibility of all security activities to a single manager, whereas all the organization's managers are accountable for security routine within their areas of management.

On the other hand, GMITS endorses a decentralized responsibility. In all the organization's divisions (departments, business units or project teams) an appointed security manager supervises IT security within that area.

B.4 ASSET CLASSIFICATION AND CONTROL

B.4.1 Background context

As it would be impossible, in a business perspective, to protect at the same level all assets [Alberts02], classification of asset serves to differentiate them by value and importance for an organization. Therefore, all assets of any kind (software, hardware, information assets, etc.) must be evaluated by the organization.

ISO advocates that information assets, in addition to the value estimation, should also receive a security classification. This security label identifies the degree of protection required by each of the three information security properties [Moberg01]: confidentiality, integrity and availability.

This classification should provide an appropriate labelling of information, showing whether the information is confidential or not, and indicate the procedure required to copy, store, transmit or destroy information.

B.4.2 ISO requirements

The standard recommends that all "important assets associated with each information system" [ISO00a:p.8] be:

a) identified (should include the current location);
b) estimated for its relative value and importance for the organization;
c) have a nominated owner.

In this process, the organization has to use a valuation scale of assets. Since ISO does not specify a procedure to evaluate the importance of assets for an organization, the risk analyst can choose any classification scheme.

In addition, information assets (i.e. tables of data in databases, paper documents, etc.) should also be:

a) classified in accordance with a security classification;
b) have a label that indicates this classification;
c) have specific handling procedures, i.e. copying, storage, transmission or destruction, according to its security rank.

This security categorisation is performed by the *information owner* (the person responsible for the information resource), who applies the information classification policy, adopted by the organization. An information classification policy establishes (1) a security classification scheme, formed by several levels (as public or confidential) and (2) particular procedures to handle assets in accordance to its classification, involving the reception, modification, copy, storage, transmission and destruction of information.

Information, following ISO instructions, should be graded as a function of (1) how sensitive it is and (2) how critical it is for an organization. Sensitivity refers to confidentiality. *Criticality* is measured in terms of availability and integrity. Consequently, ISO classifies information taking into account the three CIA dimensions.

The *Code of Practice* categorises assets in the following taxonomy:

a) information assets (databases and data files, archived information);
b) software assets (application software, development tools and utilities);
c) physical assets (as computer equipment, tapes, etc.);
d) services (as communications services, heating, and general utilities).

Assets must be inventoried with at least the following records: (1) asset name, (2) asset category (according to ISO taxonomy of assets, as described above), (3) asset value (in case of information asset include also the security classification), (4) location and (5) owner.

B.4.3 Comparisons with other models

The analysis of ISO and other catalogues shows that:

- Asset inventory is common to all standards, as seen in Table B.6, in section B.12 (actually, only ISO details the data to be collected in the inventory).
- The list of asset types of ISO (as described above) has similarities to the list of GMITS.

- All catalogues evaluate assets in terms of their value to the conduct of business in organizations. This process, instead of assessing the accounting value of assets, aims to evaluate an asset based on the business consequences that its damage would have.
- Only ISO and COBIT endorse a security classification for information assets. Both use the CIA aspects of information security as classification criteria. Neither describes a classification scheme, i.e. top secret, secret and public.

B.5 PERSONNEL SECURITY

B.5.1 Background context

Employees are the main *actors* in the security processes within an organization but are also its foremost threat. This ambivalence places the human element at the centre of all efforts targeted to improve security in organizations. On the one hand, a vast number of security controls are designed to have an effect on the actions of workers, enforcing the adoption of safer procedures. On the other hand, employees are regarded as the most probable initiator of an attack [Alberts02].

For a security catalogue as ISO, concerned with the protection of information, the human management issue has an utmost importance as workers are considered to be the main holders of information in an organization. [34]

B.5.2 ISO requirements

The objective of personnel controls is to reduce human error, theft, fraud or misuse acts committed by workers in an organization.

ISO mandates security requirements to be included in:

a) job responsibilities (security responsibilities must be included in the job description of every employee);
b) recruitment process (through validation of information provided by candidates);
c) formal agreements for confidentiality and acceptance of security responsibilities (non-disclosure agreement signed by all personnel);
d) user training;
e) procedures to report security incidents and software malfunctions;
f) monitoring mechanisms to identify and learn from incidents;
g) disciplinary measures for employees who have violated organizational security policies and procedures.

[34] Intellectual information (information stored in people's minds) can be considered to be the most important information resource [Mendes04].

The aforementioned requirements demonstrate that ISO assigns security measures for five of the human resources management areas: (1) job responsibilities definition, (2) recruitment, (3) contract obligations, (4) training and (5) disciplinary procedures.

In addition to the human resource issues, the *Code of Practice* appends to the personnel security (1) monitoring procedures and (2) incidents reporting.

Regardless of whatever controls implemented, security incidents are likely to happen. In this context, the security of an organization can only be improved if incidents are analysed, a diagnostic is made about its causes and insights are grasped to readjust security practices.

The importance of gaining insights from security incidents is emphasized by ISO. This is the heart of the operational system [DNV01], and it is through learning from incidents that measures can be readjusted.

All incidents and suspected weaknesses must be reported. A weakness can involve an IT tool or non-IT issues (a violation of written procedures, a malfunctioning door, etc.)

Reporting procedures must be accurate and rapid, since it is based on the reported data that disciplinary procedures can be undertaken.

B.5.3 Comparisons with other models

A set of assertions may be draw from ISO and other catalogues about personnel security:

- All four standards address personnel security;
- Controls of ISO are covered by COBIT, excluding the screening control (investigation of references provided by candidates for sensitive positions);
- Only ISO considers that incident response is a security measure for personnel security;
- Controls of the four catalogues point to the same strategy to improve personnel security.

The strategy underlining security practices can be regarded to be founded on three tactics:

a) imposition of security obligations;
b) promotion of security awareness and knowledge;
c) disciplinary measures.

Employees are forced to respect security obligations by means of formal agreements, acceptance of Acceptable User Policies and written procedures.

Security awareness and knowledge is achieved by training users. The staff has to be conscious of the relevance of security, be knowledgeable of the organization’s procedures and should be motivated to act in accordance.

In consequence, training is a key activity to ensure the success of a BSI implementation. [35] If the pervious tactics fail, disciplinary actions can be taken against employees. [36]

B.6. PHYSICAL AND ENVIRONMENTAL SECURITY

B.6.1 Background context

Physical attacks, such as theft are the infringement category that requires less IT knowledge from the offender [Wadlow00]. The easiness of these attacks vastly enlarges the group of suspected human agents able to initialise it.

On the other hand, electronic equipment is very sensitive to environmental changes, as its correct operation is dependent on an array of environmental conditions [Russell92].

Besides concerns related to the physical and environment threats, the increasing importance of physical safeguards [Mainwald04] is also explained by the dissuasive role it is considered to have on people.

Physical protection measures are highly visible to clients and employees by projecting a sign of the organization’s commitment to security [Russell92]. This transmits to potential transgressors the idea that any attack would be a vain endeavour, due to the high difficulty to overcome unnoticed barriers.

B.6.2 ISO requirements

ISO requires the protection of (1) facilities, (2) equipment and (3) *information support media* (paper, tapes, etc.) that hold sensitive information for an organization. [37]

The three objects must be protected from unauthorised physical access or interference, loss, theft and damage, as explained in Table B.1.

[35] Appropriate training and education is considered a critical success factor by ISO [ISO00a].

[36] An organization has the possibility to apply disciplinary actions only when the worker has been informed and has tacitly agreed with the security norms [Mendes04].

[37] Neither ISO nor BSI uses the expression of *information support media*, which is simply described as *media*. We suggest this expression because its meaning denotes, following the spirit of ISO, paper and non-electronic media supports.

Areas of concern	Explanations
Physical perimeters with access control	The organization has to implement a mechanism to control the access and traceability of persons on its premises.
Isolation of the area of reception and displacement of deliveries	These vulnerable areas must consequently have rigorous controls.
Sensitive equipment should be stored in places where risk of inadvertent damage or unauthorised access is reduced	Critical resources (equipment, vital records, etc.) have to be isolated, by means of physical provisions at the data centre entry or other.
Power supplies (protection from interruptions or anomalies in electrical power).	Electrical protection ensures availability of services and prevents power supply failures. Organizations may choose to implement controls to soften electrical surges or decide, for instance, to have alternative electrical suppliers or in-house generators. [38]
Cabling security (isolation from potential interference or damage sources)	Any latent threat on cabling must be identified (for example, an air-conditioning unit that might leak water over a switch).
Equipment maintenance	It is advised to maintain support contracts with manufactures. Due to the short existence cycle of IT products [Icove01], corrective repair of obsolete systems that require the acquisition of new components is often more expensive than the whole system's replacement.
Secure disposal or reuse of equipment	Organizations should erase residual information on storage devices prior to disposal or reuse. Shredders for paper destruction and low level formatting procedures for storage devices are ordinary provisions. [39]
"Clear desk" policy	To avoid theft or compromise of information, desks and monitor screens must be cleared.
Removal of property from the organization	This situation has to be properly approved.
Security of equipment off-premises	Management must authorise the utilisation of equipment under these circumstances.

Table B.1: Physical and environmental controls

B.6.3 Comparisons with other models

Physical and environmental security is, usually, identified with the protection of [Mainwald04], [Icove01]: (1) physical access, (2) climate, (3) fire and (4) electrical power.

In addition, ISO also notes concerns about the equipment security properties (sitting, power supplies, cabling, etc.) and its secure usage (several policies that indicate how the equipment and information should be physically protected).

[38] The protection level that technological controls furnish has to be assessed in a technological context. For example, in the case of a power supply interruption, in-house electrical generators take a few minutes to start delivering power supply. During this delay, Uninterrupted Power Supply (UPS) equipment ensures the power supply to critical resources. This example shows that effective protection requires a set of measures where each control compensates the others.

[39] The removal of information from a storage medium, like a hard disk or tape, is designated as sanitization [NIST95]. Information can be purged using methods such as overwriting information, degaussing (for magnetic media only), and destruction.

As a result, the analysis discusses the three dimensions of physical and environmental security: (1) physical access, (2) environmental security and (3) equipment security.

a) Physical access

Physical access is targeted to control the access to and trace people in secured areas of an organization [Silva03]. Through this manner, all access to secured areas is subjected to authorisation and records are made for future reference.

As illustrated in the Table B.6 (in Annex B.12), all control sets address physical access.

b) Environmental threats

All four-control directories address protection against environmental factors, as seen in Table B.6 (*c.f.* B.12).

c) Equipment security

The protection of equipment is of universal interest for security standards, as demonstrated by the four catalogues studied. As we may perceive from Table B.6 (*cf.* B.12), clear desk policy and a formal authorisation for the removal of property outside the organization, are unique to ISO.

B.7 COMMUNICATIONS AND OPERATIONS MANAGEMENT

B.7.1 Background context

This domain is concerned with how the information is processed, stored and transmitted in an organization and across its borders.

Frequently, this section is simply entitled *computer and network management*. [40] This designation translates a scope lessening: moreover to desktop and network management, this section deals with incident response procedures, exchange of information and software and e-commerce requirements.

B.7.2 ISO requirements

ISO subdivides this section into seven aspects whish are further explained below:

[40] An example can be found at http://www.securityauditor.net/iso17799/what.htm .

Areas of concern	Explanations
Operational procedures and responsibilities	As far as ISO is concerned, the correct operation of information systems depends largely on properly documented procedures. ISO requires the establishment of detailed operating instructions for the development, maintenance and testing of systems. Following this orientation, the *Code of Practice* asserts that procedures must be defined in order to instruct workers how to react to perilous events (as a hacker attack). [41]
System planning and acceptance	To ensure that systems have adequate capacity and resources, the organization should have planning and acceptance procedures.
Protection against malicious software	ISO recommends a range of countermeasures to detect and prevent malicious software code (viruses, worms, etc.). User training and regular update of anti-virus software are part of these recommendations.
Housekeeping	Housekeeping is the daily maintenance tasks in IT, which for ISO consist of back-up procedures, events logging and monitoring of the equipment environment.
Network management	Network management, according to ISO, intends to provide safe passage of information in transit and protection of networking devices. Several measures are suggested including: - separation of duties between the network and the computer operations (have distinctive workers for these two areas); - definition of procedures for management of remote equipment; - if necessary, special controls to protect the transmission of data over public networks.
Media handling and security	This issue refers to procedures for protecting documents, computer media (tapes, disks, cassettes) printed reports and system documentation from damage, theft and unauthorised access.
Exchange of information and software	The information exchanged between organizations should be protected from loss, modification and misuse. Organizations are urged to (1) assess security implications of electronic data interchange, (2) establish an information exchange agreement between them and (3) apply security controls in electronic mail, e-commerce and other forms of information exchange (electronic office system, voice, facsimile, video, etc.).

Table B.2: Communications and operations management control

B.7.3 Comparisons with other models

Table B.6 (in B.12) illustrates that controls of ISO are also addressed by the other standards studied in this thesis.

[41] This topic addresses operational procedures in response to incidents. Other aspects of incident management, such as, a disciplinary process or the need to report software vulnerabilities, are discussed in B.5.

Similarities among catalogues indicate that network and operation security could be part of a universally accepted controls baseline [Brainthwaite02], formed by the most essential security measures for any organization. As observed in the mentioned Table, COBIT essentially covers the same controls as ISO except the minor aspect of external facilities management (the use of an external contractor to manage IT facilities). NIST Handbook and GMITS tackle the main controls of ISO.

Despite the universality of these safeguards, a particular issue may be difficult to implement [DNV01]: separation of duties may not be appropriate for small organizations. [42]

B.8 ACCESS CONTROL

B.8.1 Background context

Access control is defined as the mechanism that provides the *ability* to perform an action in a computer resource [NIST95]. [43]

The above definition covers the concept of user identification and authentication. [44] Whilst the identification and authentication process authorise users to operate the system or not; access control examines whether users are authorised for the type of action requested.

Access control is considered the core of logical security [Waldon00]. Due to this relevance, several access control models were developed at universities and some have been implemented in commercial products. [45]

B.8.2 ISO requirements

As far as ISO is concerned, access control involves not only identification and authentication mechanisms but also associated issues, such as:

a) the business requirement for access control (access control policy);
b) the user access management (user registration, password management);

[42] The principle of separation of duty calls for the division of roles and responsibilities, so that a single individual cannot subvert a critical process [Pfleeger00].

[43] The NIST handbook distinguishes the term *access* from *authorisation* and *authentication*. For NIST, access is the *ability* to do something with a computer resource. Thus access is a technical ability (for example: read, create, modify, or delete a file, execute a program or use an external connection). Authorisation is the *permission* to use a computer resource. Authentication is proving, to some reasonable degree, that users are who they claim to be [NIST95].

[44] Identification is a method for the system to know who we are (with a username, for example), authentication is a mode to prove to the system that we are really the person we say we are (using a password for instance) [Russell92].

[45] The Bell-La Padula model was implemented by the Honeywell Multics operating system [Russell92], [Pfleeger00]. A current example of an applied access control model is the Extremely Reliable Operating System (EROS) of Jonathan Shapiro (http://www.eros-os.org) that enforces the separation between the authentication and the other access control mechanisms [Karp03]. This separation tends to be neglected in commercial operating systems [Davies89].

c) user responsibilities (how to use the password, what to do when equipment is left unattended);
d) network access control (protection of networked services);
e) operating system access control;
f) application access control;
g) monitoring system access and use (intends to detect unauthorised activities);
h) mobile computing and teleworking.

Consequently, access control defines the rules to access information across several security *entities*, as network resources, operating systems, applications and mobile computing equipment.

A common concern in the *Code of Practice* for these security aspects is the formulation of access control policies. These policies describe the systems, the users and the accessibility conditions of users to particular systems [DNV01], as shown in Table B.3.

Systems **User Groups**	**SystemA**	**SystemB**	**SystemC**
UsersGroup1	Right A	Right A	Rights A, B
UsersGroup2	Rights A, B, C	Right A	Right A
UsersGroup3	Rights A, B	Right A	Rights A, B, C,

Table B.3: An example of access control policy

Lastly, in case of applicability, mobile computing equipment and teleworking professionals are to be subjected to specific security measures.

B.8.3 Comparisons with other models

Applying to investigated standard two conventional access policies taxonomies, it might be said that:

- These catalogues offer organizations the possibility of implementing an access control policy based on a mandatory access control (MAC) or a discretionary access control (DAC) model or Non-Discretionary Access Control (NDAC). [46]
- Standards agree that users must be subjected to an access control system by authorisation [Albuquerque02], which follows the principle to forbid any action requested by the user unless expressly permitted. [47]

[46] Mandatory access control (MAC) means that the owner does not have the ability to grant permissions over the objects he created [Pfleeger00]. In the discretionary access control (DAC), access permissions can be assigned, deleted, altered at the discretion of the object owner. The control is discretionary in the sense that the object owner may determine who has permission to access the object [Sullivan03]. In the Non-Discretionary Access Control, the access is granted based on the role or function of the subject.

[47] According to Albuquerque & Ribeiro [02] access control systems can be classified as authorisation, negation or a combination of both. On an access control system by negation, the user has full rights to all objects, excluding the objects, which the user has been explicitly prohibited to access. Internet is an example of this system; all users have access to all objects, except, if explicitly forbidden. The access control system by authorisation enables the user to have access only to the authorized system. Some systems apply a combination of the two, hence objects have a list authorising some users and another list denying the access to other users [Albuquerque02].

The authorisation for the user to perform a specific type of access on a particular object [NIST95] is granted based on an identification and authentication system. The four safeguard sets share the same concerns about the usage of a unique identifier (user ID) for every user.

They also suggested the combination of several authentication systems (password, tokens, smart cards, etc.) and having a central management of user rights within the organization.

All catalogues employ the terms, *rights* and *privileges*, to express different types of actions that users may perform on systems and data. A user, who has been granted privileges for a specific system, is able to override system or application controls or even take ownership of data. Rights enable the performance of all remaining actions. All standards, except NIST, defend that privileges should be subjected to special safeguards. For example, GMTS suggests a shorter revision period for privileges in comparison with rights.

The term *user* refers as well to applications. In this sense, all applications that need to run with privileges are a potential security hazard, making the system vulnerable to a buffer overflow attack. [48] For instance, in Windows several applications run as Local System, the highest privilege in Windows operating systems. [49]

Convergence principles govern the allocation of rights to users by each paradigm. COBIT and NIST recommend that access to data should be provided on a *need-to-know* basis and following the least privilege principle. [50]

ISO refers only explicitly to the need-to know rule. The general concept of this principle is "as many right as necessary, as few rights as possible" [ISO0b].

Comparisons in Table B.6 (*cf.* B.12) show that:

- The other access control parameters - network, application and mobile computing - are only partially addressed by NIST and GMITS. For COBIT these matters are out of its scope.
- Event logging is addressed by ISO 17799, COBIT and NIST.
- As for cover mobile computing and teleworking, excluding *The Code of Practice,* all other standard do not mention this topic.

[48] Buffer overflow is the most common network attack [Graff03], which consists of overwriting code segments in the stack by feeding the application long strings or other data. Some programming languages (C, especially) encourage programmers to allocate a buffer of fixed length for a character string received from the user. If the attacker manages to overflow the buffer it can run unauthorised commands or actions [Davies89].

[49] An example is the Internet Information Service 4.0. The Microsoft web service needs to have the highest privilege, because, in case the user accessing the WWW service desires to authenticate in the Windows user database, IIS has to be able to start a process or a threat to call Windows user database [Norber01].

[50] Need-to-know principle states that access is provided only to users who need to know a particular data in order to execute their tasks [Pfleeger00]. Least privilege rule is the practice of granting users the fewest rights possible to perform their tasks [NIST95] [Norberg01].

B.9 SYSTEMS DEVELOPMENT AND MAINTENANCE

B.9.1 Background context

As most organizations are departing from the in-house system development model, the applicability of this domain could be thought of as modest [DNV01]. However, ISO does not restrict this section to system development process only. All security requirements for the development process that might be appropriate can also be used to evaluate the purchase of software packages.

The *Code of Practice* comprises a group of controls of the several phases in a system's life cycle (design, development, implementation, support and disposal).

Nevertheless, ISO cannot be regard as security standard for system development. More appropriate schemes that enable a security classification of the system or of processes followed in development are: (1) ISO 15408 - *The Common Criteria for Information Technology Security Evaluation* [51] and (2) Systems Security Engineering Capability Maturity Model (SSE-CMM). [52]

B.9.2 ISO requirements

ISO controls concerning system development and maintenance can be abridged in the following way:

Areas of concern	Recommended measures
System development projects or evaluation of third party systems	Security requirements must be included within the analysis and specification phase of a system. Or in the evaluation of a third party system.
Data which is input, processed and output from application systems	Validate the input and output data, the internal processing and verify the integrity of messages between applications.
Information which is considered at risk	Organization may have a defined policy on the use of encryption, digital signatures, digital certificates and protection of cryptographic keys.
System files	Access control to program source libraries, system test data and verification of the implementation of systems in a production environment.
Software	Organizations must maintain a strict change management process (in order to control implementations of changes), restrict alterations on software packages, control outsourced development and check against covert channels and Trojan code.

Table B.4: System development and maintenance controls

[51] Common Criteria is a set of criteria which enables the specification of the security of an application, based on the characteristics of the development environment. ISO 15408 also defines the means to ensure assurance for the software customer [Albuquerque02].

[52] Systems Security Engineering Capability Maturity Model (SSE-CMM), developed initially at the Software Engineering Institute, describes the essential characteristics of a security engineering process that involves the life cycle of an entire system (development, operation, maintenance, and decommissioning activities) and related activities, such as acquisition and accreditation.

B.9.3 Comparisons with other models

Controls concerning system development and maintenance can be organised in two categories [Albuquerque02], [NIST95]: (1) controls related to the system life cycle (involving development or acquisition, implementation, maintenance and disposal) and (2) security mechanisms of applications.

In terms of system life cycle measures, Figure B.3 revels that:

- ISO, NIST and COBIT concur that security requirements should be integrated in the analysis and specification phases (ISO adds also this concern to the evaluation phase, prior to the acquisition of a system).
- Implementation is only tackled by the *Code of Practice* and COBIT.
- Maintenance is common to the four standards.[53]
- Disposal is covered by ISO, NIST and COBIT. ISO establishes that systems that hold private information should be subject to the complete erase of residual information - *cf.* section B.6.3.

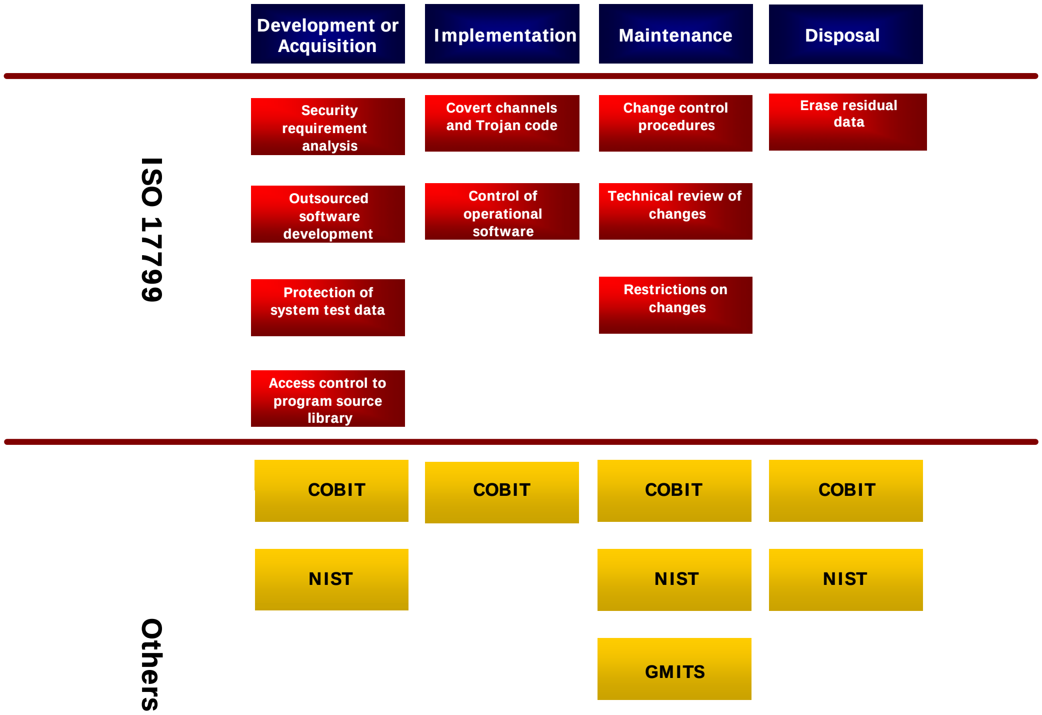

Development or Acquisition
Implementation
Maintenance
Disposal
ISO 17799
Security requirement analysis
Covert channels and Trojan code
Change control procedures
Erase residual data
Outsourced software development
Control of operational software
Technical review of changes
Protection of system test data
Restrictions on changes
Access control to program source library
Others
COBIT
COBIT
COBIT
COBIT
NIST
NIST
NIST
GMITS

Figure B.3: Controls related to the system life cycle

[53] An important aspect of maintenance is configuration management. ISO advises organizations to define procedures to implement changes in running platforms. This procedure might take into account the operational readiness, stability of the system [Graff03], as well as security concerns.

As far as controls integrated on applications are concerned, ISO recommends:

a) Protection of information considered at risk by means of encryption, message authentication and digital signature.
b) Prevention of loss, modification or misuse of data in applications, regarding all data as untrustworthy. This implies validation of all input variables, verifying whether the variable is out-of- range or has invalid characters.

As shown in Table B.6 (*cf*. B.12), cryptographic controls are addressed also by GMITS, NIST and COBIT. Validation of data is only discussed by COBIT, besides ISO itself. As explained (*cf*. 4.3.c), COBIT includes a group of indicators to gauge controls.

B.10 BUSINESS CONTINUITY MANAGEMENT

B.10.1 Background context

In spite of all controls, some security disasters are impossible to prevent or avoid [Trivedi03]. In such events the only managerial attitude is to try to minimise the negative effects of them. Business continuity seeks survivable mechanisms capable of maintaining the essential business processes after a major incident (e.g. earthquake) affected information systems [Silva04].

B.10.2 ISO requirements

ISO urges organizations to design, implement and periodically test a Business Continuity (BC) process. ISO advocates the following sequence of phases in this process:

a) Identification of the critical organizational processes and their related risks, capable of causing an interruption in the business operation.
b) Analysis of probability and impact (the impact of interruption should be measured in terms of a damage scale and recovery period).
c) Formulate a business continuity strategy consistent with the agreed business objectives and priorities.
d) Development of business continuity plans (ISO specifies the structure of these documents).
e) Implementation (involves necessary procedures to activate the plan, in case of incident, for example training on emergency procedures).
f) Testing and updating the plans (as a continuous process, BC has to be re-assessed whenever circumstances change).

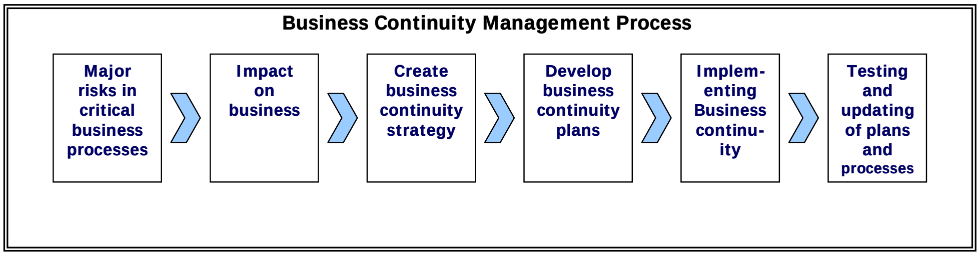

Business Continuity Management Process
Major risks in critical business processes
Impact on business
Create business continuity strategy
Develop business continuity plans
Implem-enting Business continu-ity
Testing and updating of plans and processes

Figure B.4: Business Continuity process according to ISO

Business Continuity plans should addressed these issues:

Areas of concern	Recommended measures
Conditions for activating the plans	Process to be followed before each plan is activated (how to assess the situation, who is to be involved, etc.).
Emergency procedures	Actions to be taken following an incident which jeopardises business operations (i.e. arrangements for public relations management and for effective liaison with appropriate public authorities, as police).
Fallback procedures	Actions to be taken to move essential business activities to alternative temporary locations and to bring business processes back into operation in the required time-scales.
Resumption procedures	Actions to be taken to return to normal business operations.
Maintenance schedule	Specifies how and when the plan will be tested, and the process for maintaining the plan.
Responsibilities of individuals	Who is responsible for executing which component of the plan (alternatives should be nominated as required).

Table B.5: Business Continuity controls

B.10.3 Comparisons with other models

The four Business Continuity (BC) models are presented in chronological order.

NIST, published in 1995, supports a sequence of six phases to ensure the continuity of mission or business critical functions, as seen in Table B.6 (in section B.12). [54] GMITS, released in 2000, maintains the same process model, assembling the four initial steps in the Business Continuity Strategy phase. COBIT and ISO, both published in 2000, share common concerns about BC.

For these set of safeguards, BC has to be supported in an organizational framework, which involves issues such as definition of roles, establishment of approval procedures of business continuity plans, the acceptance of risk methodology, etc.

As an ongoing activity, BC for ISO and COBIT is a responsibility for the whole management structure. Every manager accountable for a critical asset or process has to ensure its continuity in case of disaster.

[54] As seen, NIST *Computer Security Handbook* [NIST95] was primarily designed for public institutions in the US. The term *mission* is applied to the objective of public institution.

The difference between the two catalogues derives from their distinctive objectives. Due to its management focus, COBIT regards the IT continuity plan as part of the overall business continuity strategy.

Although, ISO is also concerned about critical business processes, it is more focused on protection of information assets. For COBIT, BC involves tasks not related to security, as for example communicating with stakeholders, key customers, critical suppliers or stockholders.

B.11 COMPLIANCE

B.11.1 Background context

The last ISO domain is about auditing. The *Code of Practice* establishes what to audit (the auditing object) and raises some methodological caveats for the auditing process. Due to the necessity of regular audits, ISO advises organizations to establish auditing procedures that pose a minimal disruption to the normal business operation.

B.11.2 ISO requirements

Compliance has to be verified with respect to two dimensions: (1) legal requirements and (2) implementation of security policies. Both of these compliance requirements have to be assessed through the regulations, procedures and systems of an organization, as illustrated in Figure B.5.

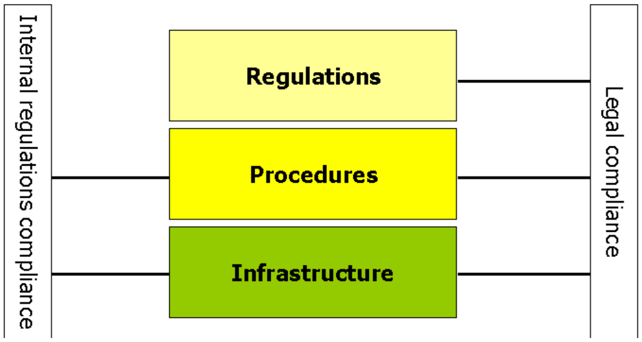


Figure B.5: Compliance issues associated with organizational aspects

The observance of legal impositions by the organization is evaluated in terms of normative statements (regulations), activities performed by workers and management (procedures), and system configuration (infrastructure), as seen in Figure B.5.

The implementation of security regulations (defined internally) is audited at the levels of infrastructure and procedures. Actual actions of workers (procedures) are compared against the security rules of the organization (security policies), with the purpose of assessing whether procedures are complied with or not.

The infrastructure's compliance with internal security rules assesses how effectively IT systems follow security policies and technical standards. [55]

Legal compliance is checked through the analysis of laws and regulations applicable to the organization. ISO enumerates a number of concerns for this analysis:

a) Identification of applicable legislation and regulations for each information system.
b) Compliance with software copyright and other intellectual property rights.
c) Safeguard of organizational records (it is recommended specific controls for storage and handling of relevant organizational records).
d) Privacy protection (in countries with privacy protection laws, as Portugal, a data protection officer could be appointed to oversee law enforcement).
e) Prevention of computer misuse (ISO provides guidelines to enforce legislation to protect against computer misuse).
f) Regulation of cryptographic controls (in case it is required by law or regulation, specific controls can be applied).
g) Collection of evidence of a security incident (ISO offers recommendations in the field of computer forensic). [56]

Concerning the last point above, *evidence of a security breach*, intends to ensure that an information system complies with the requirements applicable to the "production of admissible evidence" [ISO00a:p.63]. Hence, to achieve quality and completeness of the evidence [ISO00a], a strong evidence trail is required.

The conformity of the actual actions of workers in relation to security policies should be demonstrated by regular audits. Those audits ought to cover all areas within the organization and include these items: (1) information systems, (2) systems providers, (3) owners of information and information assets, (4) users and (5) management.

In the matter of technical compliance, ISO stipulates regular reviews that might involve manual examination, the use of automated tools and penetration tests (*c.f.* 3.5.2).

Lastly, ISO offers recommendations for the auditing process. With the aim of minimising interference in business caused by auditing, auditors must (1) carefully plan their operations and (2) have a limited access to production systems.

B.11.3 Comparisons with other models

As formerly perceived, ISO outlines compliance requirements involving several levels of an organization's security: regulations, procedures and systems.

[55] As discussed (*cf.* section B.2.3), policies define general requirements for systems, whereas standards establish specific technical requirements. For instance, the technical compliance of a firewall system could be evaluated based on an Access Control Policy and a technical standard. The policy establishes the need for a network control mechanism, and the technical standard describes how a firewall has to apply access control rules, how it should be updated, etc.

[56] Computer forensics is the identification, extraction, preservation and interpretation of computer data relevant to computer crime investigations [Carrier03].

Two conformity requirements are addressed: (1) compliance with legal impositions and (2) compliance of procedures and systems with security regulations.

GMITS, NIST, and COBIT also share concerns about compliance with legal requirements, security policies and technical standards.

As far as COBIT is concerned, compliance has a particular importance, as it is one of the seven information criteria [ISACA00]. This means that one of the attributes of the information delivered for business processes is to be compliant with laws, regulations and contractual arrangements. [57]

Auditing recommendations in COBIT are in some extend distinct from ISO. The *Code of Practice* suggests precautions to minimise the impact of auditing work, similar to the auditing recommendations of ISO 9000 [DNV01].

COBIT, on the other hand, gives specific recommendations to arrange and manage independent auditors and provides guidance to audit each management process. [58]

In conclusion, COBIT sifts through the same areas of concerns, as ISO, i.e. legal, security policies, technical compliance and auditing precautions. The other standards do not explicitly address auditing as a compliance mechanism.

COBIT has a broader understanding of what compliance is. The auditor's standard which positions compliance at the same level as confidentiality is one of the seven information criteria.

The *Code of Practice* is more specific about legal requirements and computer forensics than any other. On the other hand, COBIT is the framework that provides more specific auditing recommendations.

B.12 SUMMARY

The comparison between the catalogues is summarised in Table B.6. This chart compares the 127 controls practices of ISO, with the 318 measures of COBIT, with the 60 controls of GMITS, and with the 61 mechanisms of NIST.

In this table, fields with pale blue mean that the issue was not addressed by the catalogue. When two or more issues of ISO are covered by the same objective of another catalogues a label "repeat" is shown.

This chart is analysed in section 4.3.3 and 4.4 of the dissertation text.

[57] The compliance objective is sustained by several processes in COBIT: (1) Ensure compliance with external requirements (law, etc.); (2) Communicate management aims and direction (verifying whether personnel understands policies); (3) Obtain independent assurance (through certification and accreditation of the organization); (4) Provide for independent audit (external audit to assess compliance).

[58] COBIT proposes specific auditing procedures for each one of its 34 management processes. COBIT suggests assessment criteria, methods and practical approaches to perform the assessment of process. COBIT is, therefore, a true toolkit for auditing (*cf*. section 4.2.2).

ISO 17799	GMITS	NIST Handbook	COBIT
3. Security Policy			
3.1 INFORMATION SECURITY POLICY	8.1.1.1 Corporate IT security policy	5.1 Program policy	PO2 Define the information architecture
3.1.1 Information security policy document			
3.1.2 Review and evaluation			PO6 Communicate management aims and direction
4. Security Organization			
4.1 INFORMATION SECURITY INFRASTRUCTURE	8.1.1.3 IT security management	6. Computer security program management	PO4 Define the information technology organization and relationships
4.1.1 Management information security forum			
4.1.2 Information security co-ordination			
4.1.3 Allocation of information security responsibilities	8.1.1.4 I Allocation of responsibilities	3. Roles and responsibilities	
4.1.4 Authorization process for information processing facilities			DS12 Manage facilities
4.1.5 Specialist information security advice			PO8 Ensure compliance with external requirements
4.1.6 Co-operation between organizations			
4.1.7 Independent review of information security			M3 Obtain independent assurance
4.2 SECURITY OF THIRD PARTY ACCESS		10.3 Contractor access considerations	DS2 Manage third-party services
4.2.1 Identification of risks from third party access			
4.2.2 Security requirements in third party contracts			
4.3 OUTSOURCING			
4.3.1 Security requirements in outsourcing contracts			
5. Asset Classification and Control			
5.1 ACCOUNTABILITY FOR ASSETS	8.1.1.6 Assets identification and valuation	7.1 Risk assessment (asset identification and valuation)	DS5 Ensure systems security
5.1.1 Inventory of assets			
5.2 INFORMATION CLASSIFICATION			PO2 Define the information architecture
5.2.1 Classification guidelines			
5.2.2 Information labelling and handling			
6. Personnel Security			
6.1 SECURITY IN JOB DEFINITION AND RESOURCING	8.1.4.1 Safeguards for permanent and temporary staff	10 Personnel/user issues	
6.1.1 Including security in job responsibilities			PO4 Define the information technology organization and relationships
6.1.2 Personnel screening and policy			
6.1.3 Confidentiality agreements			
6.1.4 Terms and conditions of employment			PO7 Manage human resources
6.2 USER TRAINING	8.1.4.3 Security awareness and training	13 Awareness, training and education	PO6 Communicate management aims and direction
6.2.1 Information security education and training			
6.3 RESPONDING TO SECURITY INCIDENTS AND MALFUNCTIONS		12. 2 Characteristics of a successful incident handling capability	DS5 Ensure systems security
6.3.1 Reporting security incidents	8.1.3.1 Reporting security incidents		
6.3.2 Reporting security weaknesses	8.1.3.2 Reporting security weakness		
6.3.3 Reporting software malfunctions	8.1.3.3 Reporting security malfunctions		
6.3.4 Learning from incidents			
6.3.5 Disciplinary process	8.1.4.4 Disciplinary process	5.1.1 Basic components of program policy	
7. Physical and Environmental Security			
7.1 SECURE AREAS	8.1.7.1 Material protection	15.1 Physical access controls (repeated)	DS12 Manage facilities
	8.1.7.5 Protection against theft	15.1 Physical access controls (repeated)	
7.1.1 Physical security perimeter			
7.1.2 Physical entry controls			
7.1.3 Securing offices, rooms and facilities			
7.1.4 Working in secure areas			
7.1.5 Isolated delivery and loading areas			
7.2 EQUIPMENT SECURITY			
7.2.1 Equipment sitting and protection	8.1.7.2 Fire protection	15.2 Fire safety factors	DS12 Manage facilities
	8.1.7.3 Water/liquid Protection	15.5 Plumbing leaks	
	8.1.7.4 Natural Disaster Protection	15.4 Structural collapse	
7.2.2 Power supplies	8.1.7.6 Power and air-conditioning		
7.2.3 Cabling security	8.1.7.7 Cabling		
7.2.4 Equipment maintenance	8.15.4 Maintenance		DS11 Manage data
7.2.5 Security of equipment off-premises			

7.2.6 Secure disposal or re-use of equipment		8.4.5 Disposal	DS11 Manage data
7.3 GENERAL CONTROLS			
7.3.1 Clear desk and clear screen policy			
7.3.2 Removal of property	8.2.3.3 Removable media circulation control		

8. Communications and Operations Management

8.1 OPERATIONAL PROCEDURES AND RESPONSIBILITIES			M2 Assess internal control adequacy
8.1.1 Documented operating procedures	8.1.5.3 Documentation (repeated)	14.6 Documentation (repeated)	
8.1.2 Operational change control			
8.1.3 Incident management procedures	8.1.3.4 Incident management		
8.1.4 Segregation of duties	8.1.5.10 Segregation of duties		PO4 Define the information technology organization and relationships
8.1.5 Separation of development and operational facilities			PO10 Manage projects
8.1.6 External facilities management			
8.2 SYSTEM PLANNING AND ACCEPTANCE	8.1.5.1 Configuration and Change Management	14.3 Configuration management	DS3 Manage performance and capacity
8.2.1 Capacity planning	8.1.5.2 Capacity Management		
8.2.2 System acceptance			
8.3 PROTECTION AGAINST MALICIOUS SOFTWARE	8.2.3 Protection against malicious code		DS5 Ensure systems security
8.3.1 Controls against malicious software			
8.4 HOUSEKEEPING	8.1.5.6. Audit trails and Logging	18. Audit trails and logs	
8.4.1 Information back -up	8.1.6.4 Back-ups		DS4 Ensure continuous service
8.4.2 Operator logs			DS5 Ensure systems security
8.4.3 Fault logging			
8.5 NETWORK MANAGEMENT			PO4 Define the information technology organization and relationships
8.5.1 Network controls	8.2.4.1 Operational procedures		
8.6 MEDIA HANDLING AND SECURITY	8. Media controls	14.5 Media controls	DS11 Manage data
8.6.1 Management of removable computer media			
8.6.2 Disposal of media			
8.6.3 Information handling procedures	8.1.5.3 Documentation (repeated)	14.6 Documentation (repeated)	
8.6.4 Security of system documentation			PO6 Communicate management aims and direction
8.7 EXCHANGES OF INFORMAT ION AND SOFTWARE			DS5 Ensure systems security
8.7.1 Information and software exchange agreements			
8.7.2 Security of media in transit			
8.7.3 Electronic commerce security			
8.7.4 Security of electronic mail			
8.7.5 Security of electronic office systems			
8.7.6 Publicly available systems			
8.7.7 Other forms of information exchange			

9. Access Control

9.1 BUSINESS REQUIREMENT FOR ACCESS CONTROL	8.2.2.1 Access control policy	17. Logical access control (repeated)	DS5 Ensure systems security
9.1.1 Access control policy			
9.2 USER ACCESS MANAGEMENT	8.2.2.2 User access to computers		
9.2.1 User registration			
9.2.2 Privilege management			
9.2.3 User password management			
9.2.4 Review of user access rights	8.2.2.4 Review and updating access rights		
9.3 USER RESPONSIBILITIES		10. Personnel/user issues	
9.3.1 Password use			
9.3.2 Unattended user equipment			
9.4 NETWORK ACCESS CONTROL	8.2.2.3 User access to data, services and applications (repeated)	17. Logical access control (repeated)	
9.4.1 Policy on use of network services			
9.4.2 Enforced path			
9.4.3 User authentication for external connections			
9.4.4 Node authentication			
9.4.5 Remote diagnostic port protection			
9.4.6 Segregation in networks	8.2.4 Network segregation		
9.4.7 Network connection control			
9.4.8 Network routing control			
9.4.9 Security of network services			
9.5 OPERATING SYSTEM ACCESS CONTROL			
9.5.1 Automatic terminal identification			
9.5.2 Terminal log-on procedures			

9.5.3 User identification and authentication	8.2.1 Identification and authentication	16. Identification and authentication	
9.5.4 Password management system			
9.5.5 Use of system utilities			
9.5.6 Duress alarm to safeguard users			
9.5.7 Terminal time-out			
9.5.8 Limitation of connection time			
9.6 APPLICATION ACCESS CONTROL	8.2.2.3 User access to data, services and applications (repeated)	17. Logical Access control (repeated)	
9.6.1 Information access restriction			
9.6.2 Sensitive system isolation			
9.7 MONITORING SYSTEM ACCESS AND USE	8.2.2.5 Audits logs	18. Audit trails	
9.7.1 Event logging			DS13 Manage operations
9.7.2 Monitoring system use			
9.7.3 Clock synchronization			
9.8 MOBILE COMPUTING AND TELEWORKING			
9.8.1 Mobile computing			
9.8.2 Teleworking			

10. System Development and Maintenance

10.1 SECURITY REQUIREMENTS OF SYSTEMS			
10.1.1 Security requirements analysis and specification		8.4.2.1 Determining security requirements	DS5 Ensure systems security
10.2 SECURITY IN APPLICATION SYSTEMS			DS11 Manage data
10.2.1 Input data validation			
10.2.2 Control of internal processing			
10.2.3 Message authentication			DS5 Ensure systems security
10.2.4 Output data validation			DS11 Manage data
10.3 CRYPTOGRAPHIC CONTROLS		19.2 Uses of cryptography	DS5 Ensure systems security
10.3.1 Policy on the use of cryptographic controls			
10.3.2 Encryption	8.2.5.1 Data confidentiality protection		
10.3.3 Digital signature	8.2.5.2 Data integrity protection		
10.3.4 Non-repudiation services	8.2.5.4 No-repudiation		DS11 Manage data
10.3.5 Key management	8.2.5.5 Key management		DS5 Ensure systems security
10.4 SECURITY OF SYSTEM FILES			DS9 Manage the configuration
10.4.1 Control of operational software			DS5 Ensure systems security
10.4.2 Protection of system test data			DS11 Manage data
10.4.3 Access control to program source library			DS9 Manage the configuration
10.5 SECURITY IN DEVELOPMENT AND SUPPORT PROCESSES			
10.5.1 Change control procedures	8.1.5.12 Software change control	8.4.4.3 Managing change	AI6 Manage changes
10.5.2 Technical review of operating system changes			
10.5.3 Restrictions on changes to software packages	8.1.5.12 Software change control		
10.5.4 Covert channels and Trojan code			DS5 Ensure systems security
10.5.5 Outsourced software development			

11. Business Continuity Planning

11.1 ASPECTS OF BUSINESS CONTINUITY MANAGEMENT	8.1.6.1 Business continuity strategy	11.1 Identifying the mission- or business-critical functions.	DS4 Ensure continuous service
11.1.1 Business continuity management process		11.2 Identifying the resources that support critical Functions	
11.1.2 Business continuity and impact analysis		11.3 Anticipating potential contingencies or disasters 11.4 Selecting contingency planning strategies	
11.1.3 Writing and implementing continuity plans	8.1.6.2 Business continuity plan	11.5 Implementing the contingency strategies	
11.1.4 Business continuity planning framework			
11.1.5 Testing the plans and maintaining and re-assessing business continuity plans	8.1.6.3 Testing and updating the business continuity plans	11.6 Testing and revising	

12. Compliance

12.1 COMPLIANCE WITH LEGAL REQUIREMENTS	8.1.2.2 Compliance with legal and regulatory requirements	6.3 Elements of an effective central computer security program	PO8 - Ensure compliance with external requirements
12.1.1 Identification of applicable legislation			
12.1.2 Intellectual property rights (IPR)	8.1.5.11 Correct software use		
12.1.3 Safeguarding of organizational records			
12.1.4 Data protection and privacy of personal information			
12.1.5 Prevention of misuse of information processing facilities			
12.1.6 Regulation of cryptographic controls			
12.1.7 Collection of evidence			
12.2 REVIEWS OF SECURITY P OLICY AND	8.1.2.1 Compliance with IT security	10.2.2 Audit and management	PO6 Communicate management aims and

TECHNICAL COMPLIANCE	policies and safeguards	reviews	direction
12.2.1 Compliance with security policy			
12.2.2 Technical compliance checking			
12.3 SYSTEM AUDIT CONSIDERATIONS			M3 - Obtain independent assurance M4 - Provide for independent audit
12.3.1 System audit controls			
12.3.2 Protection of system audit tools			

Table B.6: Comparison of ISO control with other catalogues

ANNEX C

CASE-STUDY:
INFORMATION SECURITY MANAGEMENT
IMPLEMENTATION REPORT

Annex C

Case-Study:
Information Security Management Implementation Report

Associação para o Desenvolvimento das Telecomunicações e Técnicas de Informática

Lisboa, 23rd of June 2004

Paulo Coelho

Version Control

Version	Author	Reason	Date
01	Paulo Coelho	Initial document version	10/05/2004
02	Paulo Coelho	General revision	03/06/2004
1.0	Paulo Coelho	Modification of Introduction; Update of Table of contents;	23/06/2004

Distribution List

Date	Version	Name
<23/06/04>	<1.0>	Not applicable

Table of Contents

0. Introduction

The present document "**Information Security Management Implementation Report**" compiles the deliverables of the implementation methodology of an Information Security Management System (ISMS), which was developed and tested in ADETTI.

0.1 Definitions, acronyms and abbreviations

ADETTI	Associação para o Desenvolvimento das Telecomunicações e Técnicas de Informática
Ad room	Administrative room
ADU	Administrative Unit
Availability	Ensuring that authorized users have access to information and associated assets when required [ISO/IEC 17799:2000]
AUM	Administrative Unit Manager
AUE1	Administrative Unit Employee 1
AUE2	Administrative Unit Employee 2
AV	Asset Value
Cache remote poisoning	This sort of attack enables the redirecting of internal consults of legitimate addresses to bogus servers, already prepared to obtain information from visitors.
Confidentiality	Ensuring that information is accessible only to those authorized to have access [ISO/IEC 17799:2000]
Continual improvement	Recurring process of enhancing the security management system.
Corrective Action	Action to eliminate the cause of a detected nonconformity or other undesirable situation.
DoS	Denial of service
DHCP	Dynamic Host Configuration Protocol
Information security	Preservation of confidentiality, integrity and availability of I information
ISCTE	Instituto Superior de Ciências do Trabalho e da Empresa
ISMS	That part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security NOTE The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.

Integrity
Safeguarding the accuracy and completeness of information and processing methods [BS ISO/IEC 17799:2000].

IV
Impact Value

NA
Not applicable

Multi lab
Multimedia Lab

MTBF
Mean time between failure is the average expected interval between failures of a product in steady state, after the infant mortality and before the wear-out periods of its life [Cisco04].

Preventive Action
Action to eliminate the cause of a potential nonconformity or other undesirable potential situation.

PV
Probability Value

Process
Set of interrelated or interacting activities which transforms inputs into outputs.

PDCA
Plan, Do, Check, Act

Risk acceptance
Decision to accept a risk [ISO Guide 73]

Risk analysis
Systematic use of information to identify sources and to estimate the risk [ISO Guide 73]

Risk assessment
Overall process of risk analysis and risk evaluation [ISO Guide 73]

Risk evaluation
Process of comparing the estimated risk against given risk criteria to determine the significance of risk [ISO Guide 73]

Risk management
Coordinated activities to direct and control an organization with regard to risk [ISO Guide 73]

Risk treatment
Treatment process of selection and implementation of measures to modify risk [ISO Guide 73]

Security Plan
Documents specifying which procedures and associated resources shall be applied by whom and when.

SM
Security Management

Statement of applicability
Document describing the control objectives and controls that are relevant and applicable to the organization's ISMS, based on the results and conclusions of the risk assessment and risk treatment processes

S. Forum
Security forum

S. Officer
Security Officer

1. Project management definition

1.1 Requirements

Inputs		Practices and techniques	Outputs
T01.1	• Manager representative with capacity to approve the project decisions • Participation of future members of security management (SM) structures • After ISMS scope selection, representatives from the selected areas may be included	• Definition of the project management model (role and participants in the project management) • Briefing of project members regarding the methodology which will be followed	• Project management model: - steering committee (with upper management and user representatives); - implementation advisor (project manager). • Project team trained (team may be changed after scope selection)

1.2 Project management model and team (T01.1)

The project's steering committee was formed by the president of ADETTI, by a user representative and by the author who assumed the role of implementation advisor, as shown in the next table.

Steering Committee Structure			
Code	Description	Role	Name
MR	Management Representative	Supervision of the project	Miguel Dias
PA	Project Advisor	Project responsible	Paulo Coelho
UR	User Representative	Representative of the area under evaluation	Fátima Estevens*

* - After the first meetings was represented by Management Representative.

This committee supervised the conductance of the project and approved the deliverables of all the phases of the project. In the project beginning, the President of ADETTI was informed about overall implementation methodology and consequences of a security management system in an organization.

2. Evaluation scope definition

2.1 Requirements

Inputs		Practices and techniques	Outputs
T02.1	• Business objectives towards Security Management (SM) • Project constraints (time, resource and money)	• Define criteria for the selection of the evaluation arena within the organization	• Decision criteria for scope selection
T02.2	• Decision criteria for scope selection (from T02.1) • Perception of information types and related processes within the organization	• Process description • Process flowchart diagram • Information flow diagram • Organizational chart • Physical and network diagram	• Evaluation sphere definition
T02.3	• Evaluation sphere within the organization (from T02.2)	• Context diagram • Interfaces and dependencies list	• Interfaces and dependencies of the ISMS with other parts of the organization and other entities (as supplies and partners)

2.2 Decision criteria for scope selection (T02.1)

The steering committee decided that, although a security management framework in ADETTI would be relevant in the long run, this project – conducted by academic reasons by the author – should had a minimum impact in the normal activities of the organization.

From this principle, the Steering Committee composed the following guidelines:

- the project's scope should be confined to a restricted area, preferably in the administrative unit, and not in the research units, which have stringent time restrictions;
- the project should strive to engage the minimum human resources, occupying it the minimum time.

2.3 Evaluation sphere definition (T02.2)

The definition process of the area of ADETTI, which would be subjected to security evaluation, is illustrated in Figure R.1.

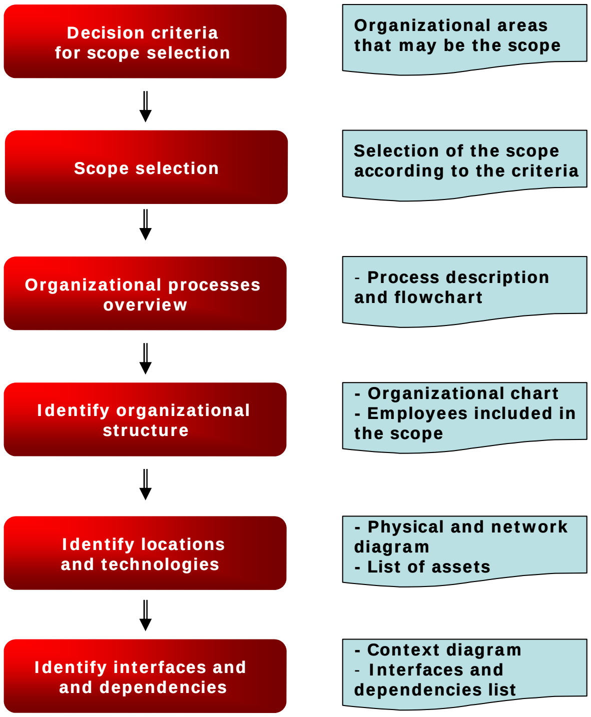

Decision criteria for scope selection
Organizational areas that may be the scope
Scope selection
Selection of the scope according to the criteria
Organizational processes overview
- Process description and flowchart
Identify organizational structure
- Organizational chart
- Employees included in the scope
Identify locations and technologies
- Physical and network diagram
- List of assets
Identify interfaces and and dependencies
- Context diagram
- Interfaces and dependencies list

Figure R.1: Scope definition activities

2.3.1 Scope selection (application of the criteria of T02.1)

As a result of the criteria adopted in T02.1, the Steering Committee decided that the evaluation area would be restricted to the Administrative Unit (AD).

The Steering Committee identified that a critical issue, within this area, was the activities related to the project's financial report. Some difficulties were encountered in the process of compiling the financial data and submitting the financial statement of projects.

Therefore, the scope was identified as the financial data pertained to the financial report of projects and the associated process of colleting, composing, delivering and storing that type of information.

It was decided to analyse the process to collect financial documents and produce the project's final financial report from a point of view of the ADU. For simplicity reasons, it was conceived a process of financial reporting without other research partners.

2.3.2 Process description

The activities related to the financial reporting data were identified based on a series of interviews with the ADU personnel. The data collected was then organized in a group of categories and a flowchart diagram, following the advocated techniques of Clements [96].

Process objective:
Preparation, delivery and storage of the financial data of final report of the research projects.

Information protected:
Financial data

Entities involved:
- Administrative unit – verifies the correction of financial data and prepares the final report;
- Accountant – audits the Expense Statement (financial report);
- Project leaders – collects financial data.
- Other organization areas

Physical locations:
Administrative room

Process owner:
AUM – Administrative Unit Manager

Process flow descriptions:
1 - The project leader sends all invoices and expenses statements to the ADUE01.

2 - AUE1 collects and stores this documentation in the respective folder, which is stored in the project file cabinet.

3 - The Ad Unit manager (ADM) verifies if the financial documentation is colleted and properly signed by a project responsible. This verification intends to checks if the collected documents are consistent with the financial budget of the project and with the requirements of the funding institution. If a document is missing or is not signed the ADM asks by e-mail to the project leader, who then hands out the missing document or goes to the AD office to sign the document.

4 - The Ad Unit manager (ADM) prepares the final financial report, which is placed at the BSCW server at the project's folder, with restrict access to the project leader, research line leader and members of the Administrative Unit. Once the report is finished, the report and the supporting documents are send to the accountant who audits the data in the report. This transportation is done by courier or by hand (an employee from the accountant office goes to ADU office). Copies of all documents, which are sent to the accountant, are maintained at the project folder.

5 - The Accountant sends the audited report to Ad Unit manager (ADM) through courier.

6 - The ADU finishes the report and then sends an email to the project leader notifying him that the financial report is ready for approval.

7 – The project leader approves the financial report and then informs by email the ADU.

8 – The ADU submits the financial report to the funding organization, employing a courier, registered letter or in even some cases by fax.

9 – A notification of reception is signed by the funding organization.

10 – The ADU stores the financial report in BSCW and the project file cabinet, closed by lock.

Critical resources for this process:
- Ad unit manager;
- Ad unit manager desktop with spreadsheet (Microsoft Excel 2003), mail client (Microsoft Outlook 2003) - [identified in 2.3.5.2.c];
- Mail server [identified in 2.3.5.2.c];
- BSCW server [identified in 2.3.5.2.c] ;
- Data communication infrastructure [identified in 2.3.5.2.c] ;
- Electrical power;
- Office material;
- Facilities.

Frequency:
The projects tend to end at the same time, twice a year (especially in June and February).

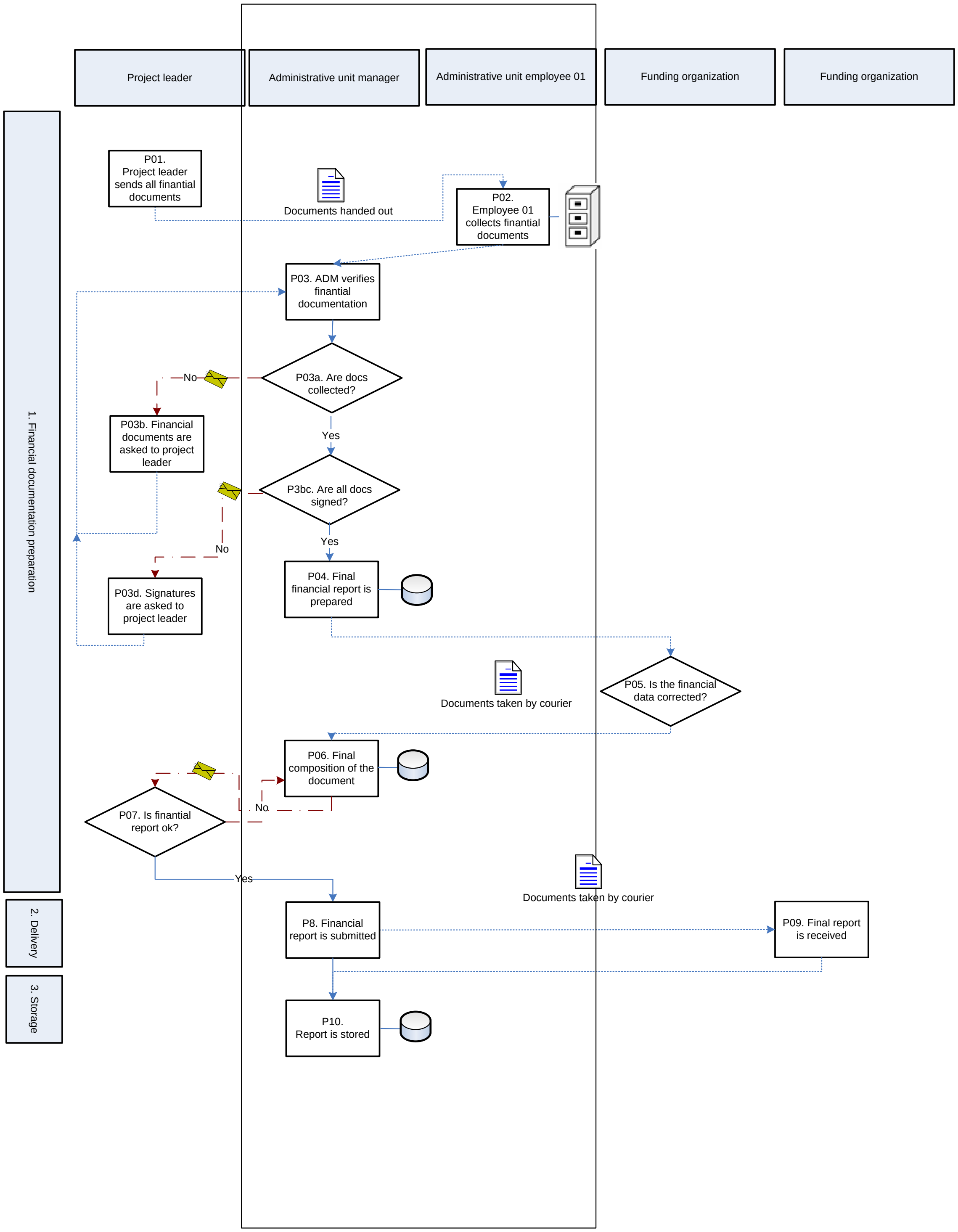

Project leader
Administrative unit manager
Administrative unit employee 01
Funding organization
Funding organization
1. Financial documentation preparation
2. Delivery
3. Storage
P01. Project leader sends all finantial documents
Documents handed out
P02. Employee 01 collects finantial documents
P03. ADM verifies finantial documentation
P03a. Are docs collected?
No
Yes
P03b. Financial documents are asked to project leader
P3bc. Are all docs signed?
No
Yes
P03d. Signatures are asked to project leader
P04. Final financial report is prepared
Documents taken by courier
P05. Is the financial data corrected?
P06. Final composition of the document
No
P07. Is finantial report ok?
Yes
Documents taken by courier
P8. Financial report is submitted
P09. Final report is received
P10. Report is stored

Figure R.2: Scope flow chart diagram

2.3.4 Organizational structure

ADETTI is an association organized into the following structures: General Assembly (GA), Executive Commission (EC), Council of Auditors (CA) and Advice Council (AC).

The GA is formed by all the associates with full rights. The EC is formed by a President and two vice presidents. The President is responsible to coordinate the overall activities of the Association. To the EC is trusted the conductance of all appropriate managerial tasks. The CA is formed by three members elected from the associates. The AC is formed by the President of the EC, projects coordinators and other internal or external members without right to vote. The election of these structures is done by secret vote.

Managerial structure
General Assembly
President: Prof. António Almeida
Vice-President: Prof. Pedro F. Lopes
Secretary: Eng. Manuel Gamito

Executive Commission
President: Prof. Miguel Dias
Vice-President: Prof. Paulo Rita
Vice-President: Dr. Carlos Serrão

Council of Auditors
President: Prof. Henrique O'Neill
Vice-President: Prof. Mário Romão
Vice-President: Eng. João B. Regueira

Research and development activities in ADETTI are organized in six areas: (1) Multimedia and Virtual Environments, (2) Networking and Information Security, (3) Technologies for Business Processes, (4) Intelligent and Integrated Communication Systems, (5) Management and Strategy and (6) "We, the Body and the Mind".

The first research area, Multimedia and Virtual Environments, focuses on 3D computer graphics and virtual reality. Networking and Information Security area addresses computer network and security, especially secure access to multimedia information. Technologies for Business Processes studies advanced information technologies infrastructures that attain the requirements modern management methodologies. The fourth area, Intelligent and Integrated Communication, is focused on the development of new Artificial Intelligent techniques. Management and Strategy tackles industrial economics, ecology and strategic management. The "We, the Body and the Mind" area researches methods for human-computer interaction.

The above structure is illustrated in Figure R.3.

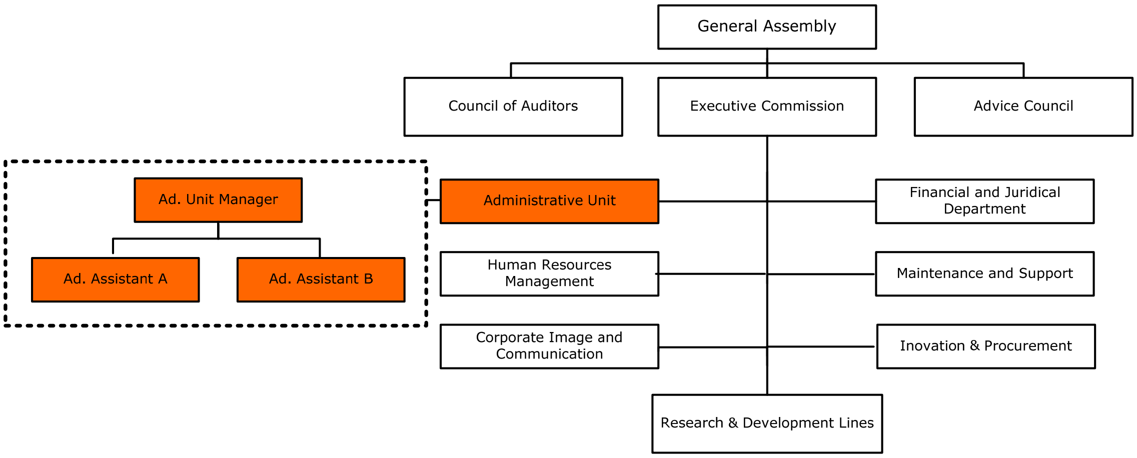


Figure R.3: Organizational chart of ADETTI with the areas in the scope filled with orange

Currently, ADETTI has 80 researchers (30 of which are full-time researches) and 11 support staff (3 of which work in the Administrative Unit). Most of the full-time researchers are lecturers and professors of the Information Sciences and Technologies Department, of ISCTE. A large number of undergraduate students of Computing and Engineering, are also participating in ADETTI projects in the scope of their final work for graduation.

IT support is provided by a contracted technician with a service delivery contract (avença).

The evaluation sphere included the following human resources:

ADETTI employees included in the scope		
Code	**Description**	**Role in the financial process**
AUM	Administrative Unit Manager	Verifies financial documentation Prepares financial report
AUE1	Administrative Unit Employee 1	Receives financial documentation Supports ADM in her tasks
AUE2	Administrative Unit Employee 2	Supports the process when AUE1 is not available.

2.3.5 Technological and physical description

2.3.5.1 Physical description

The facilities of the ADETTI comprise of four research labs and an administrative office. The office and three labs (Multimedia and Virtual Environments Lab, New Media Lab, Caixa Mágica Lab) are located in the ISCTE campus. The Security and Imaging Lab is situated in LISPOLIS, a science and technology park in Lisbon, at distance of approximately 8 km from ISCTE.

The Administrative Unit Office is located in the first floor of the ISCTE building, in the same physical room as Caixa Magica lab, the BSCW Server and mail server are located at Multimedia lab, as depicted in Figure R.4.

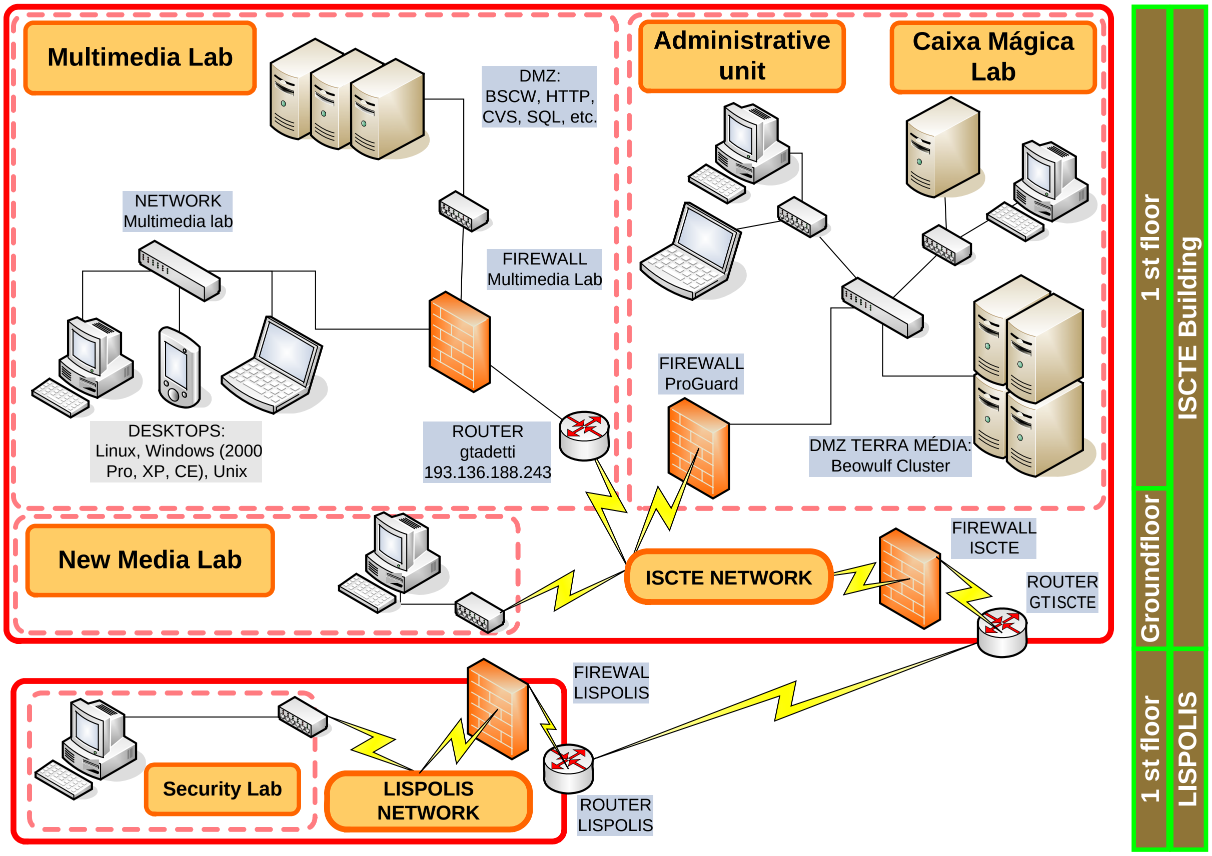


Figure R.4: ADETTI network infrastructure at ISCTE and LISPOLIS buildings

A comprehensive analysis of the physical security perimeters and entry controls of ADETTI is made in the present document in 5.3.1, as part of the compliance assessment with BSI controls.

2.3.5.2 Technological description

a) IT infrastructure

ADETTI uses the IT infrastructure of ISCTE (cabling, Internet access and SMTP services are provided by ISCTE). Only within ADETTI facilities, the hosts and networking equipment is under the jurisdiction of the association.

The cabling is UTP 5 Enhanced, deployed in a structured manner. Following the Steering Committee it was investigated two subnets used by ADETTI and, in particular, the addresses belonging to the organization:

- (1) 193.136.190.0 - 193.136.190.254 – Public IP addresses (registered by ISCTE)
- (2) 10.10.96.0 - 10.10.96.254 – Private IP addresses

The Multimedia Lab has an Ethernet LAN with teen desktops, four Silicon Graphics workstations, a Windows 2000 based domain server, a Linux file server, two printers and a scanner. The LAN rack is equipped with a Linux based router, two Ascend pipeline Bridge/Routers with ISDN connections, an ATM switch, a sixteen ports Fast Ethernet switch and a twelve ports Fast Ethernet hub.

BSCW server is situated in this lab, in an open rack (without any physical protection).

The Caixa Mágica Lab has a Beowulf Network Cluster with nine nodes, two of which are double processors systems. The LAN infrastructure connects thirteen Personal Computers and has three printers.

The New Media Lab was donated by Hewlett-Packard and comprise of twenty-one workstations, two printers, all connected by a third-two ports Fast Ethernet switch.

The Network and Security laboratory (at LISPOLIS) has sixteen nodes, two of which are double processors systems.

b) Network perimeters

The Internet access is provided by ISCTE. External access is filtered by ISCTE´s firewall (Check Point Next Generation) and by ADETTI´s own firewalls. Access from the Multimedia lab and LISPOLIS lab is controlled by separate Linux IPchains firewalls. Caixa Magica lab/administrative unit room use Caixa Magica´s Proguard firewall solution. The New Media lab is not protected from ISCTE network by any firewall.

c) Host identification techniques

The following techniques were conducted:

i) Enumeration of hosts

Host were enumerated through network scanners (GFI LANGuard and Shadow Security Scanner), which was applied in the ADETTI local area network and from the Internet. The data collected was then verified by other tools as NMAP 3.74 for Windows for operating system recognition.

ii) Identification of services and vulnerabilities

The detection of vulnerabilities was conducted by GFI LANGuard, Shadow Security Scanner and Nessus.[1] The network scanning was performed without domain credentials.

Microsoft hosts (the management unit desktops in ADETTI) were further inspected with Microsoft Baseline Security Scanner and Shavlik EnterpriseInspector (using an account with domain credentials) to verify the status of systems packs and patches of the operating system.

The service which is associated with the port number was verified through banner fingerprinting analysis and heuristic detection by the tool (Shadow Security Scanner). Nevertheless, in some cases, the port was associated with the service assigned by IANA (www.iana.org/assignments/port-numbers).

iii) Compilation of data in the Table

The data collected was organized in the following table in accordance with these rules:

- Hosts, which are considered by the Steering Committee to be under the scope, are shaded by light green.
- As some hosts had public (available from the Internet) and private IP addresses, it was listed both types of addresses.

[1] GFI LanGuard Network Security Scanner v3.0 beta2 is a commercial product, available at http://www.gfi.com. Safety-Lab Shadow Security Scanner 7.96 from www.safety-lab.com. The author used Network Security Tool (http://www.networksecuritytoolkit.org), a Linux bootable CD, which includes Nessus, as well as other security tools.

- The vulnerabilities indication obtained by the network scanner were not verified by local examination of the host, therefore it could be false positives. Vulnerabilities of are rated as High (H), Medium (M) and Low (L) according to the classification of the X-Force, a vulnerability rating scheme available at http://xforce.iss.net/xforce/alerts. When available the vulnerabilities are associated with the Common Vulnerability Evaluation identification, maintained by the MITRE organization [Tasker99] at the website http://cve.mitre.org.

- IP configuration: Servers are configured with fixed IP addresses. The workstations of the Administrative Unit are DHCP clients of RAIDER (Windows 2000 Server with the role of Domain Controller of RSI domain).

- In RAIDER, the manual updates are performed by the IT technician, in the workstations, the users, which are local administrators, perform this task.

#	Private IP address	Public IP address	Hostname	Operating System	Software	Domain / Workgroup	Open Ports	Vulnerabilities
01	10.10.96.1	193.136.190.121	lithium.adetti.intranet			ADETTI		
02	10.10.96.3		psi.adetti.intranet	Linux/SUSE	Apache 2.0.50 ; SSH-1.99-OpenSSH_3.8.1p1	ADETTI	21-FTP, 22-SSH, 80-HTTP, 111-SUNRPC	H: Several DoS bugs related with Apache and OpenSSH
03	10.10.96.4					ADETTI	21-FTP, 22-SSH, 111-SUNRPC	
04	10.10.96.7		raider.adetti.intranet	Windows 2000 Server with Service Pack 4	Microsoft-IIS 5.0, McAffe 7.0, Microsoft Office XP, Winzip 8.0, Terminal Services	RSI	21-FTP, 25-SMTP, 53-DNS, 80-HTTP, 135-RPC LOCATOR, 139-NETBIOS-Session, 389-LDAP, 445-MSF DS	M: Guest and krbtgt users never logged on
05	10.10.96.8		universe.adetti.intranet	Windows 2000		ADETTI	139-NETBIOS-SSN	
06	10.10.96.19		pedro.adetti.intranet			ADETTI	21-FTP	
07	10.10.96.21		sec.adetti.intranet			ADETTI	21-FTP	
08	10.10.96.22		lm-printer.adetti.intranet			ADETTI	21-FTP, 139-NETBIOS-Session, 445-MSF DS	
09	10.10.96.33		rede33.adetti.intranet			ADETTI	21-FTP	
10	10.10.96.34		rede34.adetti.intranet			ADETTI	21-FTP	
11	10.10.96.35		rede35.adetti.intranet			ADETTI	21-FTP	
12	10.10.96.36		nb-carlos.adetti.intranet			ADETTI	21-FTP	
13	10.10.96.37		rede37.adetti.intranet			ADETTI		
14	10.10.96.38		rede38.adetti.intranet			ADETTI		
15	10.10.96.39		rede39.adetti.intranet			ADETTI		
16	10.10.96.40		rede40.adetti.intranet			ADETTI		
17	10.10.96.41		rede41.adetti.intranet			ADETTI		
18	10.10.96.42		rede42.adetti.intranet	CaixaMagica 11	Postfix, Oracle XML DB/Oracle Database, SSH-1.99-OpenSSH_4.2	ADETTI	21-FTP, 22-SSH, 25-SMTP, 111-SUNRPC, 8080	L: SMTP server without AuthLogin
19	10.10.96.43		rede43.adetti.intranet			ADETTI		
20	10.10.96.44		rede44.adetti.intranet			ADETTI		
21	10.10.96.45		rede45.adetti.intranet			ADETTI		
22	10.10.96.46		rede46.adetti.intranet			ADETTI		
23	10.10.96.47		rede47.adetti.intranet	CaixaMagica 11	SquirrelMail, Apache 2.2.0, SSH-1.99-OpenSSH_4.2, Samba	Caixa Magica	21-FTP, 22-SSH, 80-HTTP, 111-SUNRPC, 139-NETBIOS-Session, 143-IMAPv2, 445-MSF-	H: SquirrelMail read_body.php Cross Site Scripting Vulnerability (CAN-

							DS, 687-RPC-UNIX	2002-1341) H: SquirrelMail read_body.php Cross Site Scripting Vulnerability (CVE-1999-0059) M: Apache Mod_SSL Custom Error Document Remote Denial Of Service Vulnerability (CVE-2005-3357)
24	10.10.96.48		rede48.adetti.intranet			ADETTI		
25	10.10.96.49		rede49.adetti.intranet			ADETTI		
26	10.10.96.50		rede50.adetti.intranet			ADETTI		
27	10.10.96.51		rede51.adetti.intranet			ADETTI		
28	10.10.96.53		rede53.adetti.intranet		SSH-1.99-OpenSSH_4.2	ADETTI	21-FTP, 22-SSH, 111-SUNRPC	
29	10.10.96.56		rede56.adetti.intranet			ADETTI	21-FTP, 139-NETBIOS-Session, 445-MSF DS	
30	10.10.96.58		rede58.adetti.intranet			ADETTI	21-FTP, 139-NETBIOS-Session, 445-MSF DS	
31	10.10.96.60		rede60.adetti.intranet	Windows 2000 Pro	Visual Studio.NET, MSF SQL	WORKGROUP	21-FTP, 135-RPC-LOCATOR, 139-NETBIOS-Session, 445-MSF DS	
32	10.10.96.70		rede70.adetti.intranet	Windows 2000 Pro	Visual Studio.NET, MSF SQL	MEDIALAB	21-FTP, 135-RPC-LOCATOR, 139-NETBIOS-Session, 445-MSF DS	L: Guest user never logged on
33	10.10.96.73		rede73.adetti.intranet	Windows 2000 Pro	Apache 2.0.52; mod_ssl/2.0.52 OpenSSL/0.9.7e PHP/5.0.4; Visual Studio.NET	WORKGROUP	21-FTP, 80-HTTP, 135-RPC-LOCATOR, 139-NETBIOS-Session, 445-MSF DS	H: OpenSSL insecure protocol negotiation weakness (CAN-2005-2969) M: Apache mod_ssl SSLCipherSuite Access Validation Vulnerability (CAN-2004-0885)
34	10.10.96.80		rede80.intranet			ADETTI	21-FTP, 139-NETBIOS-Session, 445-MSF DS	
35	10.10.96.95		rede95.intranet	Windows 2000 Pro	Adobe Photoshop 7.0 Autodesk AEC Object Enabler 2.0 SafeCast Shared	MEDIALAB	21-FTP, 25-SMTP, 80-HTTP, 135-RPC-LOCATOR, 139-NETBIOS-Session, 445-	H: Ftpd allows root access (CVE-1999-0082) H: SNMP Remote Access for this community

					Components Cortona® VRML Client Creative WebCam NX Ultra Driver (1.01.03.0112) Creative WebCam NX Pro Driver (1.00.06.0512) Creative Video Blaster WebCam 3 USB/WebCam Plus Driver Deep Exploration Doc-O-Matic 4 for .NET (Commercial) Easy CD-DA Extractor 4.3.1 FlashGet(JetCar) OpenGL Extension Viewer Java 2 Platform, Enterprise Edition 1.4 SDK Developer Release Java Web Start GnuWin32: LibPng version 1.2.5 C-Dilla Licence Management System Macromedia Shockwave Player Microsoft .NET Framework 1.1 Microsoft .NET Framework 2.0 Ahead Nero Burning ROM NVIDIA Windows 2000/XP Display Drivers NVIDIA Display Driver OpenSceneGraph Export version 0.9.2b for 3ds max osgEdit 0.5.0 Windows Media Player Hotfix [See wm828026 for more information] Sentinel System Driver Remote Administrator v2.2 Macromedia Flash Player 8 SightSpeed (remove only) Tiff-3.6.1 Complete package, except sources		MSF DS	L: Anonymous FTP is enabled (CAN-1999-0497) L: Guest user never logged on

					(GnuWin32) Update Rollup 1 for Windows 2000 SP4 Microsoft Visual Studio .NET Enterprise Architect 2003 - English VobSub v2.23 (Remove Only) VR4MAX Navigator Lite R4.01 VR4MAX Navigator Pro R4.01 VR4MAX Translator R4.01 VrmlPad Winamp3 (remove only) WinCvs 1.2 WinRAR archiver XviD MPEG-4 Codec ZoneAlarm Microsoft Office 2000 SR-1 Premium Hi-Speed DVD Creator Java 2 Runtime Environment, SE v1.4.1_01 Microsoft FrontPage Client - English McAfee VirusScan Enterprise Microsoft Visual J# .NET Redistributable Package 1.1 M3D-Editor Ulead VideoStudio 6 SE DVD Dawn MSDN Library for Visual Studio .NET 2003 ZyDAS Wireless LAN - USB NVIDIA Cg Compiler WebFldrs Microsoft .NET Framework 2.0 3ds max 5 Microsoft DirectX 9.0 SDK MSN Messenger 6.2 Autodesk VIZ 2005 Visual Studio .NET Enterprise Architect 2003 -			

					English			
36	10.10.96.97		rede97.intranet	Windows 2000 Pro	Microsoft-IIS 5.0, Visual Studio.NET, SQL	MEDILAB	21-FTP, 25-SMTP, 80-HTTP, 135-RPC-LOCATOR, 139-NETBIOS-Session, 445-MSF-DS	H: Ftpd allows root access (CVE-1999-0082) L: Anonymous FTP is enabled (CAN-1999-0497) L: Guest user never logged on
37	10.10.96.114		rede114.intranet			ADETTI	21-FTP, 139-NETBIOS-Session, 445-MSF-DS	
38	10.10.96.129		rede129.adetti.intranet	Windows	Microsoft-IIS 6.0, Apache 2.0.58, PHP 5.1.4, FileZilla Server version 0.9.18 beta,	ADETTI	21-FTP, 80-HTTP, 135-RPC-LOCATOR, 139-NETBIOS-Session, 445-MSF-DS, 8080	H: FileZilla FTP FileZilla FTP H: PHP Error_Log Safe_Mode Restriction-Bypass Vulnerability
39	10.10.96.132		rede132.adetti.intranet			ADETTI	21-FTP, 80-HTTP, 139-NETBIOS-Session, 445-MSF-DS	
40	10.10.96.137		rita.adetti.intranet	Windows XP Pro 2002 version Service Pack 1	McAffe 7.0, Microsoft Office 2003, Winzip 8.0, Corel Draw 12, Winrar, Adobe Acrobat Reader, SSH, ws_ftp, Open Office 1.1 for Windows, Internet Explorer 6.0, Yahoo Messenger e o MSN Messenger	RSI	135-EPMAP, 139-NETBIOS-Session, 445-MSF-DS	
41	10.10.96.165		rede165.adetti.intranet			ADETTI	21-FTP, 80-HTTP, 135-RPC-LOCATOR, 139-NETBIOS-Session, 445-MSF-DS	
42	10.10.96.169		rede169.adetti.intranet		SSH-1.99-OpenSSH_4.2	ADETTI	21-FTP, 22-SSH, 111-SUNRPC	
43	10.10.96.177		rede177.adetti.intranet			ADETTI	21-FTP, 139-NETBIOS-Session	
45	10.10.96.190		rede190.adetti.intranet		SSH-1.99-OpenSSH_4.2	ADETTI	22-SSH, 111-SUNRPC	
46	10.10.96.198		rede198.adetti.intranet	Windows XP Pro 2002 version Service Pack 1	McAffe 7.0, Microsoft Office 2003, Winzip 8.0, Corel Draw 12, Winrar, Adobe Acrobat Reader, SSH,	RSI	135-EPMAP, 139-NETBIOS-Session, 445-MSF-DS	H: Administrator account without password.

					ws_ftp, Open Office 1.1 for Windows, Internet Explorer 6.0, Yahoo Messenger e o MSN Messenger			
46	10.10.96.200		rede200.adetti.intranet	Windows XP Pro	Microsoft-IIS 5.1	MEDIALAB	21-FTP, 25-SMTP, 80-HTTP, 135-RPC-LOCATOR, 139-NETBIOS-Session, 389-LDAP, 445-MSF-DS, 4899 - RAdmin	L: SMTP server without AuthLogin
47	10.10.96.211		rede211.adetti.intranet	Windows XP Pro 2002 version Service Pack 1	McAffe 7.0, Microsoft Office 2003, Winzip 8.0, Corel Draw 12, Winrar, Adobe Acrobat Reader, SSH, ws_ftp, Open Office 1.1 for Windows, Internet Explorer 6.0, Yahoo Messenger	RSI	21-FTP, 137-NETBIOS-NS, 139-NETBIOS-Session, 445-MSF-DS	
48	10.10.96.212		rede212.adetti.intranet	Windows XP Pro	Microsoft-IIS 5.1, Visual Studio.Net, RAdmin 3.0	MEDIALAB	25-SMTP, 80-HTTP, 135-RPC-LOCATOR, 139-NETBIOS-Session, 389-LDAP, 445-MSF-DS, 4899 - RAdmin	H: Microsoft IIS WebDAV PROPFIND and SEARCH Method Denial of Service Vulnerability (CAN-2003-0226) H: IIS Showcode ASP Vulnerability (CAN-1999-0736) L: Guest user never logged on
49	10.10.96.215		rede215.adetti.intranet	CaixaMagica 11	Apache 2.2.0; SSH-1.99-OpenSSH_4.2	ADETTI	21-FTP, 22-SSH, 80-HTTP	M: Apache Mod_SSL Custom Error Document Remote Denial Of Service Vulnerability (CVE-2004-3357)
50	10.10.96.218		rede218.adetti.intranet			ADETTI	21-FTP, 139-NETBIOS-Session, 445-MSF-DS	
51	10.10.96.220		rede220.adetti.intranet			ADETTI	21-FTP, 139-NETBIOS-Session, 445-MSF-DS	
52	10.10.96.228		rede228.adetti.intranet	Windows	Apache 2.2.3, PHP 5.2.0	ADETTI	21-FTP, 80-HTTP, 139-NETBIOS-Session	
53	10.10.96.237		rede237.adetti.intranet			ADETTI	21-FTP, 139-NETBIOS-Session, 445-MSF-DS	
54		193.136.188.3	neftis.iscte.pt	Linux	SMTP (postfix, mysql, courier-imap)	ADETTI	25-smtp, 110-pop3, 143-imap2, 993-imaps, 995- pop3s	H: Gain root remotely: Xtramail pop3 overflow (CVE-1999-1511)
55		193.136.190.33	indigoxz.adetti.iscte.pt			ADETTI		

56		193.136.190.34	indy1.adetti.iscte.pt			ADETTI		
57		193.136.190.35	o2video.adetti.iscte.pt			ADETTI		
58		193.136.190.36	lablin1.adetti.iscte.pt			ADETTI		
59		193.136.190.37	labmult1.adetti.iscte.pt			ADETTI		
60		193.136.190.38	labmult2.adetti.iscte.pt			ADETTI		
61		193.136.190.39	labmult3.adetti.iscte.pt			ADETTI		
62		193.136.190.40	labmult5.adetti.iscte.pt			ADETTI		
63		193.136.190.41	labmult4.adetti.iscte.pt			ADETTI		
64		193.136.190.42	superlab.adetti.iscte.pt			ADETTI		
65		193.136.190.43	dhl.adetti.iscte.pt			ADETTI		
66		193.136.190.44	labmult6.adetti.iscte.pt	Linux	Apache 2.0.52, mod_ssl/2.0.52, OpenSSL/0.9.7, PHP/4.3.10 Server, Sun-Java-System/Web-S	ADETTI	21-FTP, 22-SSH, 80-HTTP, 8080	H: Apache allows directory browsing H: Folder with copyrighted music H: PHP memory_limit Remote Code Execution Vulnerability (CAN-2004-0594) M: Apache mod_ssl SSLCipherSuite Access Validation Vulnerability (CAN-2004-0885) M: OpenSSH-portable PAM Authentication Remote Information Disclosure Vulnerability (CAN-2003-0190) M: PHP Strip_Tags() Function Bypass Vulnerability (CAN-2004-0595)
67		193.136.190.45	labmult7.adetti.iscte.pt	Linux	Apache 2.2.2, PHP/5.1.4	ADETTI	21-FTP, 22-SSH, 80-HTTP, 111-SUN RPC	H: Access to the phpinfo page
68		193.136.190.46	labmult8.adetti.iscte.pt			ADETTI		
69		193.136.190.47	labmult9.adetti.iscte.pt			ADETTI		
70		193.136.190.48	telemed.adetti.iscte.pt			ADETTI		
71		193.136.190.49	labserver.adetti.iscte.pt			ADETTI		
72		193.136.190.50	web1.adetti.iscte.pt			ADETTI		

73		193.136.190.51	lablin2.adetti.iscte.pt	Linux	Server: Apache/1.3.27 (Linux/SuSE) PHP/4.3.1 BSCW 4.2.1 - released 040429-1151, (http://lablin2.adetti.iscte.pt/bscw) BIND 8.1.1 OpenSSH	ADETTI	21-FTP, 22-SSH, 80-HTTP, 111-SUN-RPC, 113-IDENT, 8080, 36251-RPC-UNIX	H: OpenSSH LoginGraceTime Remote Denial Of Service Vulnerability (CAN-2004-2069) M: Apache mod_ssl SSLCipherSuite Access Validation Vulnerability (CAN-2004-0885)
74		193.136.190.52	labmut10.adetti.iscte.pt			ADETTI		
75		193.136.190.53	labmut11.adetti.iscte.pt			ADETTI		
76		193.136.190.54	labmut12.adetti.iscte.pt			ADETTI		
78		193.136.190.55	www.aitear.com			ADETTI		
79		193.136.190.56	toshiba2.adetti.iscte.pt			ADETTI		
80		193.136.190.58	pl75.adetti.iscte.pt			ADETTI		
81		193.136.190.59	gtadetti.adetti.iscte.pt	Linux		ADETTI	21-FTP, 443-HTTPS	
82		193.136.190.60	iris.adetti.iscte.pt			ADETTI		
83		193.136.190.61	indy2.adetti.iscte.pt			ADETTI		
84		193.136.190.62	fore-switch-eth.adetti.iscte.pt			ADETTI		
85		193.136.190.64				ADETTI	21-FTP, 80-HTTP	
86		193.136.190.65	gtrsi.adetti.iscte.pt	Linux	Bind 8.2.4	ADETTI	21-FTP, 53-DNS, 443-HTTPS	H: Multiple DoS vulnerabilities associated with BIND 8 as CAN-2002-1221, CAN-2003-0914, CAN-2002-1219, CAN-2002-0651 and CVE-1999-0851.
87		193.136.190.70	router3.adetti.iscte.pt	Cisco IOS 12.1(22)E5,		ADETTI	21-FTP, 23-TELNET, 80-HTTP	H: Router with access from the Internet to configuration tools H: SNMP access enabled
88	172.16.0.104	193.136.190.97	ipserver.adetti.iscte.pt		Bind 8.1.1	ADETTI	21-FTP, 53-DNS	H: Multiple DoS vulnerabilities associated with BIND 8 as CAN-2002-1221, CVE-2001-0012, CAN-2002-1219, CVE-1999-0024, CAN-2002-0651, CVE-1999-

								0851.
89	172.16.0.100	193.136.190.98	otelo.adetti.iscte.pt		Apache, SSH-2.0-OpenSSH_3.9p1	ADETTI	21-FTP, 22-SSH, 53-DNS, 80-HTTP, 8080	M: SSH server with a Remote Information Disclosure Vulnerability (CAN-2003-0190)
91		193.136.190.99	tonivirtual.adetti.iscte.pt			ADETTI		
92	172.16.0.13	193.136.190.100	gandalf.adetti.iscte.pt	CaixaMagica	Apache 2.0.50, SSH-1.99-OpenSSH_3.9p1	ADETTI	21-FTP, 22-SSH, 80-HTTP	H: Apache DoS (CAN-2004-0809, CAN-2004-0748, CAN-2004-0751, CAN-2004-0747) M: SSH server with a Remote Information Disclosure Vulnerability (CAN-2003-0190)
93	172.16.0.10	193.136.190.101	hobbit.adetti.iscte.pt			ADETTI	21-FTP	
94	172.16.0.11	193.136.190.102	aragorn.adetti.iscte.pt	CaixaMagica 11	Apache 2.2.0, Apache-Coyote 1.1, SSH-1.99-OpenSSH_4.2	ADETTI	21-FTP, 22-SSH, 80-HTTP, 113-IDENT, 119-NETWORK_NEWS, 143-IMAP, 389-LDAP, 8080	H: Apache allows directory browsing
95	172.16.0.12	193.136.190.103	isildur.adetti.iscte.pt	Linux	Zope/(unreleased version, python 2.3.4, linux2) ZServer/1.1 Plone/2.0.5, vsFTPd 2.0.1	ADETTI	21-FTP, 80-HTTP	M: Anonymous FTP is enabled (CAN-1999-0497)
96	172.16.0.101	193.136.190.104	tonyvirtualadetti.iscte.pt			ADETTI		
97	172.16.0.105	193.136.190.106	scluisa.adetti.iscte.pt			ADETTI		
98		193.136.190.107	scrufi.adetti.iscte.pt			ADETTI		
100		193.136.190.108	3DURBAN	Windows 2000 Server	Microsoft-IIS 5.0, Microsoft ESMTP Server 1.x - 6.x – “220 labmult7.adetti.iscte.pt”, IMAP - Interim Mail Access Protocol v2 SSH-2.0-OpenSSH_3.7.1p1, Terminal Service, ASP.NET, SQL	RSI	21-FTP, 22-SSH, 25-SMTP, 80-HTTP, 135-RPC-LOCATOR, 139-NETBIOS-Session, 445-MSF-DS	H: OpenSSH (CAN-2004-2069) H: IIS 5.0 DoS (CAN-2003-0226) M: SSH server with a Remote Information Disclosure Vulnerability (CAN-2003-0190)
101	172.16.0.1	193.136.190.113	ricky.adetti.iscte.pt	CaixaMagica 11	Apache/2.0.54, Bind 8.1.1, SSH-1.99-OpenSSH_4.1		22-SSH, 23-TELNET, 25-SMTP, 42-NAMESERVER, 53-DNS, 79-FINGER, 8080	H: Multiple DoS vulnerabilities associated with BIND 8 as CAN-2002-1221, CVE-2001-0012, CAN-2002-1219, CVE-1999-0024, CAN-2002-0651, CVE-1999-0851.
102	172.16.0.2	193.136.190.114		CaixaMagica 11	Apache 2.2.0, vsFTPd 2.0.4	ADETTI	21-FTP, 22-SSH, 80-	M: Anonymous FTP is

							HTTP	enabled (CAN-1999-0497)
103	172.16.0.3	193.136.190.115	sclara.adetti.iscte.pt	CaixaMagica 11	Apache 1.3.27, mod_ssl/2.8.12, OpenSSL/0.9.6i, mod_perl/1.27, PHP/4.3.1	ADETTI	21-FTP, 80-HTTP	H: Apache mod_include Local Buffer Overflow Vulnerability CAN-2004-0940, CAN-2003-0851, CAN-2003-0542 H: OpenSSL (CAN-2003-0131, CAN-2004-0079, CAN-2003-0147, CAN-2004-0975, H: PHP CAN-2004-0594
104	172.16.0.14	193.136.190.120	angra.adetti.iscte.pt			ADETTI		
105		193.136.190.122	scmada.adetti.iscte.pt			ADETTI		
106		193.136.190.123	scrute.adetti.iscte.pt			ADETTI		
107		193.136.190.124	scana.adetti.iscte.pt			ADETTI		

In conclusion of the network security assessment it was found that:

- The five hosts included in the ISMS scope (raider, rita, rede198, rede211, lablin2) revealed few vulnerabilities. The most perilous vulnerabilities were found in lablin2 and rede198.
- The neighbouring hosts of the scope present indications of multiple vulnerabilities, in particular some security configurations not recommended as anonymous FTP access and outdated software versions with known vulnerabilities. A fact that is especially relevant is that some hosts which support services to the scope (as neftis.iscte.pt, which is the SMTP server) present some traces of possible vulnerabilities.
- Most found problems in lablin2 and rede198 are related to outdated services, such as the web server, PHP module, proxy module and the names server (BIND), which can easily resolved if the operating system and the mentioned software are updated. These issues are described below:

Host	Vulnerability	Resolution	Level of danger (following X-Force at http://xforce.iss.net)	Remarks
lablin2	Outdated DNS version (BIND 8.1.1 version)	Update the DNS to any superior version	Medium	In first place, this version allows the identification of the DNS software version, which then can be used by hackers to organized specific version attacks, such as cache remote poisoning.
	Outdated Web server version (Apache 1.3.27)	Update the Apache to any superior version	High	This version allows several attack types, especially Denial of Service (DoS), among others. The complete list is at: http://www.apache.org/dist/httpd/CHANGES_1.3.
	Outdated PHP module version (PHP 4.3.1)	Update the PHP to the current version (4.3.9)	Medium	This outdated version of PHP can be subjected to attacks of Denial of Service (DoS). The full list of vulnerabilities is available at: http://pt.php.net/ChangeLog-4.php#4.3.10.
	Internal IP address exposed in web server reply	Reconfigure BIND server as expounded in XX.	High	The server identifies himself as: Server: Apache/1.3.27 (Linux/SuSE) PHP/4.3.1 Apache/1.3.27 Server at 172.16.0.1.
	Outdated CVS service version	Update the CVS to any superior version	Medium	The features of this version of CVS can be exploited to gain remote access to the server with the CVS credentials.
rede198	Local administrator account without password	Set a policy for a minimum of 8 digits	High	Anyone can logon and use the administrator account.

2.4 Interfaces and dependencies of the ISMS (T02.3)

From the examination of the process description, it was possible to uncover a series of external entities to which the scope is dependent or simply has interfaces.

A dependency represents a relationship capable of stopping the process within the scope. An interface is a point of interconnection between the scope and other areas of the organization or other entities.

a) Interfaces

The process under evaluation has a group of different relationships with external entities. Most of these interfaces with a third party are formalised by a form of contractual relationship, therefore the related contractual requirements are identified at 3.3.2. The cited interfaces are listed in the following table and depicted in the Figure R.5.

Type of relationship	Organization	Interface
Main supplier and partner	- ISCTE	- Controls the external physical access to the facilities. - Controls the Internet router, Internet proxy, mail server and data network between ADETTI rooms. - Controls the delivery of snail mail (letters) sent to ADETTI. - Provides electricity, water for the office.
Funding for projects and activities	- European Commission - FCT	- Main clients of ADETTI activities - Organizations that demand compliance with security requirements (availability of reports for 4 years, confidentiality of results)
Research partners	Examples: Hospital Garcia da Orta; Câmara Municipal de Lisboa	- Sensitive information need to be shared among partners.
Provider of accountant services	Accountant	- Processes and stores financial data of projects.
Provider of legal counselling services	Legal counselling	- Supervises all contracts that ADETTI signs.
Contracted supplier	Banks, Insurance companies	
Contracted supplier	Equipment consumables and supplies	- Printing paper, laser toner, stationery, etc. for the office.
Contracted supplier	IT service	- Service provider for helpdesk support and systems maintenance - Procurement of spare parts to repair IT equipment
Government	Finance Ministry (tax authority)	- Establishes requirements for storage of financial data and delivery of financial declarations in a determined point of time

Table R.1: Main interfaces of the scope

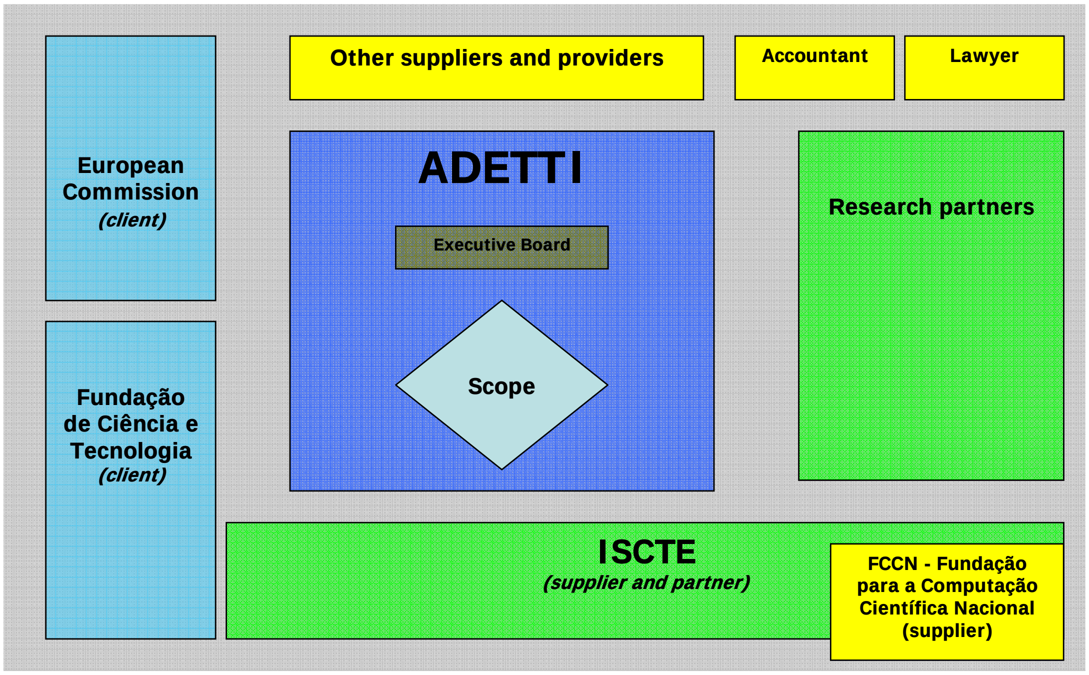

Other suppliers and providers
Accountant
Lawyer
European Commission (client)
ADETTI
Executive Board
Scope
Research partners
Fundação de Ciência e Tecnologia (client)
ISCTE (supplier and partner)
FCCN - Fundação para a Computação Científica Nacional (supplier)

Figure R.5: Organizational context of the scope showing its interfaces

b) Dependencies

The scope is dependent of the following from the third party service providers:

- Accurate and timely delivery of financial information by projects managers;
- Stable and continuous provisioning of electricity by EDP;
- Reliable SMTP service provided by ISCTE;
- Reliable Internet access provided by ISCTE (who is client of the FCCN´s network).

3. Define business and legal requirements

3.1 Requirements

Inputs		Practices and techniques	Output(s)
T03.1	• Business requirements	• Review of documents with strategic requirements • Interviews • SWOT analysis	• List of business concerns for SM
T03.2	• Legal literature • Existing contracts	• Catalogue contractual and legal requirements	• List of legal and contractual requirements for SM

3.2 List of business requirements for SM (T03.1)

The establishment of business objectives was undertaken through a number of environmental and strategic analyses that include:

a. A review of the relevant ADETTI´s documents
b. Interviews
c. SWOT analysis

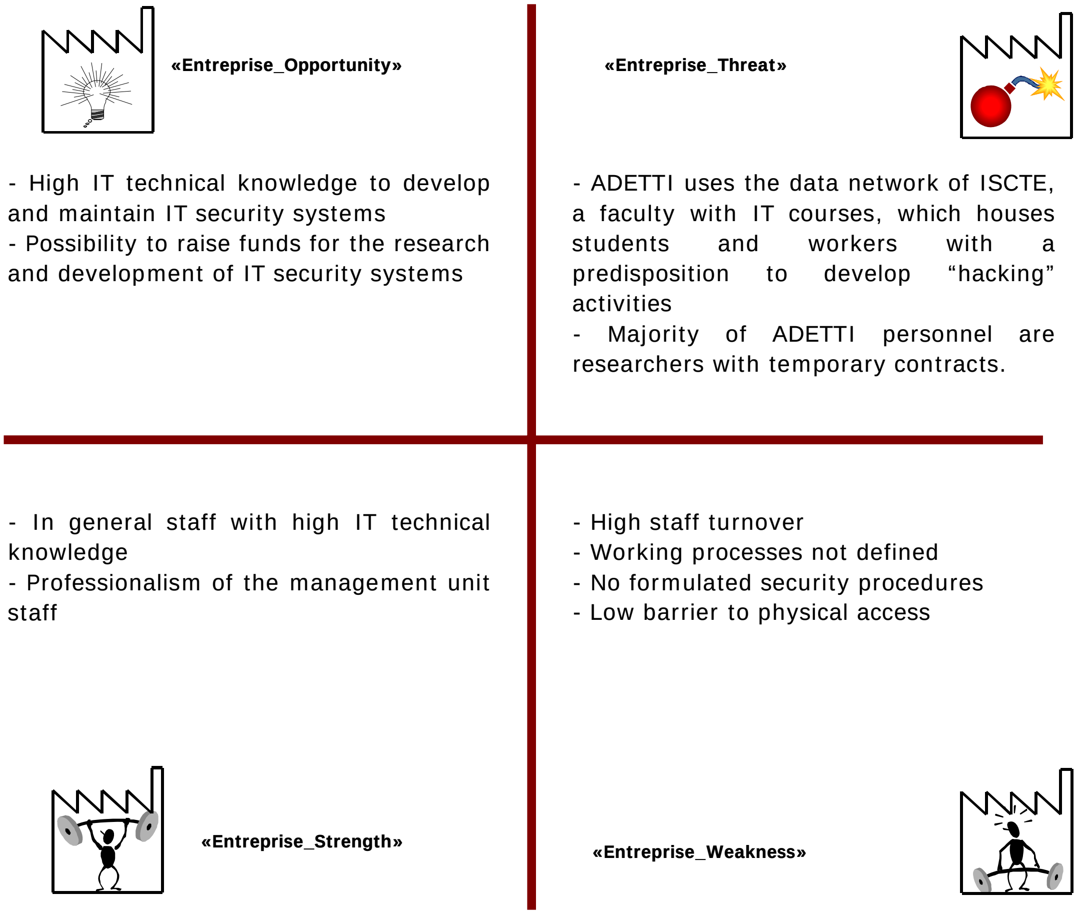
Firstly, a group of documents regarding ADETTI strategy were analysed. The following documents were scrutinized:

[ADETTI02]	ADETTI, Relatório e Contas 2000, 2001/ Plano e Orçamento 2002, Lisboa, Portugal, 2002
[ADETTI03]	ADETTI, Creating Knowledge, PowerPoint Presentation, Lisboa, Portugal, 2003
[Dias03]	Dias, Miguel, General Presentation of the ADETTI Research Unit, PowerPoint Presentation, Lisboa, Portugal, 2003
[Neves01]	Neves, Daniel, ADETTI Presentation, PowerPoint Presentation, Lisboa, Portugal, 2001
[Neves03]	Neves, Daniel, Análise da Estrutura Organizacional, PowerPoint Presentation, Lisboa, Portugal, 2003

From these documents it was uncovered a series of issues with possible influence in SM. The relevance of these issues was verified in interviews with the three members of Administrative Unit and a manager with technical responsibilities (Eng. Manuel Gamito).

In these interviews, it was identified vulnerabilities/threats and strengths/improvement opportunities of ADETTI in relation to the protection of the evaluation scope.

The collected answers were then classified in a SWOT (Strength, Weaknesses, Opportunities and Threats) analysis, as evinced in Figure R.6.



- High IT technical knowledge to develop and maintain IT security systems
- Possibility to raise funds for the research and development of IT security systems

- ADETTI uses the data network of ISCTE, a faculty with IT courses, which houses students and workers with a predisposition to develop "hacking" activities
- Majority of ADETTI personnel are researchers with temporary contracts.

- In general staff with high IT technical knowledge
- Professionalism of the management unit staff

- High staff turnover
- Working processes not defined
- No formulated security procedures
- Low barrier to physical access

Figure R.6: SWOT analysis of ADETTI

The final outcome of this work is Table R.2, which was revised and approved by the Steering Committee.

ID	Strategic requirement	Underlying issue	Implications for security management
B1	Develop new partnership relationships for new research projects	Opportunities for new projects have to be found within the European community of ICT organizations	Not directly applicable
B2	Reinforcement of the research support activities in order to sustain the growth of the scientific capacity	Improvements in the organization of research support activities should be seek in order to increase the efficiency of services (deliver more services with the same resources)	The analysis of the protection of working processes can be used as a input to future reengineering project
B3	Increment and develop the integration of ADETTI in ISCTE universe	Increase relationships with other entities within ISCTE	The SM implementation will involve contacts with ISCTE in order to define SLA of provided services (e.g. electrical power)
B4	Maintain the efforts to improve the	Not applicable	Not applicable

	corporative image and website		
B5	Improve financial reporting process	Ensure better and faster integration of the financial report in the final report of projects	Increase availability of the financial reporting data through the application of security safeguards

Table R.2: Business requirements

3.3 List of legal and contractual requirements for SM (T03.2)

This deliverable was produced by the following actions by the implementation advisor:

1. Analyse the existing legislation concerning security management (employing data taken from the CNPD and PJ website).
2. Develop an index of the legislation, grouping it by subject; legal requirements are identified as "L(number)" as evinced in the column "Issues" in the next table.
3. Identify implications for security management of the legislation and adequate actions to achieve compliance as shown in the table below.
4. Review and approve the above outcome by the Steering Committee.

3.3.1 Legal requirements

Issues	Applicable legislation	Description	Implications in security management	Actions to ensure compliance
L1. Labour legislation				
L1.1 Legal status of internal security regulations	(1) Lei Preambular ao Código do Trabalho – law number 99/2003 from 27th August (2) Regulamento do Código do Trabalho – law number 35/2004 from 29th July	For security norms to be recognised with the legal status of internal regulations under the Portuguese labour legislation, they have to be published according to a defined procedure.	- Security norms must be communicated to employees according to a procedure compliant with the Portuguese labour legislation. - Records of this communication must be kept for legal reasons.	- Verify legal compliance of exiting internal norms. - Application of security regulations as policy and procedures
L2. Personal data protection legislation				
L2.1 Personal data protection principle	(1) Lei 67/98 - Lei da Protecção de Dados Pessoais from 26th October 1998 (derives from the European Commission's Data Privacy Directive 95/46/EC). (2) Lei 41/2004 - Lei sobre o tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas, from 18th August 2004. (3) Lei 43/2004 - Lei de organização e funcionamento da Comissão Nacional de Protecção de Dados, from 18th August	Portuguese law recognises to citizens the ability to exercise control over how others use their personnel information. These rights are: (1) information right - citizens are entitled to be informed, by the organization, which is collecting or processing the personal data, of the following: – the identity of the organization, – the purpose of the processing, – the recipients of the data,	- Every system that processes or database that stores personal data, except those excluded by the law 67/98 (as database used to process salaries), are required to be notified and authorised by the Data Protection National Commission. - The rulings from the Data Protection National Commission cover issues as controlling web access of employees, controlling content of emails, usage of video surveillance, usage of any access control devices that required biometric data.	- Verify legal compliance of all applicable database and systems in ADETTI (web included). - Include a step of legal compliance in all system development/acquisition process.

	2004. (4) Rulings from the Data Protection National Commission (Comissão Nacional de Protecção de Dados).	– the rights of the data subjects, - before the data is disclosed for the first time to third parties or before they are used on their behalf for the purposes of direct marketing. (2) Access right – individuals have the right to access their personal data (3) rectification and erasure right – data which is inaccurate or incomplete may be rectified by the individual. (4) objection right – Citizens are entitled to object at any time, on compelling and legitimate grounds, to the processing of personal data. This protection covers the capture, processing, storage, use and disclosure of data relating to individuals. Personal data is any information relating to a person identified or identifiable either directly or indirectly, in particular by reference to an identification number. This information may, for example, be the name, date of birth, a telephone number, biometric data, medical data, professional details, etc [CNPD04].		
L2.2 Video surveillance		The installation of video surveillance cameras is subjected to the authorization of the CNPD [CNPD04].		- Verify legal compliance of exiting systems.
L2.3 Use of biometric data in access control devices		Any database which stores biometric data is subjected to the authorization of the CNPD.		- Verify legal compliance of exiting databases.

L2.4 Access to personal emails and files		Within the Portuguese legislation, employees are entitled to not disclose the content of e-mails and files which contain personal information (art. 21º1 from Código do Trabalho). However, the organization can define usage rules of the communication devices and may collect statistic data to verify the compliance of their employees. In cases that the organization has strong suspicions of unlawful behaviour of an employee, the organization may access to his personal emails and files.		- Verify legal compliance of exiting procedures.
L2.5 Internet access control		Organization can define usage rules of the communication devices and may collect statistic data to verify the compliance of their employees.		- Verify legal compliance of exiting procedures.
L3. Computer crimes legislation				
L3.1 Computer crimes principle	(1) Portuguese Informatics Criminal Law (Lei da Criminalidade Informática, law number 109/91 from 17th August) (2) Portuguese Penal Code - 193º, 194º and 221º	The computer crime law defines crimes such as forgery, deliberate misuse of data and programs, computer sabotage, illegitimate access, illegitimate interception, illegitimate reproduction of protected programs. The Penal Code establishes crimes such as profligate, deception using computer systems.	- As this law, considers individuals as personally liable if they commit any of the defined crimes, the organization may hold the right of criminal prosecution against any employee suspected of misuse of computer equipment/systems. This right can be expressed in a policy and disciplinary procedure. - Guidance to staff regarding the use of computer equipment/systems is incorporated within security norms.	- Define a disciplinary procedure as part of the Human Resource documentation. - Incorporate in the applicable polices the warning that misuse of computer equipment/systems is subject to legal prosecution and a disciplinary procedure.

L4. Copyright protection legislation				
L4.1 Protection of copyrighted content	(1) Código dos Direitos de Autor e dos Direitos Conexos - law number 144/91 (2) Regime de Protecção Jurídica das Bases de Dados - law number 252/94 from 20 October (3) Protecção Jurídica das Bases de Dados - law number 122/00	Covers the need for compliance with legal restrictions on the use of material in respect of which there may be intellectual property rights, such as copyright, design rights or trademarks. In the same context, proprietary software products, supplied under a licence are also covered.	- The software licensed by ADETTI can not be copied to be used for other purpose that the work usage.	- Verify legal compliance against this law. - Guidance and awareness to staff regarding compliance copyright laws is incorporated within security norms.
L5. Electronic signature				
L5.1 Electronic signature	(1) Decreto-lei nº 290-D/99 from 2 August	Defines the legal framework of electronic documents and digital signatures		- Verify legal compliance against this law.
L6. Organizational records protection legislation				
L6.1 Retention period of organizational records	(1) Código do IRC, art.º 98 (2) Código Comercial, art.º 40 (3) Lei n.º 105/97 from 13th September, art.º 6º	- Accountant books and records must be kept for 10 years. - Recruitment records must be kept for 5 years (derives from Lei n.º 105/97).		- Verify legal compliance against this law.
L7. Safety, hygiene and occupational health legislation				
L7.1 Safety, hygiene and occupational health legislation	(1) Lei Preambular ao Código do Trabalho – law number 99/2003 from 27th August (2) Regulamento do Código do Trabalho – law number 35/2004 from 29th July (3) Juridical Framework of safety, hygiene and health and safety - Decreto-Lei nº 441/91 from 14 de November (4) Prevention of professional risks - Decreto-Lei nº 133/99 from 29th March	- ADETTI office and equipment must be complaint with the safety regulations, e.g. fire protection, noise, emanation of electronic waves.		- Verify legal compliance against this law. - Incorporate in the procedure related to procurement, the verification of legal compliance of system with the Safety, hygiene and occupational health legislation.

L8. Legislation concerning research activities				
L8.1 Legal framework of research institutions	Regime Jurídico das Instituições de Investigação (Decreto-Lei Nº 125/99)	Art. 27.º of this governmental law defines confidentiality duties of experts and external entities working in advisory and assessment roles.	According to this law, ADETTI is allowed to ask a non disclosure agreement for any external individual or institution that access relevant data of the research projects.	- Create a non disclosure agreement
L8.2 Fundação para a Ciência e Tecnologia funding legal framework	Documents from the Fundação para a Ciência e Tecnologia (FCT) related to funding programme.	These documents define the obligations of ADETTI related with this funding programme.	Definition of the requirements related to financial reporting.	- These requirements are mandatory for the security scope.
L8.3 European Commission funding legal framework	Documents from the Sixth Framework Programme (FP6) 2002-2006 from Information Society Technologies (IST).	These documents define the obligations of ADETTI related with this funding programme.	Definition of the requirements related to financial reporting.	- These requirements are mandatory for the security scope.
L9. Information security legislation for public institutions				
L9.1 Information classification legislation	Instructions for the national security, safeguard and defence of classified information (Instruções para a Segurança Nacional, Salvaguarda e Defesa das Matérias Classificadas – SEGNAC 1 - Resolução do Conselho de Ministros n.º 50/88 de 3 de Dezembro de 1988	Classified information	This law is not applicable to ADETTI.	- Verify if any existing funding contract requires the conformity with this law.

3.3.2 Contractual requirements

This outcome was produced by the following actions:

1. Review the identified interfaces and dependencies of the scope (T02.4).
2. Analyse the existing contracts and Memorandum of Understanding with third parties – based on data taken from the Annual Report [ADETTI02] and interviews with the AD Unit Manager and President of the institution.
3. Develop an index of the contractual requirements, identified them as “C#” in “ID” column.
4. Fulfil the below table in order to identify implications for security management of those external requirements.
5. Review and approval by the Steering Committee.

ID	Organization	Supporting document	Type of relationship	Implications for security management
C1.	UNIDE-ISCTE, Unidade de Investigação em Desenvolvimento Empresarial	Memorandum of Understanding	Funding for projects and activities.	None
C2.	DCTI-ISCTE, Departamento de Ciências e Tecnologias de Informação do ISCTE	Memorandum of Understanding		None
C3.	European Commission	Memorandum of Understanding for each project	Service delivery	Availability of reports for 4 years, confidentiality of results)
C4.	FCT	Memorandum of Understanding for each project	Service delivery	Availability of reports for 4 years, confidentiality of results)
C5.	Câmara Municipal de Lisboa	Memorandum of Understanding	Research partner in a project to develop a multimedia game.	None
C6.	Hospital Garcia da Orta – cardiology service	Memorandum of Understanding	Research partner in a project to develop an imaginology system.	- The usage of medical data of actual patients for the development and tests of the system must comply with the applicable legislation. - The development of the system must include as system’s requirements the legal requisites applicable to medical data.
C7.	Instituto de Ciências Sociais, ICS	Memorandum of Understanding	Service delivery (ICS provided consultancy services for the organization and management of a networking internal project.)	None
C8.	Faculdade de Belas Artes da Universidade de Lisboa (Faculty of Arts of the Lisbon University)	Memorandum of Understanding	Service delivery (Faculdade de Belas Artes provided consultancy services for the organization and management of a networking internal project.)	None
C9.	EIA - Ensino, Investigação e Administração, S. A., (Universidade Atlântica) – Atlântica University	Memorandum of Understanding	Partner	Sharing of information about projects

ID	Organization	Supporting document	Type of relationship	Implications for security management
C10.	Accountant	Service delivery contract	Contracted supplier	None
C11.	Legal counselling	Service delivery contract	Contracted supplier	None
C12.	Telephone service	Service delivery contract	Contracted supplier	Maintain confidentiality and availability of telephone communications. The integrity of telephone equipment is ensured by contract.
C13.	IT service	Service delivery contract	Contracted supplier [an technician with service delivery contract “avença”]	Maintain confidentiality of IT configuration data of ADETTI and of any information with business value. Ensure the correct functioning of IT equipment.
C14.	Courier	Service delivery contract	Contracted supplier	Confidentiality and integrity of documents, availability of the service.

4. Develop an asset register

4.1 Requirements

Inputs		Practices and techniques	Outputs
T04.1	• Existing inventories in the organization • Types of records for the asset register (taken from ISO) • Asset taxonomy (taken from ISO) • Scope definition (T02.1) Business and legal requirements (T03.1)	• Records categories of the register • Taxonomy of assets • Asset evaluation formula • Asset identification criteria	• Asset inventory structure (T04.1) • Asset inventory completed (T04.2)

4.2 Asset inventory structure (T04.1)

The configuration of the asset register was defined considering the guidelines of ISO and available registers in literature [BSI03a], [AEXIS04].

The recommendations of ISO were inspiring source of:

a) The type of records used to identify assets (asset name, description location and asset owner).
b) The asset taxonomy employed (physical assets, information assets, software assets and services).
c) The employment of the CIA dimensions to measure the asset value.

From the literature review, it was drawn (1) the need to justify the numerical classifications given [BSI03a], [AEXIS04], (2) the idea of using a qualitative scale of five levels in order to represent the asset value - inspired by GMITS [ISO98] (*cf*. A.3.2.2 b) - and (3) measurement the assets, a part from the CIA factors, could include also a business impact factor [AEXIS04].

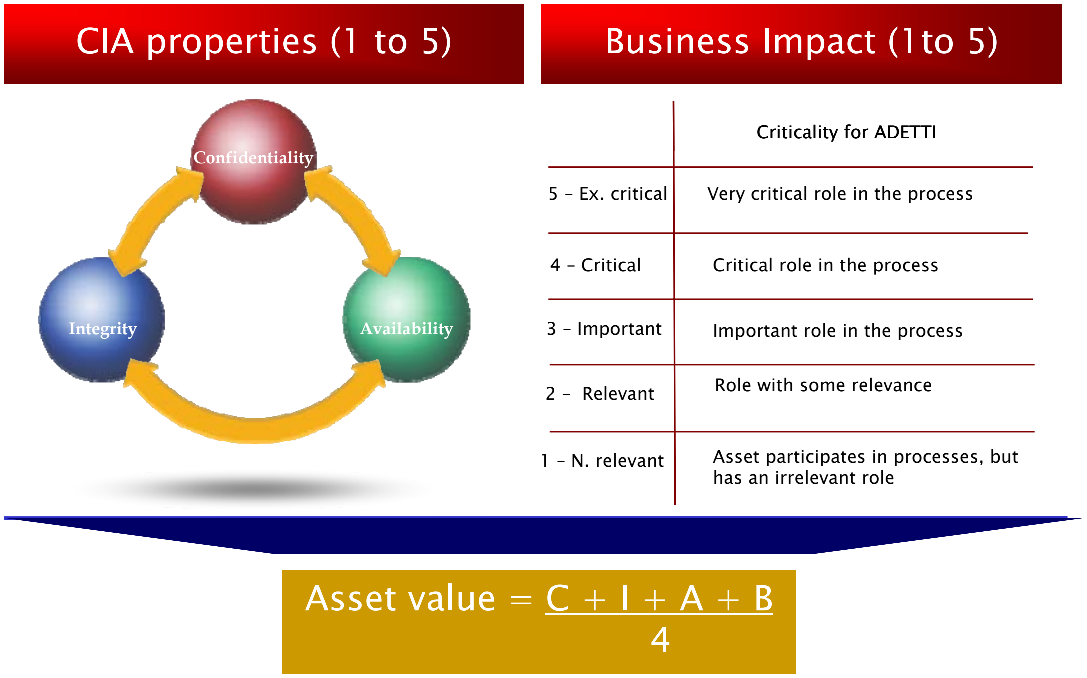
The combination of these two influences - ISO and literature review - with the concern to align the all steps of the present methodology with the business and legal requirements of ADETTI (*cf*. 5.4), lead to the adoption of a business factor in the asset evaluation formula.

The Steering Committee decided that although each of the CIA dimensions incorporates in itself business relevance, (for example, the level of confidentiality of a document depends of the level of business impact caused by a possible lack of it), it was considered better to include a factor of business impact in the asset evaluation.

It was deemed that isolating the asset evaluation within the information security properties could deprive the estimated asset value from concerns which may be not accurately reflected in the mentioned CIA dimensions. As examples it was referenced the legal requirements, in particularly the personal data protection legislation, which places specific requisites not entirely contemplated in the confidentiality aspect.

As a result, it was decided to employ an asset evaluation formula based on the CIA dimensions and "pure" business relevance. The preceding factor depicts the business and legal requirement in criticality scale of 1 to 5. The resulting values of the four classifications are divided by 4 to ensure that the final asset value reproduces the average value from all the different four aspects.

An illustration of the asset value equation is depicted in Figure R.7.



CIA properties (1 to 5)

Business Impact (1to 5)

	Criticality for ADETTI
5 - Ex. critical	Very critical role in the process
4 - Critical	Critical role in the process
3 - Important	Important role in the process
2 - Relevant	Role with some relevance
1 - N. relevant	Asset participates in processes, but has an irrelevant role

$$\text{Asset value} = \frac{C + I + A + B}{4}$$

Figure R.7: Asset value formula

To help in the asset evaluation, a description for each degree was composed by the author (descriptions were based on [AEXIS04] and [BSI03a]) and approved by the Steering Committee, as shown next.

a) Confidentiality classification

Value	Description
5 – Very high	Information, information processing facilities and system resources that are labelled as "extremely confidential". This asset should only be accessed by specific personnel authorised by top management and strictly on need to know basis. The impact of anybody unauthorised accessing this asset would be very serious.
4 – High	Information, information processing facilities and system resources that are labelled as "confidential". This asset should only be accessed by specific personnel. The impact of unauthorised access can be serious.
3 – Medium high	This classification relates to all information, information processing facilities and system resources that is restricted to ADETTI staff. The impact of anybody unauthorised accessing this asset can be noticeable, and should be avoided.
2 – Medium low	This confidentiality level relates to all information, information processing facilities and system resources that can be accessed by any member of the ADETTI staff and by partners involved in research projects in which that asset may be required. The impact of anybody unauthorised accessing this asset is minor.
1 – Low	This confidentiality degree applies to open information, information processing facilities and system resources, i.e. information that is freely accessible by anybody. An example for this is the information on the Web site of ADETTI.

b) Integrity classification

Value	Description
5 – Very high	This integrity status is employed for assets where integrity is extremely important, and should be maintained under all circumstances. For this asset, the loss of integrity has very serious or total failure of processes under the ISMS scope, and should be strongly protected against.
4 – High	This integrity status is employed for all information, information processing facilities and system resources where integrity is very important, and should be maintained under all circumstances. For this asset, the loss of integrity has serious negative influence on the ISMS scope, and should be strongly protected against.
3 – Medium high	This integrity level is used for the resources in where integrity is important, and should be maintained. For this asset, the loss of integrity has noticeable influence on the ISMS scope, and should be protected against.
2 – Medium low	This integrity level is used for all information, information processing facilities and system resources where integrity is not very important, but should generally be maintained. For this asset, the loss of integrity has some minor influence on the ISMS scope.
1 – Low	This integrity level is used for all assets with negligible impact on the ISMS scope.

c) Availability classification

Value	Description
5 – Very high	This availability level is used for all information, information processing facilities and system resources which should be available immediately on demand, and unavailability of the asset would cause serious impact on the ISMS scope.
4 – High	This availability level is used for all information, information processing facilities and system resources which should be available within few hours (less than 4), and unavailability of the asset would cause noticeable impact on the ISMS scope.
3 – Medium high	This availability level is used for all information, information processing facilities and system resources which should be available within a working day, and unavailability of the asset would cause noticeable impact on the ISMS scope.
2 – Medium low	This availability level is used for all information, information processing facilities and system resources which should be available within a 48 business hours, and unavailability of the asset would cause some minor impact on the ISMS scope.
1 – Low	This availability level is used for all information, information processing facilities and system resources where availability is not critical, and it is sufficient for this asset to available within 72 business hours.

d) Criticality classification (business impact)

Value	Description
5 – Extremely critical	The asset has a very critical role in the process or is critical for compliance with a law.
4 – Critical	The asset has a critical role in the process and/or some legal requisites are applicable..
3 – Important	The asset has an important role in the process and/or some legal requisites are applicable.
2 – Relevant	The asset has a relevant role in the process relevance and/or some legal requisites are applicable.
1 – Not relevant	The asset participates in business processes, but has an irrelevant role in the process.

4.3 Asset inventory completed (T04.2)

For the identification of assets in ADETTI it was employed:

a) An outdated register of IT systems and software licenses was found in [ADETTI2002]. This register was used as a guideline to inventory those types of assets.
b) Data collected from the scope definition (T02.1).
c) Business and legal requirements (T03.1).

Due to the restricted size of the selected scope, it was possible to consider each resource as a separate asset in terms of asset identification criteria (*cf*. 5.8.1). The application of this principle has lead to the identification of 35 assets, categorised by the four asset types.

In the inventory of IT systems, the hardware, operating system and applications were grouped together in the same asset; but the data supported by the IT system was regarded as another asset.

For each asset, it was identified an “asset owner”, that is an employee who works or is responsible for that asset. This allocation of responsibilities was performed by the Steering Committee.

Asset code	**Asset general data**				**Asset evaluation**							
	Asset name	**Description**	**Location**	**Owner**	**CIA requirements**	**Legal requirements**	**Business requirements**	**C**	**I**	**A**	**B**	**T**
Physical assets81												
PA001	Ad room	Room where the Administrative Unit works; location of process	ISCTE	AUM	Ad room has a very high availability requirement, because all working processes are carrying out in that room. Other security requirements are not applicable.	Compliance with L7.1, in terms of building safety, is ensured by ISCTE	Any problem with this room may have a significant impact.	1	1	5	5	3
PA002	File cabinets	Physical storage of documents	Ad room	AUE1	The file cabinets are instrumental to ensure the confidentiality and integrity of the report's documents. It was assessed the CIA requisites of the access control mechanism (key).	No direct requisite over this asset.	The storage performed by the asset is relevant.	3	3	1	3	3
PA003	Desktop AUE1	Employee01 desktop, processes accounting data (IP address: 10.10.96.137)	Ad room	AUE1	Desktop with no confidential requirement itself, but which processes and stores critical financial data, therefore integrity and availability is required.	- Compliance with L2.4, L4.1	This desktop inherits some of the relevance of the data which he supports.	1	5	4	4	4
PA004	Desktop AUE2	Working station that belongs to AUE2 (IP: 10.10.96.211)	Ad room	AUE2	This desktop does not usually processes financial data.	- Compliance with L2.4, L4.1	Desktops are systems that support most of work of the ADU.	1	5	4	3	4
PA005	DesktopAUM	Desktop of AUM (IP: 10.10.96.198)	Ad room	AUM	Desktop essential for financial data processing. CIA requirements inherit the attributes of this information type.	- Compliance with L2.4, L4.1	Desktops are systems that support most of work of the ADU.	1	5	4	5	4
PA006	ServerRSI	Domain controller of Windows network. (IP: 10.10.96.7)	Ad room	AUM	Confidentiality and integrity of the account database (Active Directory) are relevant. Server unavailability can be overcome by alternative means of sharing data.	- Compliance with L4.1	Not essential for electronic information sharing.	4	4	4	4	4
PA007	ServerBSCW	Includes operating system and applications that supports the BSCW database. (IP: 193.136.190.51)	Multi lab	AUM	This server holds the BSCW database, which is the electronic repository of project information. Consequently, the service provided by this server is considered extremely important for ADETTI.	- Compliance with L4.1 and L8.	The availability and correct operation of the web interface of BSCW is needed to increase the interaction with the research partners.	5	5	5	5	5

PA008	SwitchCISCO	Cisco 2950 – 48 ports 10/100 Mbps switch	Ad room	AUM	The switch availability is relevant, however it can be overcome by alternative means of sharing data.	- Compliance with L7.1	Equipment easily replaced.	2	4	4	2	3
PA009	Backup cartridges	Tape DLT	Multi lab	AUM	Confidentiality and integrity is relevant.	- Compliance with L6.1 and L8.1	Some cartridges are relevant (projects), others not.	5	5	3	4	4
PA010	Fax machine	Panasonic Laser KX-FL501 – fax machine connected to an analogue line	Ad room	AUE1	Availability and integrity of the fax are important. The equipment holds no data with business value.	- Compliance with L7.1	Not essential.	2	5	5	4	4
PA011	PrinterRicoh	Ricoh Aficio 1515	Ad room	AUM	Problems with availability and integrity can be easily fixed – due to existing other printers and verification of printing output by employees.	- Compliance with L7.1	Printer related to accounting process	3	3	3	4	3
PA012	Printer LaserJet	HP Colour Laserjet 4600dn	Ad room	AUM	Problems with availability and integrity can be easily fixed – due to existing other printers and verification of printing output by employees. No confidential requisite.	- Compliance with L7.1	Printer related to accounting process	1	3	3	4	3
PA013	Printer Lexmark	Lexmark Optra T612	Ad room	AUM	Problems with availability and integrity can be easily fixed – due to existing other printers and verification of printing output by employees. No confidential requisite.	- Compliance with L7.1	Not used for the accounting process	1	3	3	3	3
PA014	PBXSiemens	Siemens Hicom 150E OfficePoint	Ad room	AUM	Availability and integrity of the system are important. No confidential requisite.	- Compliance with L7.1	Essential for voice communication.	1	4	4	4	3
PA015	Data and voice cabling	Structured cabling Category 5 Enhanced	ISCTE	ITT	Availability and integrity of the data and voice communication is important.	Not applicable	Essential for data communication.	3	5	5	4	4
PA016	ADETTI stamp	Official stamp	Ad room	AUE1	Availability is the only applicable requirement.	Not applicable	Certification of documentation	1	1	2	2	2
PA017	Office furniture	Desk, chairs and other office furniture	Ad room	AUE1	Availability is the only applicable requirement.	- Compliance with L7.1	Important for working conditions	1	1	2	2	2
Information assets												
IA001	User and computers database	Microsoft Active Directory	Ad room	ITT	The repository of computer accounts stores user's passwords and authorizes domains authentications.	No requisite.	Without domain authentication, users can work locally.	4	3	4	2	3
IA002	System documentation	Software licenses and technical manuals	Ad room	ITT	System documentation should be available only internally, integrity and availability is high because lack of these requirements can aggravate a system breakdown.	- Compliance with L4.1	Failure to maintain a record of license may result in fines.	2	4	4	3	3
IA003	ISMS documentation	Files and database with financial data	Ad room	ADM	It is important that the ISMS documents are available.	- Compliance with L6.1	Identified as a key issued needed improvement – B1	3	2	4	3	3

IA004	Current project's accountability	Files and database with financial data	Ad room	ADM	The integrity and availability in financial data is more important than confidentiality.	- Compliance with L6.1	Identified as a key issued needed improvement – B1	3	5	5	5	5
IA005	Contracts related to research projects	Funding contracts, etc.	Ad room	ADM	All contracts are managed by the ADU, Executive Commission and project leaders. Other staff can only view them with a specific authorisation. The integrity and availability of contracts is required by funding organizations.	- Compliance with L6.1		3	5	5	5	5
IA006	Projects documentations	Produced reports and other documents associated with research projects	Ad room	ADM	These documents have a critical value in terms of CIA. This includes all documents of closed projects and non financial data of current projects.	- Compliance with L6.1	Deliverables of the research activities (the business of ADETTI).	5	5	5	5	5
IA007	Employees personal data	Data, which according to CNPD, must be protected.	Ad room	ADM	The CIA requirements for these documents are high.	- Compliance with L6.1	This data must be protected.	4	4	2	4	4
IA008	Internal documentation	Examples are the Annual Report. Correspondence.	Ad room	ADM	The CIA requirements for these documents are medium.	- Compliance with L6.1		3	3	3	4	3
Services												
SC001	Electrical power	Provided by ISCTE (external source: EDP)	NA	AUE2	As a stable and continuous provision of electrical power is critical for the process, therefore the availability and integrity of the electrical service is critical; confidentiality is not applicable.	- Application of C2	Without electrical power, operations stops.	1	5	5	5	4
SC002	Air conditioning	Two air conditioning equipments	Ad room	AUE2	Availability of the air conditioning service helps to maintain systems and personnel working.	NA	Not relevant.	1	1	3	2	1
SC003	Internet access	Direct provider: ISCTE (which is supported by FCCN)	NA	AUM	The integrity and availability is more important than the confidentiality of Internet traffic (does not include SMTP traffic).	- Application of C2	Without Internet, operations can be carryout.	3	5	5	4	3
SC004	Telephone service (TDM operator)	Provider: PT Comunicações	Multi lab	AUE2	Financial data is not, usually, transmitted by phone. However, this is an alternative mean for the ADU communicate with projects leaders and submit financial report to the funding organizations.	- Application of C12	"Without phone, we do not exist"	4	4	5	5	4
SC005	SMTP service	Provider: ISCTE	ISCTE	NA	Availability and integrity of the mail service are critical for the ADU to communicate with projects leaders. The service availability involves access to backbone of FCCN.	- Application of C.2	Any problem can cause a significant impact.	4	5	5	5	5
SC006	IT service	Provider:	Ad room	AUE2		- Application of C13		5	5	5	4	5

SC007	Courier		Ad room	AUE1	This service must be available and maintain integrity and confidentiality of documentation.	- Application of C14		4	5	5	4	5
Human resources												
HA001	AUM	Administrative Unit Manager	Ad room	NA	AUM must be available and assure the integrity of the data deal with. Confidentiality is not very relevant for the financial data handled in this process.	L1.1 - Labour Code L2. - Personal data protection L3. Computer crimes legislation	This employee manages the overall financial process.	3	5	5	5	5
HA002	AUE1	Administrative Unit Employee 1	Ad room	NA	Availability is critical, confidentiality and integrity are not.	L1.1 - Labour Code L2. - Personal data protection L3. Computer crimes legislation	AUE1 operates an essential part of the process.	3	5	5	5	5
HA003	AUE2	Administrative Unit Employee 2	Ad room	NA	Availability is critical, confidentiality and integrity are not.	L1.1 - Labour Code L2. - Personal data protection L3. Computer crimes legislation	AUE2, sometimes, assists the other employees in the process.	3	5	3	5	4

5. Conduct risk management

5.1 Requirements

Inputs		Practices and techniques	Output(s)
T05.1	• Asset evaluation scale (from T04.2)	• Monetary or non-monetary formula • Probability estimation type • Impact level definition • Probability level definition	• Risk calculation formula
T05.2	• Risk calculation formula (from T05.1)	• Identify threats • Identify vulnerabilities • Estimate risks	• List of identified risks
T05.3	• List of identified risks	• Define the risk acceptance criteria	• Risk acceptance criteria
T05.4	• List of identified risks • Risk acceptance criteria	• Identify the treatment strategy • Identify the applicable controls from ISO	• Risk Treatment Plan

5.2 Risk calculation formula (T05.1)

The Steering Committee decided that risk would be calculated using a formula employing a non-monetary approach (*cf*. 3.4.4 in the dissertation text). From the several non-monetary risk formulas, discussed in Annex A.3.2.2, it was selected the risk equation with 3 variables and a numerical output (from GMITS). The selected risk algorithm correlates three ingredients: (1) probability, (2) impact and (3) the asset value.

The Steering Committee considered that a risk with three factors could represent better the risks than a two factors formula. In fact, it was conceived that in the formulas with two factors, usually probability and impact/severity, the last factor – impact – would be better characterized if decomposed in the asset value and the severity caused by the “risk action”.

It was argued that in a two factors formula, the impact of a risk is evaluated in terms of the loss for the business caused by the risk, and not regarding the consequences in the asset itself (a risk that causes the destruction of an asset with a minor value is deemed as lower than one that just causes a minor failure in a asset with a high business relevance). Oppositely, in a three factors formula the business perspective is applied through the asset value, permitting that the impact is assessed based on the negative effects of the risk on the asset itself.

The resulting risk equation multiples the asset value (1 to 5), with probability (1 to 5) and with impact (1 to 5). The first item is an outcome of the previous phase (T04.2), the second is estimated based on a combination of variables (*cf*. Annex A.6.2.2) and the last gauges the possible negative consequences on the business and the protection of the financial process in ADETTI of the risk occurring.

In order to mitigate the subjectivity of those classifications, each numerical level was associated with a description, which was adapted from [AEXIS04], [BSI03a] and from the description adopted to describe the asset value (exposed in 4.2).

Impact

Level	Description	Impact on the business	Impact on the legal requirements	Impact on the information security properties		
				Confidentiality	Integrity	Availability
5	Very high	Risk most probably will cause an serious interruption or degradation of the business process (e.g. a funding organization cancelling a project)	Serious punitive measurement and litigation expected or certain	Any unauthorised access will cause an serious impact	Any data corruption will cause an serious impact	Serious impact of unavailability (e.g. any permanent loss of service)
4	High	Risk can cause an minor interruption or degradation of the business process	Minor punitive measurement and litigation expected or certain	Any unauthorised access will cause an minor impact	Any data corruption will cause an minor impact	Any unavailability will cause an minor impact
3	Medium high	The risk can indirectly cause a degradation of the business process.	Litigation possible but not certain. Potential for punitive measurement.	Any unauthorised access will cause negative consequences	Any data corruption will cause negative consequences	Noticeable impact of unavailability. It should be available within a 24 business hours.
2	Medium low	Minimal risk for ADETTI	Litigation unlikely. No punitive measurement.	Failure to meet legal obligations that may result in a departmental embarrassment	Data corruption with minimal impact	Unavailability would cause some minor impact. It should be available within a 48 business hours.
1	Low	No risk for ADETTI	Unlikely to cause litigation or any punitive measurement (as fines)	Failure to meet legal obligations that may result in a individual member of staff embarrassment	Minor data corruption with no risks	Not critical, it can be available within 72 business hours.

Probability

How likely is it that an incident could occur, taking account of the controls in place and their adequacy

5	Almost certain	Likely to occur with some frequency
4	Likely	Will probably occur
3	Possible	Do not expect it to happen but it is possible
2	Unlikely	May occur occasionally
1	Rare	Can’t believe that this will ever happen

5.3 List of identified risks

Following the BSI recommendations, threats and vulnerabilities were identified sequentially (*cf*. 3.5.2). Nevertheless, both processes were performed at the same time, because during the detection of vulnerabilities new threats were found and vice versa.

5.3.1 Identification of threats

Several methods can be employed to identify threats, as discussed in 3.5.4 in the dissertation text.

In ADETTI in order to minimize the resource's usage it was adopted the threat catalogue approach. Based on the literature review made it was adapted to the reality of ADETTI the list of threats from Gillingham [03].

Each threat agent from the list of Gillingham [03] was assessed by employees and manager of the Administrative Unit [as approved by the Steering Committee] based on the proximity, motivation and skills to perform risks. Afterwards, a group of applicable threat agent was divided according to the proximity criteria, as shown in column "perimeter" in the next table. The motivation and skills criteria were evaluated with a scale of 1 to 5.

Perimeter	Threat agent	Motivation	Skills	Observation	Overall level of threat
Internet	Hackers	3	5	Some of ADETTI competitors – other R&D organizations or individual researchers – are very proficient in network intrusion techniques, but they could lack the motive for engaging in illegal or unethical actions.	3
	Malicious code	Not applicable	4	The capacity of malicious code is constantly being upgraded.	3
ISCTE campus	Environmental threats	Not applicable	4	The area where ADETTI is located can suffer earthquakes and aviation accidents.	2
	Civil unrest	2	3	Strikes of the ISCTE employees or other civil service employees can impact on ADETTI.	2
	Discontent student	3	3	ADETTI is within a university campus, so student protest can impact ADETTI activities.	2
ADETTI	Absent mind Administrative Unit employee	Not applicable	3	Employees can perform unintentional actions that cause risks.	3
	Discontent Administrative Unit employee	1	4	Employees can perform intentional actions that cause risks.	4

5.3.2 Identification of vulnerabilities

As explained in Annex A.5.2, fragilities in IT assets were identified by electronic tools and vulnerabilities in other types of assets through the application of audit frameworks. Therefore, vulnerabilities in IT equipment were collected previously in the scope description phase (in 2.3.5.2), as for the general vulnerabilities they were verified by the application of the following audit framework.

a) Exiting security management practices and controls

Following the instructions of 5.9 in the dissertation text, security management practices and controls were collected by the following table. In the following table the rows in green are regarded as the recommended by ISO (*cf.* 3.8.3). In this audit, it was employed a conformity scale of four values:

0 – requirement not applicable for the scope under analysis;
1 – the practice or safeguard mechanism recommended by ISO is not found in ADETTI;
2 - the existing practice in ADETTI is, in some way, abides by the BSI standard;
3 - the existing practice in ADETTI abides by the BSI standard.

The data which supports this audit was collected through a questionnaire (applied to the Administrative Office employees) and several observations.

N.	Clause	Normative requirement	Existing practice/control	Conformity
A.3 Security policy				
A.3.1 Information security policy Control objective: To provide management direction and support for information security.				
A.3.1.1	Information security policy document	A policy document shall be approved by management, published and communicated, as appropriate, to all employees.	Inexistence of formal security norms. Some guidelines concerning the protection of facilities, equipment and some specific information were defined, but not in a written format.	1
A.3.1.2	Review and evaluation	The policy shall be reviewed regularly, and in case of influencing changes, to ensure it remains appropriate	No procedure to update security norms.	1

A.4 Organizational security				
A.4.1 Information security infrastructure Control objective: To manage information security within the organization.				
A.4.1.1	Management information security forum	A management forum to ensure that there is clear direction and visible management support for security initiatives shall be in place. The management forum shall promote security through appropriate commitment and adequate resourcing.	There is no management forum to support information security management.	1
A.4.1.2	Information security coordination	In large organizations, a cross-functional forum of management representatives from relevant parts of the organization shall be used to coordinate the implementation of information security controls.	There is no management coordination function for information security management.	1
A.4.1.3	Allocation of information security responsibilities	Responsibilities for the protection of individual assets and for carrying out specific security processes shall be clearly defined.	Inexistence of a formal security management with defined responsibilities. It was found some evidences of ad-hoc security processes carry out by the IT department (e.g. malicious code protection).	2
A.4.1.4	Authorization process for information processing facilities	A management authorization process for new information processing facilities shall be established.	No practice or procedure was found.	1
A.4.1.5	Specialist information security advice	Specialist advice on information security shall be sought from either internal or external advisors and coordinated throughout the organization.	ADETTI benefits from the expertise of its researchers, both on the management and the technological aspects of security – as defined in the SWOT analysis.	3
A.4.1.6	Cooperation between organizations	Appropriate contacts with law enforcement authorities, regulatory bodies, information service providers and telecommunications operators shall be maintained.	ADETTI maintains contacts, which can be used for security cooperation, with ISCTE and Portugal Telecom (voice communication provider). The Internet provider of ADETTI - Fundação para a Computação Científica Nacional is establishing a Computer Emergency Response Team for its clients (ISCTE is a client of FCCN, ADETTI uses the Internet gateway of ISCTE).	3
A.4.1.7	Independent review of information security	The implementation of the information security policy shall be reviewed independently.	Information security of ADETTI is not reviewed by an independent auditor (according to ISO/IEC 19011 an auditor can not audit his own work).	1
A.4.2 Security of third-party access Control objective: To maintain the security of organizational information processing facilities and information assets accessed by third parties.				

A.4.2.1	Identification of risks from third-party access	The risks associated with access to organizational information processing facilities by third parties shall be assessed and appropriate security controls implemented.	No practice or procedure was found.	1
A.4.2.2	Security requirements in third-party contracts	Arrangements involving third-party access to organizational information processing facilities shall be based on a formal contract containing all necessary security requirements.	No practice or procedure was found.	1
A.4.3 Outsourcing Control objective: To maintain the security of information when the responsibility for information processing has been outsourced to another organization.				
A.4.3.1	Security requirements in outsourcing contracts	The security requirements of an organization outsourcing the management and control of all or some of its information systems, networks and/or desktop environments shall be addressed in a contract agreed between the parties.	No practice or procedure was found.	1
A.5 Asset classification and control				
A.5.1 Accountability for assets Control objective: To maintain appropriate protection of organizational assets.				
A.5.1.1	Inventory of assets	An inventory of all important assets associated with each information system shall be drawn up and maintained.	A register of IT systems (as servers, desktops, laptops, communication devices among others) exists. Other types of assets associated with information systems as file cabinet are not inventoried.	2
A.5.2 Information classification Control objective: To ensure that information assets receive an appropriate level of protection.				
A.5.2.1	Classification guidelines	Classifications and associated protective controls for information shall take account of business needs for sharing or restricting information, and the business impacts associated with such needs.	There is no information classification procedure in ADETTI. Nevertheless: - an application (a macro for MSF Word) is being developed that would allow the security classification of electronic documents; - information related to projects is maintained in a user restricted file systems (BSCW software) and kept in a closed file cabinet.	1
A.5.2.2	Information labelling and handling	A set of procedures shall be defined for information labelling and handling in accordance with the classification scheme adopted by the organization.	There is no information classification procedure in ADETTI.	1
A.6 Personnel security				
A.6.1 Security in job definition and resourcing Control objective: To reduce the risks of human error, theft, fraud or misuse of facilities.				

A.6.1.1	Including security in job responsibilities	Security roles and responsibilities, as laid down in the organization's information security policy shall be documented in job definitions.	Job descriptions did not include - explicitly - security responsibilities.	1
A.6.1.2	Personnel screening and policy	Verification checks on permanent staff, contractors and temporary staff shall be carried out at the time of job applications.	No verification of credentials was performed.	1
A.6.1.3	Confidentiality agreements	Employees shall sign a confidentiality agreement as part of their initial terms and conditions of employment.	There is no confidentiality agreement.	1
A.6.1.4	Terms and conditions of employment	The terms and conditions of employment shall state the employee's responsibility for information security.	Not found in ADETTI.	1
A.6.2 User training Control objective: To ensure that users are aware of information security threats and concerns, and are equipped to support organizational security policy in the course of their normal work.				
A.6.2.1	Information security education and training	All employees of the organization and, where relevant, third-party users, shall receive appropriate training and regular updates in organizational policies and procedures.	ADU members have participate in internal meetings were security issues were discussed. However never has a specific session to train and raise awareness for information security.	2
A.6.3 Responding to security incidents and malfunctions Control objective: To minimize the damage from security incidents and malfunctions, and to monitor and learn from such incidents.				
A.6.3.1	Reporting security incidents	Security incidents shall be reported through appropriate management channels as quickly as possible.	Reporting of IT incidents is well established. This is not the case for security incidents of other sources.	2
A.6.3.2	Reporting security weaknesses	Users of information services shall be required to note and report any observed or suspected security weaknesses in, or threats to, systems or services.	Reporting of security weaknesses related with IT system is defined. For the remaining categories of security weaknesses, no practice was found.	2
A.6.3.3	Reporting software malfunctions	Procedures shall be established for reporting software malfunctions.	Inexistent.	1
A.6.3.4	Learning from incidents	Mechanisms shall be put in place to enable the types, volumes and costs of incidents and malfunctions to be quantified and monitored.	Inexistent.	1
A.6.3.5	Disciplinary process	The violation of organizational security policies and procedures by employees shall be dealt with through a formal disciplinary process.	The disciplinary process is not defined. In situation of an allegedly grave violation of a work instruction, ADETTI may apply the general procedures for disciplinary process defined in the Portuguese Labour Code.	2
A.7 Physical and environmental security				

A.7.1 Secure areas Control objective: To prevent unauthorized physical access, damage and interference to business premises and information.				
A.7.1.1	Physical security perimeter	Organizations shall use security perimeters to protect areas that contain information processing facilities.	The working areas in the ISCTE building which are under the scope of the ISMS are protected by security perimeters. The office room of the Administrative Unit (ADU) is isolated by a door from the rest of ADETTI office. The office is separated by a door, which remains closed, from the other areas of the ISCTE building. The ISCTE compound has surveillance guards at his entrances. The working areas of the project are also isolated from outside. The mail server is protected in the ISCTE datacenter.	3
A.7.1.2	Physical entry controls	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	The entrance in ISCTE compound is guarded by surveillance officers. The ADETTI office has a door which the lock is given only to authorised personnel. The lock of the ADU room is provided only to the ADU staff. Neither at ISCTE or ADETTI entrance there is an identification, registration or traceability mechanism for visitors.	2
A.7.1.3	Securing offices, rooms and facilities	Secure areas shall be created in order to protect offices, rooms and facilities with special security requirements.	The ADU room is subjected to the constant surveillance of the staff that works here. Every time the last staff member exits the room, it closes it down. However this room is not physically separated from the visitor's area.	2
A.7.1.4	Working in secure areas	Additional controls and guidelines for working in secure areas shall be used to enhance the security of secure areas.	Personnel follow informal guidelines of maintaining documents away from the desk ("clean desk") and locked, if necessary.	2
A.7.1.5	Isolated delivery and loading areas	Delivery and loading areas shall be controlled, and where possible, isolated from information processing facilities to avoid unauthorized access.	A part of the ADU room functions as the reception of the organization, therefore there is frequent visitors in this part of the room. The working desks are isolated from this area and the file cabinets are closed.	1
A.7.2 Equipment security Control objective: To prevent loss, damage or compromise of assets and interruption to business activities.				
A.7.2.1	Equipment siting and protection	Equipment shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.	In the ADU room, assets are sited in order to separate them from visitors (see A.7.1.5) and therefore minimize the risk of theft. However this measure is regarded as not very effective.	2

A.7.2.2	Power supplies	Equipment shall be protected from power failures and other electrical anomalies.	All the desktops of the ADU and associated servers have line interactive Uninterruptible Power Supply (UPS). An line interactive Uninterruptible Power Supply incorporates an automatic voltage regulator that filters powers surges or brownout a part from allowing a graceful shut down, in case of power interruption. From the nine common power problems that UPS units are used to correct, these models are capable of handling four of those, which are: power failure, power sag, power surge (spike) and under-voltage (brownout). Problems not handled: over-voltage (increased voltages for an extended period of time), line noise (distortions superimposed on the power waveform), frequency (variation of the power waveform), switching transient (under-voltage or over-voltage for up to a few nanoseconds), harmonic distortion (multiples of power frequency superimposed on the power waveform) [Wikipedia04]).	2
A.7.2.3	Cabling security	Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage.	ADETTI´s network shares the cabling infrastructure of ISCTE. By default, all ports are physically connected and do not require authentication. There are no redundant cables between ADETTI systems and the remaining infrastructure.	1
A.7.2.4	Equipment maintenance	Equipment shall be correctly maintained to enable its continued availability and integrity.	Desktops, printers and fax are repaired by an IT service provider, under a maintenance contract. Laptops are return to factory. There are records of repairs and maintenance service provided to IT systems.	3
A.7.2.5	Security of equipment off-premises	Any use of equipment for information processing outside an organization's premises shall require authorization by management.	Management authorizes informally the removal of equipment. There is no written procedure or records of these actions.	2
A.7.2.6	Secure disposal or re-use of equipment	Information shall be erased from equipment prior to disposal or re-use.	Before computers are removed to repair, disposal or another user, the folders created by its existing user are deleted, using the operating system file system.	3
A.7.3 General controls Control objective: To prevent compromise or theft of information and information processing facilities.				
A.7.3.1	Clear desk and clear screen policy	Organizations shall have a clear desk and a clear screen policy aimed at reducing the risks of unauthorized access, loss of, and damage to information.	ADU staff locks their sessions before leaving the desktop. A schedule screensaver lock guarantees the unavailability of the system every time.	3
A.7.3.2	Removal of property	Equipment, information or software belonging to the organization shall not be removed without authorization of the management.	Management is said to supervise and approve - informally - the removal of assets.	3

A.8 Communications and operations management				
A.8.1 Operational procedures and responsibilities Control objective: To ensure the correct and secure operation of information processing facilities.				
A.8.1.1	Documented operating procedures	The operating procedures identified in the security policy shall be documented and maintained.	There is no documented policy, operating procedures or written job instructions.	1
A.8.1.2	Operational change controls	Changes to information processing facilities and systems shall be controlled.	For the assets under the scope there are no change management practices.	1
A.8.1.3	Incident management procedures	Incident management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to security incidents and to collect incident related data such as audit trails and logs.	It was not found any incident management procedure.	1
A.8.1.4	Segregation of duties	Duties and areas of responsibility shall be segregated in order to reduce opportunities for unauthorized modification or misuse of information or services.	Evidences of segregation of duties were not found.	1
A.8.1.5	Separation of development and operational facilities	Development and testing facilities shall be separated from operational facilities. Rules for the migration of software from development to operational status shall be defined and documented.	Not applicable to the area under evaluation.	0
A.8.1.6	External facilities management	Prior to using external facilities management services, the risks shall be identified and appropriate controls agreed with the contractor, and incorporated into a contract.	It was not found any evidence of risk assessment or security clause in the memorandum of understating with ISCTE.	1
A.8.2 System planning and acceptance Control objective: To minimize the risk of systems failure.				
A.8.2.1	Capacity planning	Capacity demands shall be monitored and projections of future capacity requirements made to enable adequate processing power and storage to be made available.	Capacity assessment is performed regularly in the existing systems by the ADU members. All new systems are dimensioned in terms of expected capacity needs.	3
A.8.2.2	System acceptance	Acceptance criteria for new information systems, upgrades and new versions shall be established and suitable tests of the system carried out prior to acceptance.	Within the scope, there is no formal practice for system acceptance. Nevertheless, ADU manager said that the relevant features of systems are tested before a formal acceptance of the system.	2
A.8.3 Protection against malicious software Control objective: To protect the integrity of software and information from damage by malicious software.				

A.8.3.1	Controls against malicious software	Detection and prevention controls to protect against malicious software and appropriate user awareness procedures shall be implemented.	There is IT protection mechanisms against malicious software. Although the personnel reveal signs of understanding their role in the protection against malware, there are no records to show the awareness of staff in this field.	2
A.8.4 Housekeeping Control objective: To maintain the integrity and availability of information processing and communication services.				
A.8.4.1	Information back-up	Back-up copies of essential business information and software shall be taken and tested regularly.	Backups of the BCSW and raider servers are done weekly but not tested. Desktop backup is done every month.	2
A.8.4.2	Operator logs	Operational staff shall maintain a log of their activities. Operator logs shall be subject to regular, independent checks.	The operational activities performed by the ADU can be verified by numerous records. Nevertheless these logs are not audited as required by this clause.	2
A.8.4.3	Fault logging	Faults shall be reported and corrective action taken.	No evidence was found of fault logging.	1
A.8.5 Network management Control objective: To ensure the safeguarding of information in networks and the protection of the supporting infrastructure.				
A.8.5.1	Network controls	A range of controls shall be implemented to achieve and maintain security in networks.	The access to the ADU office network is filtered by a firewall (Caixa Magica ProGuard), but from ISCTE network (from the student desktops) it is possible to launch ICMP queries, which enables host identification. It would be advisable, for security reasons, to isolate the ADU network.	1
A.8.6 Media handling and security Control objective: To prevent damage to assets and interruptions to business activities.				
A.8.6.1	Management of removable computer media	The management of removable computer media, such as tapes, disks, cassettes and printed reports shall be controlled.	The cited items are not controlled.	1
A.8.6.2	Disposal of media	Media shall be disposed of securely and safely when no longer required.	The cited items are not controlled.	1
A.8.6.3	Information handling procedures	Procedures for the handling and storage of information shall be established in order to protect such information from unauthorized disclosure or misuse.	No procedure was found.	1
A.8.6.4	Security of system documentation	System documentation shall be protected from unauthorized access.	The cited items are not controlled.	1
A.8.7 Exchanges of information and software Control objective: To prevent loss, modification or misuse of information exchanged between organizations.				

A.8.7.1	Information and software exchange agreements	Agreements, some of which may be formal, shall be established for the exchange of information and software (whether electronic or manual) between organizations.	There is no a non disclosure agreement for organizations and persons which ADETTI shares confidential information.	1
A.8.7.2	Security of media in transit	Media being transported shall be protected from unauthorized access, misuse or corruption.	Not found.	1
A.8.7.3	Electronic commerce security	Electronic commerce shall be protected against fraudulent activity, contract dispute and disclosure or modification of information.	Not applicable.	0
A.8.7.4	Security of electronic mail	A policy for the use of electronic mail shall be developed and controls put in place to reduce security risks created by electronic mail.	Not found.	1
A.8.7.5	Security of electronic office systems	Policies and guidelines shall be prepared and implemented to control the business and security risks associated with electronic office systems.	Not found.	1
A.8.7.6	Publicly available systems	There shall be a formal authorization process before information is made publicly available and the integrity of such information shall be protected to prevent unauthorized modification.	Data in the web site is published according to a defined procedure (which is not written).	2
A.8.7.7	Other forms of information exchange	Policies, procedures and controls shall be in place to protect the exchange of information through the use of voice, facsimile and video communications facilities.	Inexistent.	1
A.9 Access control				
A.9.1 Business requirement for access control Control objective: To control access to information.				
A.9.1.1	Access control policy	Business requirements for access control shall be defined and documented, and access shall be restricted to what is defined in the access control policy.	Inexistent.	1
A.9.2 User access management Control objective: To ensure that access rights to information systems are appropriately authorized, allocated and maintained.				
A.9.2.1	User registration	There shall be a formal user registration and de-registration procedure for granting access to all multi-user information systems and services.	No formal procedure was found.	1
A.9.2.2	Privilege management	The allocation and use of privileges shall be restricted and controlled.	The allocation of privileges is controlled and the usage of privileges is uncontrolled.	1

A.9.2.3	User password management	The allocation of passwords shall be controlled through a formal management process.	No formal procedure to allocate passwords.	1
A.9.2.4	Review of user access rights	Management shall conduct a formal process at regular intervals to review users' access rights.	Not done.	1
A.9.3 User responsibilities Control objective: To prevent unauthorized user access.				
A.9.3.1	Password use	Users shall be required to follow good security practices in the selection and use of passwords.	Not found.	1
A.9.3.2	Unattended user equipment	Users shall be required to ensure that unattended equipment is given appropriate protection.	Personnel follow informal guidelines of protecting unattended user equipment	1
A.9.4 Network access control Control objective: Protection of networked services.				
A.9.4.1	Policy on use of network services	Users shall only have direct access to the services that they have been specifically authorized to use.	Not implemented. All physical ports are enabled and provide access to DHCP.	1
A.9.4.2	Enforced path	The path from the user terminal to the computer service shall be controlled.	Not implemented.	1
A.9.4.3	User authentication for external connections	Access by remote users shall be subject to authentication.	Yes. Data repositories are only accessible from the Internet through authentication. Systems employ Role-Based Access Control.	3
A.9.4.4	Node authentication	Connections to remote computer systems shall be authenticated.	Not implemented.	1
A.9.4.5	Remote diagnostic port protection	Access to diagnostic ports shall be securely controlled.	Not found.	1
A.9.4.6	Segregation in networks	Controls shall be introduced in networks to segregate groups of information services, users and information systems.	Not found.	1
A.9.4.7	Network connection control	The connection capability of users shall be restricted in shared networks, in accordance with the access control policy.	Not applied. Within the infrastructure, there is no traffic segregation.	1
A.9.4.8	Network routeing control	Shared networks shall have routeing controls to ensure that computer connections and information flows do not breach the access control policy of the business applications.	ADETTI infrastructure has a perimeter filtered by a firewall (gtadetti.adetti.pt). But the ADU network is not isolated from the remaining ADETTI network (as Caixa Magica Lab).	1
A.9.4.9	Security of network services	A clear description of the security attributes of all network services used by the organization shall be provided.	Such a description does not exist.	1

A.9.5 Operating system access control Control objective: To prevent unauthorized computer access.				
A.9.5.1	Automatic terminal identification	Automatic terminal identification shall be considered to authenticate connections to specific locations and to portable equipment.	Not implemented.	1
A.9.5.2	Terminal log-on procedures	Access to information services shall use a secure log-on process.	Not implemented.	2
A.9.5.3	User identification and authentication	All users shall have a unique identifier (user ID) for their personal and sole use so that activities can be traced to the responsible individual. A suitable authentication technique shall be chosen to substantiate the claimed identity of a user.	Authentication based on a single factor (User ID and password).	2
A.9.5.4	Password management system	Password management systems shall provide an effective, interactive facility which aims to ensure quality passwords.	The passwords of the Domain and BSCW server were not configured with an expiring date and not had not also a complexity baseline configured.	1
A.9.5.5	Use of system utilities	Use of system utility programs shall be restricted and tightly controlled.	Not implemented. The users have privileges of local administrator.	1
A.9.5.6	Duress alarm to safeguard users	Duress alarms shall be provided for users who might be the target of coercion.	Not implemented.	1
A.9.5.7	Terminal time-out	Inactive terminals in high risk locations or serving high risk systems shall shut down after a defined period of inactivity to prevent access by unauthorized persons.	Not implemented.	1
A.9.5.8	Limitation of connection time	Restrictions on connection times shall be used to provide additional security for high risk applications.	Not implemented.	1
A.9.6 Application access control Control objective: To prevent unauthorized access to information held in information systems.				
A.9.6.1	Information access restriction	Access to information and application system functions shall be restricted in accordance with the access control policy.	There is no formal access control policy. Permissions are granted in a "Need to Know" basis. For example only the ADU manager has administrator credentials in the BSCW software.	2
A.9.6.2	Sensitive system isolation	Sensitive systems shall have a dedicated (isolated) computing environment.	Systems support data with different sensitivities.	1
A.9.7 Monitoring system access and use Control objective: To detect unauthorized activities.				
A.9.7.1	Event logging	Audit logs recording exceptions and other security-relevant events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring.	Security incidents and events are not recorded.	1

A.9.7.2	Monitoring system use	Procedures for monitoring the use of information processing facilities shall be established and the result of the monitoring activities reviewed regularly.	Antivirus software and Microsoft updates (operating system and Office) are monitored regularly. Other systems are not regularly monitored.	2
A.9.7.3	Clock synchronization	Computer clocks shall be synchronized for accurate recording	Computers clocks are synchronized.	3
A.9.8 Mobile computing and teleworking Control objective: To ensure information security when using mobile computing and teleworking facilities.				
A.9.8.1	Mobile computing	A formal policy shall be in place and appropriate controls shall be adopted to protect against the risks of working with mobile computing facilities, in particular in unprotected environments.	No policy. However, from the scope, the only trace of mobile computing is the external access to e-mail by POP3 of the ADU manager (notice that all personnel works with desktop).	1
A.9.8.2	Teleworking	Policies, procedures and standards shall be developed to authorize and control teleworking activities.	Only the ADU manager has teleworking activities.	1
A.10 System development and maintenance				
A.10.1 Security requirements of systems Control objective: To ensure that security is built into information systems.				
A.10.1.1	Security requirements analysis and specification	Business requirements for new systems or enhancements to existing systems shall specify the requirements for controls.	The component of this clause applicable to this scope is the specification of security requirement for the acquisition of systems. This is not performed in ADETTI.	1
A.10.2 Security in application systems Control objective: To prevent loss, modification or misuse of user data in application systems.				
A.10.2.1	Input data validation	Data input to application systems shall be validated to ensure that it is correct and appropriate.	The input to the accounting application is verified by the employee and cross referenced by another person. Other applications are not verified.	2
A.10.2.2	Control of internal processing	Validation checks shall be incorporated into systems to detect any corruption of the data processed.	Not existent. The calculation of all accounting formulas is not verified thoroughly.	1
A.10.2.3	Message authentication	Message authentication shall be used for applications where there is a security requirement to protect the integrity of the message content.	Inexistent.	1
A.10.2.4	Output data validation	Data output from an application system shall be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.	The output of the data processed by the accounting application is verified by the employee. Other applications (such as email) are not verified.	2

A.10.3 Cryptographic controls Control objective: To protect the confidentiality, authenticity or integrity of information.				
A.10.3.1	Policy on the use of cryptographic controls	A policy on the use of cryptographic controls for the protection of information shall be developed.	There is no policy for encryption usage in ADETTI.	1
A.10.3.2	Encryption	Encryption shall be applied to protect the confidentiality of sensitive or critical information.	Encryption is not employed to protect business data under the scope. The only encrypted data found was the Windows user database.	1
A.10.3.3	Digital signatures	Digital signatures shall be applied to protect the authenticity and integrity of electronic information.	Digital signatures are not used.	1
A.10.3.4	Non-repudiation services	Non-repudiation services shall be used to resolve disputes about occurrence or non-occurrence of an event or action.	Not found.	1
A.10.3.5	Key management	A key management system based on an agreed set of standards, procedures and methods shall be used to support the use of cryptographic techniques.	Not found.	1
A.11 Business continuity management				
A.11.1 Aspects of business continuity management Control objective: To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters.				
A.11.1.1	Business continuity management process	There shall be a managed process in place for developing and maintaining business continuity throughout the organization.	Business continuity concerns were found in ADETTI, but not structured as a managed process (define, plan, write, test, revise a plan). In ADETTI the most critical information is identified and is recoverable in case of a major incident. Protection mechanism of this information are: - backups of historical data stored in houses of managers and ADU members; - backup of last week e-mail; - copies of important documents are kept in the accountant office, lawyer; - any project information which might not be recoverable from these sources, can be obtained from the project's partners.	1
A.11.1.2	Business continuity and impact analysis	A strategy plan, based on appropriate risk assessment, shall be developed for the overall approach to business continuity.	An informal assessment of the most critical data in case of a disaster was performed. This assessment did not include resources to ensure continuity of services.	2
A.11.1.3	Writing and implementing continuity plans	Plans shall be developed to maintain or restore business operations in a timely manner following interruption to, or failure of, critical business processes.	It was not found evidences of planned actions to be performed in the event of a major disaster.	1

A.11.1.4	Business continuity planning framework	A single framework of business continuity plans shall be maintained to ensure that all plans are consistent, and to identify priorities for testing and maintenance.	It was not found any evidence of actions to develop a business continuity framework.	1
A.11.1.5	Testing, maintaining and re-assessing business continuity plans	Business continuity plans shall be tested regularly and maintained by regular reviews to ensure that they are up to date and effective.	The several protection mentioned in A.11.1.1 are not regularly tested (last test happen 2 years ago).	1
A.12. Compliance				
A.12.1 Compliance with legal requirements Control objective: To avoid breaches of any criminal and civil law, statutory, regulatory or contractual obligations and of any security requirements.				
A.12.1.1	Identification of applicable legislation	All relevant statutory, regulatory and contractual requirements shall be defined explicitly and documented for each information system.	There is no formal identification of legal requirements related to the information handled by ADETTI. ADETTI has a contracted service of legal counselling that ensures that the activities of the Association are compliant with the Law.	2
A.12.1.2	Intellectual property rights (IPR)	Appropriate procedures shall be implemented to ensure compliance with legal restrictions on the use of material in respect of intellectual property rights, and on the use of proprietary software products.	A not written procedure is followed to protect software copyrights. All software is registered in a software inventory. The licenses are maintained in a defined file cabinet.	2
A.12.1.3	Safeguarding of organizational records	Important records of an organization shall be protected from loss, destruction and falsification.	ADETTI follows the applicable legislation regarding organizational records.	3
A.12.1.4	Data protection and privacy of personal information	Controls shall be applied to protect personal information in accordance with relevant legislation.	ADETTI is aware and complies with the applicable legislation regarding data protection and privacy of personal information.	3
A.12.1.5	Prevention of misuse of information processing facilities	Management shall authorize the use of information processing facilities and controls shall be applied to prevent the misuse of such facilities.	Not found.	1
A.12.1.6	Regulation of cryptographic controls	Controls shall be in place to enable compliance with national agreements, laws, regulations or other instruments to control the access to or use of cryptographic controls.	Not found.	1
A.12.1.7	Collection of evidence	Where action against a person or organization involves the law, either civil or criminal, the evidence presented shall conform to the rules for evidence laid down in the relevant law or in the rules of the specific court in which the case will be heard. This shall include compliance with any published standard or code of practice for the production of admissible evidence.	Not found.	1

A.12.2 Reviews of security policy and technical compliance Control objective: To ensure compliance of systems with organizational security policies and standards.				
A.12.2.1	Compliance with security policy	Managers shall take action to ensure that all security procedures within their area of responsibility are carried out correctly and all areas within the organization shall be subject to regular review to ensure compliance with security policies and standards.	Not found.	1
A.12.2.2	Technical compliance checking	Information systems shall be regularly checked for compliance with security implementation standards.	Not found.	1
A.12.3 System audit considerations Control objective: To maximize the effectiveness of and to minimize interference to/from the system audit process.				
A.12.3.1	System audit controls	Audits of operational systems shall be planned carefully and agreed to minimize the risk of disruptions to business processes.	Not found.	1
A.12.3.2	Protection of system audit tools	Access to system audit tools shall be protected to prevent any possible misuse or compromise.	Not found.	1
A.12.3.1	System audit controls	Audits of operational systems shall be planned carefully and agreed to minimize the risk of disruptions to business processes.	Not found.	1

The analysis of the security management practices and controls in ADETTI revealed that:

a) The overall conformity of ADETTI against the ISO is low. From the 10th areas of ISO, only in two (A.4 Organizational security and A.7 Physical and environmental security) ADETTI reached a minor conformity (2 in the scale used), as shown in the below graphic.

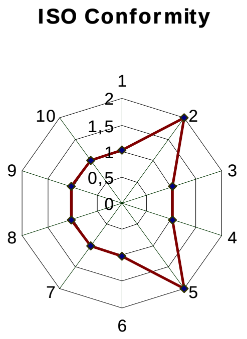


Figure R.8: ISO conformity

b) From the 127 controls analysed, 8 were regarded by BSI as the starting point for implementing information security (*cf.* 3.8.3 in the dissertation text). These 8 controls, highlighted in green in the above table, are:

  i. data protection and privacy of personal information (A.12.1.4).
  ii. safeguarding of organizational records (A.12.1.3);
  iii. intellectual property rights (A.12.1.2);
  iv. information security policy document (A.3.1);
  v. allocation of information security responsibilities (A.4.1.3);
  vi. information security education and training (A.6.2.1);
  vii. reporting security incidents (A.6.3.1);
  viii. business continuity management (A.11.1).

From these 8 controls, ADETTI has found to be minor compliant with the legal compliance issues (A.12.1.2 to A.12.1.4), reporting security incidents (A.6.3.1) and security training (A.6.2.1). In the remaining issues, it was not found practices in ADETTI compliant with the ISO.

c) From the 127, 2 controls were regarded as not applicable for the scope under assessment. In fact, in the select scope, there are not development activities (which exclude the control A.8.1.5 - Separation of development and operational facilities), e-commerce (excluding A.8.7.3 - Electronic commerce security).

d) In sum, of total of the 125 applicable controls, the present conformity auditing reveal 87 nonconformities, 27 minor conformities and 11 controls found to be applied in ADETTI.

5.3.3 List of risk (T05.2)

This outcome was produced through the revision of a serious of information sources:

1 Review the evaluation scope description, in order to identify activities, assets (T02.2).
2 Review the identified interfaces and dependencies of the scope (T02.4).
3 Review the asset register (T04.2).
4 Review the vulnerabilities identified in 5.3.2.
5 Review the threat identified in 5.3.2.

Risks were identified and assessed by the following actions:

1 Similar assets with the same value were grouped in one asset – proposed by the implementation advisor.
2 For each asset, the two employees of the Administrative Unit and its Manager select the most applicable threats, from the threat catalogue from Gillingham [03]. Then, for each threat it was decided the most suitable vulnerability from the list of technological and organizational vulnerabilities identified during the previous assessment. The AD Unit employees and manager decided to adapted the previously identified vulnerabilities and in some cases, introduce new ones.
3 For each combination of a threat and a vulnerability, it was assessed its probability of occurring and its possible impact with a scale of 1 to 5 (being 5 the highest value). To help the assessment team in estimating the impact and probability, the implementation advisor provide the findings of vulnerabilities and threats identification [detailed in the previous section of the present document].
4 The estimated values of the probability and impact of each risk and the asset value of the asset affected by that particular risk were multiplied by each other and then divided by 3. In consequence, risks were scored in a scale of 1 to 125.
5 The identification and assessment of risks were reviewed and approved by the Steering Committee.

Asset	Av	Threat	Vulnerability	Probability	PV	Impact	IV	Risk Level	Risk Ref.
Physical assets									
PA004 - Administrative room	3	Earthquake	Inadequate Physical Protection - Building	At this time it is impossible to predict the occurrence of seismic events with a high magnitude. Lisbon suffer through the centuries seismic events, being the more destroyable in 1356, 1755, 1969 (originated in the Gorringe bank), 1344, 1531 and 1909 (with the epicentre in Tagus lower valley)[CML04]. Because of this historical seismicity, Lisbon area is classified as level A, the highest seismic risk in the four level scale of the Decreto-Lei 235/83 – Regulamento de Segurança e Acções para Estruturas de Edifícios e Pontes.	2	The effect of an earthquake in the area where ISCTE is situated is deemed to be 8 (seismic with the epicentre in gorringe bank) and 7 (the epicentre in Tagus lower valley) in the Modified Mercalli intensity scale [CML04]. The Modified Mercalli scale uses a 12 degree scale to measure the intensity of an earthquake through its effects on nature and man-made structures. Level 7 in Modified Mercalli means very "strong effects": furniture broken; damage negligible in building of good design and construction; slight to moderate in well-built ordinary structures; considerable damage in poorly built or badly designed structures; some chimneys broken, noticed by persons driving motor cars. Level 8 in Modified Mercalli means very "destructive": extensive damage in poorly built structures with partial collapse; fall of chimneys, factory stacks, columns, monuments, walls; heavy furniture moved [CML04]. ISCTE building is armed concrete, and was build after the publication of 1958 anti seismic building legislation, which means that the collapse risk is lower than buildings which are nor compliant with this regulation.	3	18	R001

		Fire	Inadequate fire prevention / detection	The chance of a fire occurring is not very high due to: • general fire protection in place (fire exhauster near the office); • smoking not allowed in the offices.	2	Once started, the fire can cause a serious impact. Insurance and possibility to recover data from other places ensures minimizes some of the negative impact. To aggravate the negative impact, employees do not know the emergency procedures.	5	30	R002
		Flooding	Proximity of environmental threats	Office room is 10 meters away from a wash room. If a pipe licks, it may flood the floor near ADETTI office and even enter in the premises.	1	Regarded as not significant.	2	6	R003
		Damage caused by a external source		A probability of air plane or underground crash exists. ISCTE is near the Lisbon airport and under an airplane highway. A part of ISCTE building is located near an underground line.	2	Unavailability of the office will represent the total activity stopover of the ADU.	5	30	R004
		Unauthorised physical access	Inadequate external access control	High probability, because (1) there is no identification, registration or traceability mechanism for visitors - as recorded in A.7.1.2 (2) room not physically separated from the visitor's area - see A.7.1.1, (3) previous records of such incident.	4	The impact of a simple unauthorised physical access was deemed as low, because financial data is placed at closed cupboards or in disks.	2	24	R005
		Steal		Cases of robbery have happen before, so high probability.	5	Although, most of financial data could easily be recovered from other places, the unavailability of a system or document would represent a lost of time.	4	60	R006
		Wilful damage		ADETTI has never object of vandalism, however a probability exists of a discontent student or researcher try something.	2	The impact of vandalism could be high, as systems or documents could be destroyed.	2	12	R007
		Epidemics (as bird flu)	Location of ADETTI in a building with thousands of visitors	This scenario was deemed as theoretically possible, up to the present this never occurred in ADETTI.	1	Unavailability of the office will represent the total activity stopover of the ADU.	5	15	R008
File cabinet	3	The same as adm. room							R009 - R017
Desktops	4	Hardware failure	Inadequate maintenance	No reported previous problem. Maintenance is not performed regularly.	2	Serious problems can be recovered by back-ups made regularly and reinserting some financial data (which exist in paper). However, some data will probably be lost.	3	24	R018
		Denial of service	Malicious code/action	Desktops where users have administrative rights, such as the ones from Administrative Unit, can be	4	Serious impact. As desktops have backups perform every month, some data will probably be lost.	3	48	R019

				prone to spyware and other malicious code threat.					
		Unauthorised access	Inadequate malicious code/firewall protection	ADETTI network has a high visibility of potential “script kiddies” [see this concept at en.wikipedia.org/wiki/Script_kiddie] Moreover, the antivirus engine is outdated in these machines.	4	Impact on the integrity of financial data can be high.	5	80	R020
		Infringement of copyright law	Lack of security awareness	Probable, because the ADU employees have files which might do not follow copyright protected content [music files].	3	Infringement of a law, can cause fines and the retention of desktops, which would have a significant impact.	4	48	R021
ServerRSI	4	Server failure [hardware or software problem]	Inadequate maintenance	No reported previous problem. IT maintenance may fail to perform some procedure. For example installing patches from Microsoft, without verifying software compliance may cause software problems.	3	Serious problems can be recovered by back-ups made regularly.	2	24	R022
		Denial of service	Malicious code/action	There is always a possibility that somebody attacks, but RSI Server is not a high profile target	3	Impact on the processing of financial data is medium, because financial data is replicated at local desktops and other network services (mail, Internet access can be reconfigured by ADETTI employees).	4	48	R023
		Unauthorised access	Inadequate malicious code/firewall protection	ADETTI network has a high visibility of potential “script kiddies” [see this concept at en.wikipedia.org/wiki/Script_kiddie] Moreover, the antivirus engine is outdated.	4	Impact on the processing of financial data is medium, because financial data is replicated at local desktops.	3	48	R024
ServerBSCW	5	Server failure [hardware or software problem]	Inadequate maintenance	Hardware prone to fail (single power supply, environment with high temperatures and dust). Maintenance performed rarely.	3	The components of the server are easily obtained (from other end to life machines). Weekly back-ups are done.	2	30	R025
		Denial of service	Malicious code/action	The running software version’s Apache 1.3.27 have multiple denial of service vulnerabilities (e.g. CAN-2004-2069).	2	The degradation or stop of the server will have a serious impact on the general operations of ADETTI.	3	30	R026
		Unauthorised access	Inadequate access control management	Some user accounts are not individual. Several users share the same account. Most of these users have a motivation to access unauthorised data.	3	Most of the data which is stored in BSCW do not have a high confidential requirement. So the impact could be low.	2	30	R027
			Inadequate malicious code/firewall protection	ADETTI network has a high visibility of potential “script kiddies” [see this concept at en.wikipedia.org/wiki/Script_kiddie] Moreover, the antivirus engine is outdated.	4	Impact is serious.	4	80	R028

			Inadequate patch management procedure	The running software Apache 1.3.27 has multiple vulnerabilities.	2	These vulnerabilities if explored would cause a significant impact on the platform.	4	40	R029
SwitchCISCO	3	Hardware failure	Lack of maintenance procedure	Equipment has 1 year. The switch is designed for an MTBF of 268.876 hours (31 years), so problems are not likely to occur in the next 12 months.	1	If the equipment fails, there are other means to support the network.	2	6	R030
		Denial of service	Malicious code	An infected workstation can cause a denial of service to the switch. The worm Nimda32 is know to numerous ARP request, thus causing a Denial-of-Service in switches [taken from http://www.sans.org/resources/malwarefaq/32-nimda-exploit.php]	4	The switch availability is relevant, however it can be overcome by alternative means of sharing data.	2	24	R031
Backup cartridges	4	Media failure	Lack of testing and maintenance tasks	As media as stored in a file cabinet in office, without the recommended environmental conditions. Moreover, the restore operation is not tested.	4	A corrupted media can prevent financial data from being restored, which can cause the consumption of great period of time and effort to re-inserting or replicating this data.	3	48	R032
		Theft of media	Inappropriate physical access control measures	It has never happened before that some of the media 'vanished' from the office. There are instructions for staff that say there should always be workers in the room, which are followed. Therefore this is not very probable.	2	A stolen media can easily be replaced. The financial data stored do not have high confidentiality value.	3	24	R033
Fax machine	4	Fax unavailability	Lack of maintenance procedure	Never happen. Not probable.	1	Availability of the fax is recommended for communication with partners. The equipment holds no data with business value.	2	8	R034
Printers [Ricoh, HP LaserJet and Lexmark]	3	Printer unavailability	Lack of maintenance procedure	One printer has 1 year, the others are more old, so more likely to have problems.	2	Problems with availability can be easily fixed – due to existing other printers.	2	12	R035
		Incorrect printing output	Lack of maintenance procedure	One printer has 1 year, the others are more old, so more likely to have problems.	2	Problems with integrity can be easily fixed – due to the verification of printing output by employees.	2	12	R036
PBXSiemens	3	PBX failure	Lack of maintenance procedure	No problem ever happen according to the reported.	1	Essential for voice communication, but in case of necessity mobile phones or the telephone infrastructure of ISCTE could be used.	2	6	R037
Data and voice cabling	4	Malicious action	Inappropriate network segregation	As ADETTI shares the same infrastructure of ISCTE, ADETTI assets are not isolated from the threats of script kiddies.	3	Impact can be serious.	4	48	R038
ADETTI stamp	2	Stamp	Inappropriate	As reported that the stamp was frequently missing	1	The stamp is important for the certification of	2	4	R039

		unavailability	storage of the stamp	and some time had to be consumed in searching it.		the some documentation in the final financial report. However, the stamp can easily be repurchased.			
Office furniture	2	The same as adm. Room							R040 - R048
Information assets									
User and computers database	3	Unauthorised access	Inappropriate network segregation	An incident of this form has never happened in the past. Nevertheless this can happen in the future.	2	Without domain authentication, users can work locally.	3	18	R049
		Lack of auditable records	Inadequate access control management	There are no records of the creation, modification or deletion of users accounts. It is probable that some event occur which require this verification.	3	There are no records of the creation, modification or deletion of users accounts. In case of necessity, actions can no be trace back to their initiators.	3	27	R050
System documentation [Software licenses and technical manuals]	3	Document unavailability	Inappropriate filling and storage of documents	The IT service, which is maintaining the system documentation, has the obligation to keep a copy securely, but there is no control from ADETTI to verify if this happens.	2	Failure to maintain a record of license may result in fines. System documentation should be available only internally, integrity and availability is high because lack of these requirements can aggravate a system breakdown.	3	18	R051
ISMS documentation	3	Following an outdated version	Lack of documentation procedure	A user can access and follow an outdated version of a security regulation. This may happen if appropriate document procedures are not in place, and there are not.	2	This can mislead the user to perform an action not sanctioned by the security regulation valid at that time.	3	18	R052
		Document unavailability	Inadequate filling or storing of documents	If no document procedure is implement this may happen.	2	It is important that the ISMS documents are available.	2	12	R053
Current project's accountability	5	Fraud (discrepancies in financial data caused by deliberate action)	Difficulty to deter or detect fraud	No previous case was noticed. However a possibility exists of some worker altering financial information to provide an advantage for him.	2	It is important to ensure that any discrepancy in financial data is found timely and it is possible to correct before the submission of the final financial report. A financial report with incorrect values may cause extremely serious impact on ADETTI.	5	50	R054
		Inaccurate input, processing or output	Lack of defined procedure	All financial data is checked several times, but this risk can not be ignored. Moreover, these several checks are not formalised in a written procedure.	4	Any mistake, if not detected, before the final report submission, can be very serious.	5	100	R055

		Delivery delay of financial data	Lack of procedures	Project leaders may delivery financial data in a short period before the report submission date. This has happen before.	3	The delay in the delivery of financial data can hinder the efforts to finish timely and appropriately the report.	5	75	R056
		Document unavailability	Inappropriate filling of documents	It has happened happen before that a document is stored in the wrong folder.	3	At the time of project conclusion, all documentation is reviewed and usually a copy is made available quickly, so the any document lost can be recovered.	2	30	R057
Contracts related to research projects	5	Document unavailability	Unprotected storage (no backups of documents)	Although the file cabinet is closed, there are no digital copies of that documents stored in another location. So the contracts on the file cabinet can be destroyed or removed, and ADETTI does not have the possibility of timely recovery of the document.	2	All contracts are managed by the ADU, Executive Commission and project leaders. Other staff can only view them with a specific authorisation. The integrity and availability of contracts is required by funding organizations.	5	50	R058
Projects documentations [documents of closed projects and non financial data of current projects]	5	Unauthorised access	Inadequate access control management	The project documentation in the BSCW server could be accessed by an unauthorised user who circumvents the software protections. It has happen before a user doing so for a folder with academic data.	3	Most projects conducted by ADETTI have confidentiality requirements, so the breach of these requisites can cause problems in existing partnerships and contracts for ADETTI.	5	75	R059
		Document unavailability	Unprotected Storage (no logging of accesses)	Although the file cabinet is closed, there is not logging of accesses to the documentation. Nevertheless, no situation was reported.	2	ADETTI must maintain project documentation for 4 years (contract requirement of FCCN and , European Commission)	5	50	R060
Employees personal data	4	Breach of personal data legislation	Lack of procedures	At the moment, no situation of possible incompliance was identified or reported. But has there is no procedure to identify legal requirements the problem, exists.	2	Impact is of a legislation breach is very serious. The usage of employee's personal data (age, parents, etc.) for all other purpose than salaries processing, must be authorised by the employee.	5	40	R061
Internal documentation [all other documentation]	3	Document unavailability	Unprotected storage (no backups of documents)	There are no digital copies of these documents. So if any of these documents is destroyed or removed, ADETTI does not have the possibility of timely recovery of the document.	2	Impact is for these documents are medium. For some records, such as accountant books and records (which must be kept for 10 years) and recruitment records (it must be kept for 5 years) there are availability requirements.	4	24	R062
Service									
Electrical power	4	Power electrical failure	Unstable electrical power supply	Last year it happened just one time for a just period of less than 5 minutes.	2	All the desktops and servers of the ADU have line interactive Uninterruptible Power Supply (UPS).	2	16	R063
		Power electrical fluctuations		No record of such situation.	1	All the desktops and servers of the ADU have line interactive Uninterruptible Power Supply (UPS).	2	8	R064

Air conditioning	1	Hardware failure	No maintenance in place.	There are no records of such event. The equipment is 2 years old.	1	No significant impact. As there are no maintenance contracts in place for the office equipment, a failure would take a long time to repair.	1	1	R065
Internet connection [only web browsing]	3	Service unavailability	No redundant Internet connection solution	Probable, as this happen one time in the last year.	3	Without Internet access, the reporting process can be carry out, but with difficulties, e.g. the ADU must communicate with project leaders through telephone.	3	27	R066
		Poor quality of service	Inappropriate capacity of the infrastructure	Due to high Internet bandwidth, it was report several problems with web navigation.	4	With a low quality Internet access, the reporting process can be carry out.	2	24	R067
Telephone service	5	Communication unavailability	No redundant voice connection	Never happen.	2	Without voice communication, the reporting process can be carry out (using mobile telephones).	1	10	R068
SMTP service [includes SMTP gateway]	5	Service unavailability	Hardware failure	It was happen a before a problem with the SMTP server of ISCTE.	4	Without messaging communication, the reporting process suffers major delays.	3	60	R069
		Poor quality of service	Inappropriate capacity of the infrastructure	Due to high Internet bandwidth, it was report several problems with messaging communication.	4	With a low quality messaging service, the reporting process suffers major delays.	2	40	R070
IT service	5	Inappropriate IT support	Lack of defined procedures	IT support is provided by a contracted technician with a service delivery contract (avença). It was identified as a problem the low availability of the IT service (if a problem occurs, the service is only available in more than 6 hours).	3	As users have a good IT knowledge, most situations are dealt by them.	1	15	R071
Courier	5	Lost of a document	Inappropriate transportation of documents	For the past 2 years of working with that courier, any problem was found.	1	Copies of the document send are maintained in several places in ADETTI and its partners.	2	10	R072
		Lost of integrity of a document	Deliberate action/Inappropriate transportation of documents	For the past 2 years of working with that courier, any problem was found.	1	As all pages are numbered and indexed, it is probable that an incident related with integrity is discovered before causing any impact.	2	10	R073
		Lost of the confidentiality of a document	Deliberate action/Inappropriate transportation of documents	For the past 2 years of working with that courier, any problem was found.	2	The documents that are transported do not have a high confidentiality requirement.	1	10	R074

Personnel									
AUM /AUE1	5	Staff (AUM or AUE1) unavailability	Absence / Insufficient staff	Absence is probable.	3	Work can be easily transferred to other employees.	2	30	R075
		Total staff unavailability (both AUM and AUE1)	Impossibility to work for a long period (more than a one week)	Intrinsic reasons (related to the personnel health) and external reasons (derived from epidemic diseases such as bird flu for example) can cause a long period of staff unavailability. No record of such unavailability up to now.	1	Epidemic diseases such as bird flu can force the prohibition of people going to public places or even to work outside its home, therefore the impact is critical.	5	25	R076
		Misuse or unauthorised use of assets	Unintentional actions of absent mind employees	Probability of deliberate actions is low, but it was found evidences of actions, which may be inadvertently cause risk (in one desktop of the ADU was found an administrative account without password).	3	Some careless actions can posse a serious impact to the correct functioning of the process.	2	30	R077
			Discontent Administrative Unit employee	Administrative Unit employees can perform intentional actions that cause risks. This was regarded as high risk in section 5.3.1 in this document.	1	Impact of this sort of actions can be high. However, there is procedure that should ensure the timely detection of this event.	4	20	R078
AUE2	4	Staff (AUE2) unavailability	Absence / Insufficient staff	Absence is probable.	3	Work can be easily transferred to other employees.	2	24	R079
		Misuse or unauthorised use of the assets	Unintentional actions of absent mind employees	Probability of deliberate actions is low, but it was found evidences of actions, which may be inadvertently cause risk (in one desktop of the ADU was found an administrative account without password).	3	Some careless actions can posse a serious impact to the correct functioning of the process.	2	24	R080
			Discontent Administrative Unit employee	Administrative Unit employees can perform intentional actions that cause risks. This was regarded as high risk in section 5.3.1 in this document.	1	Impact of this sort of actions is not too high, as this employee does not have a critical role in the financial process.	2	8	R081

5.4 Risk acceptance criteria (T05.3)

To define the risk acceptance criteria, it was analysed the risk ingredients (probability and impact). For each of these factors it was discussed within the Steering Committee what situations would be acceptable and which was not.

The adopted risk formula allows possible risk scores from 1 to 125. In this range of numbers, 75 is the medium. However, based on the risk scores obtained some risks with risk score of 75 were unacceptable. Therefore, the Steering Committee decided to divide 75 by 2, which result in 32,5. Nevertheless, some risks with less than 32,5 were viewed as not acceptable. Consequently, it was decided to place the acceptance level at 32. risks higher would have to be treated, risks lower than that level could be acceptable.

The Steering Committee decided to distinguish between two types of risks:

a) risks lower than a risk level of 32 could be accepted, because they have a low or not significant probability and/or impact,;
b) risks with a level higher than 32 could not be acceptable and would be subject to analysis to verify how they could be treated. Risk treatment can involve one or a combination of the following three strategies:

    i. Transference
    ii. Avoidance
    iii. Mitigation

5.5 Risk Treatment Plan (T05.4)

The Risk Treatment Plan, as discussed in section 3.8.2 of the dissertation text, lists for all identified risks:

a) The treatment strategy (accept, mitigate, avoid or transfer) according to the risk acceptance criteria defined at T05.2.

b) Identify the more suitable controls to be implemented.

5.5.1 Treatment strategy

Risk treatment can involve one or a combination of the following three strategies:

i. Acceptance
ii. Transference
iii. Avoidance
iv. Mitigation

The Steering Committee decided all risks must be evaluated in terms of the following options:

- first risks are assessed if they are acceptable.
- ff the risk is too dangerous to be tolerable, it is evaluated consequently in terms of avoidance, transference or mitigation.

The risk to be acceptable must be below the defined risk acceptance level (a defined value in the scale of possible risk values, which differentiate the risks which are acceptable from the ones, which are not).

All residual risks were acknowledged - *cf.* 3.10.3 in the dissertation text.

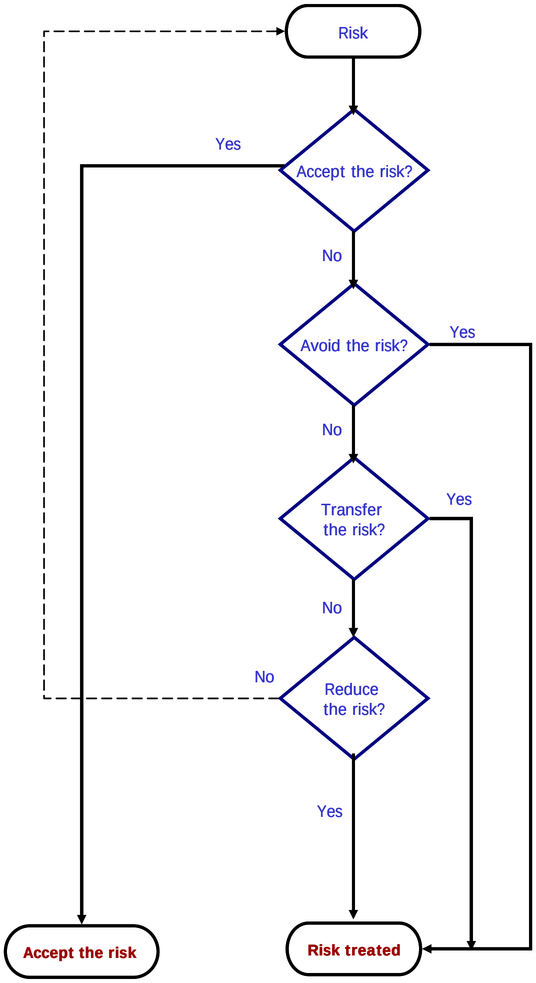


Figure R.9: Treatment strategy

5.5.2 Control selection

The selection of the countermeasures should be based on the controls of Annex A of BSI. The decision to select a particular control of ISO is based on [Humphreys02a]:

- estimated effectiveness (in what extend will reduce the level of risk);
- cost required to apply the control;
- time required to apply the control.

The Steering Committee decided the following guidelines to estimate the three criteria for a possible countermeasure type:

Type of control	Control effectiveness	Cost	Time
Develop an security procedure	5 - 10	€ 0	3 days
Train and create awareness of security issues	5 – 10	€ 0	4 days
Deploy an technological equipment (based on open source software)	5 – 10	€ 300 - € 1000 (hardware)	2 days

All risk (1) classified with a score higher than 100 or (2) which have been treated with a technological control must be addressed by a Detailed Risk Treatment Plan, which details:

- Risk priority
- Risk owner
- Risk description
- Risk assessment
- Risk indicators
- Control implemented

The Detailed Risk Treatment Plan ensures that the most dangerous risks or the risks tacked by specific controls (as for instance surveillance video camera) are properly monitored.

The distinction between risks addressed by procedures and risk tacked by controls is due to the fact that monitoring activities are integrated in the procedure, while specific technological controls do not have in build risk monitoring processes.

Asset	Risk	Threat	Vulnerability	Risk level	Treatment option	Applicable Controls	Risk reduced	Residual risk	Cost	Time	Selected
PA004 - Administrative room	01	Earthquake	Inadequate Physical Protection - Building	18	Accept	NA	NA	NA	NA	NA	NA
	02	Fire	Inadequate fire prevention / detection	30	Mitigate	Develop a Business Continuity Management that includes fire situations [A.11.1.3]	5	25	NA	90 days	Yes
						Train fire procedures under the BCM framework [A.11.1.5]	2	28	NA	90 days	Yes
	03	Flooding	Proximity of environmental threats	6	Accept	NA	NA	NA	NA	NA	NA
	04	Damage caused by a external source		30	Mitigate	Develop a Business Continuity Management [A.11.1.3]	5	25	NA	90 days	Yes
	05	Unauthorised physical access	Inadequate external access control	24	Accept	NA	NA	NA	NA	NA	NA
	06	Robbery		60	Mitigate	Install a surveillance camera at the office lobby [A.7.1.1]	10	50	€ 300	2 days	Yes
						Define norms for the physical security of the office and its equipment [A.7.1.3]	5	55	€ 0	1 day	Yes
	07	Wilful damage		12	Accept	NA	NA	NA	NA	NA	NA
	08	Epidemics (as bird flu)	Location of ADETTI in a building with thousands of visitors	15	Accept	NA	NA	NA	NA	NA	NA
File cabinet	09-17	The same as adm. room									
Desktops	18	Hardware failure	Inadequate maintenance	24	Accept	NA	NA	NA	NA	NA	NA
	19	Denial of service	Malicious code/action	48	Mitigate	Update malicious code software (from McAffe 7.0 to McAffe 8.0) [A. 8.3.1]	10	22	€ 50 per desktop	NA	Yes
	20	Unauthorised access	Inadequate malicious code/firewall protection	80	Mitigate	Implementing access control from ADETTI network to the ISCTE network (reinforce firewall policies) [A.9.4.6]	10	70	€ 300 (hardware)	2 days	Yes

	21	Infringement of copyright law	Lack of security awareness	48	Mitigate	Train and create awareness of security issues [A.6.2.1]	10	38	€ 0	3 days	Yes
ServerRSI	22	Server failure	Inadequate maintenance	24	Accept	NA	NA	NA	NA	NA	NA
	23	Denial of service	Malicious code/action	48	Mitigate	Update malicious code software (from McAffe 7.0 to McAffe 8.0) [A. 8.3.1]	10	38	€ 50 per desktop	NA	Yes
	24	Unauthorised access	Inadequate malicious code/firewall protection	48	Mitigate	Implementing access control from ADETTI network to the ISCTE network (reinforce firewall policies) [A.9.4.6]	10	38	€ 300 (hardware)	2 days	Yes
ServerBSCW	25	Server failure	Inadequate maintenance	30	Mitigate	Develop IT maintenance procedure [A.8.1.1]					
	26	Denial of service	Malicious code/action	30	Mitigate	Implementing access control from ADETTI network to the ISCTE network (reinforce firewall policies) [A.9.4.6]					
	27	Unauthorised access	Inadequate access control management	30	Mitigate	Develop access control procedure [A.9.2.2]	10	20	€ 0	3 days	Yes
	28		Inadequate malicious code/firewall protection	80	Mitigate	Implementing access control from ADETTI network to the ISCTE network (reinforce firewall policies) [A.9.4.6]	10	38	€ 300 (hardware)	2 days	Yes
	29		Inadequate patch management	40	Mitigate	Develop IT maintenance procedure [A.8.1.1]	10	30	€ 0	3 days	Yes
SwitchCISCO	30	Hardware failure	Lack of maintenance	6	Accept	NA	NA	NA	NA	NA	NA
	31	Denial of service	Malicious code	24	Accept	NA	NA	NA	NA	NA	NA
Backup cartridges	32	Media failure	Lack of testing and maintenance tasks	48	Mitigate	Develop a procedure to test and backups [A.8.4.1]					
	33	Theft of media	Inappropriate physical access control measures	24	Accept	NA	NA	NA	NA	NA	NA
Fax machine	34	Fax unavailability	Lack of maintenance	8	Accept	NA	NA	NA	NA	NA	NA
Printers	35	Printer unavailability	Lack of maintenance	12	Accept	NA	NA	NA	NA	NA	NA
	36	Incorrect printing output	Lack of maintenance	12	Accept	NA	NA	NA	NA	NA	NA
PBXSiemens	37	PBX failure	Lack of maintenance	6	Accept	NA	NA	NA	NA	NA	NA
Data and voice cabling	38	Malicious action	Inappropriate network segregation	48	Mitigate	Implementing access control from ADETTI network to the ISCTE network (reinforce firewall policies) [A.9.4.6]	10	38	€ 300 (hardware)	2 days	Yes
ADETTI stamp	39	Stamp unavailability	Inappropriate storage of the stamp	4	Accept	NA	NA	NA	NA	NA	NA

Office furniture	40-48	The same as adm. room			Accept	NA	NA	NA	NA	NA	NA
User and computers database	49	Unauthorised access	Inadequate access control management	12	Accept	NA	NA	NA	NA	NA	NA
	50	Lack of auditable records	Inadequate access control management	27	Accept	NA	NA	NA	NA	NA	NA
System documentation	51	Document unavailability	Inappropriate filling and storage of documents	18	Accept	NA	NA	NA	NA	NA	NA
ISMS documentation	52	Following an outdated version	Lack of documentation procedure	18	Accept	NA	NA	NA	NA	NA	NA
	53	Document unavailability	Inadequate filling or storing of documents	12	Accept	NA	NA	NA	NA	NA	NA
Currents project's accountability	54	Fraud (discrepancies in financial data caused by deliberate action)	Difficulty to deter or detect fraud	50	Mitigate	Produce an Information labelling and handling procedure [A.5.2.2]					Yes
	55	Inaccurate input	Inadequate verification of input data	50	Mitigate	Develop a written procedure for the financial process [A. 8.1.1], including input data validation [A.10.2.1]					Yes
	56	Delivery delay of financial data	Lack of procedures	40	Mitigate	Develop a written procedure for the financial process [A. 8.1.1]	10	30	€ 0	3 days	Yes
	57	Document lost	Inappropriate filling of documents	30	Mitigate	Produce an Information labelling and handling procedure [A.5.2.2]	5	25	€ 0	3 days	Yes
Contracts related to research projects	58	Document unavailability	Unprotected storage (no backups of documents)	50	Mitigate						
Projects documentations	59	Unauthorised access	Inadequate access control management	75	Mitigate	Develop access control procedure [A.9.2.2]	10	65	€ 0	3 days	Yes
	60	Document unavailability	Unprotected Storage (no logging of accesses)	50	Mitigate						

Employees personal data	61	Breach of personal data legislation	Lack of procedures	40	Mitigate	Develop procedure that includes the verification of legal compliance – [A.12.1.4]			€ 0	3 days	Yes
Internal documentation	62	Document unavailability	Unprotected storage (no backups of documents)	24	Accept	NA	NA	NA	NA	NA	NA
Electrical power	63	Power electrical failure	Unstable electrical power supply	16	Accept	NA	NA	NA	NA	NA	NA
	64	Power electrical fluctuations		8	Accept	NA	NA	NA	NA	NA	NA
Air conditioning	65	Hardware failure	No maintenance in place.	1	Accept	NA	NA	NA	NA	NA	NA
Internet connection	66	Service unavailability	No redundant Internet connection solution	27	Accept	NA	NA	NA	NA	NA	NA
	67	Poor quality of service	Inappropriate transportation of documents	24	Accept	NA	NA	NA	NA	NA	NA
Telephone service (TDM operator)	68	Communication unavailability	No redundant voice connection	10	Accept	NA	NA	NA	NA	NA	NA
SMTP service	69	Service unavailability	Hardware failure	60	Mitigate	Deploy an SMTP server for ADETTI separately from ISCTE [A.9.4.6]	15	45	€ 1000	4 days	Yes
						Develop procedures for regular IT maintenance for the systems that support the SMTP service [A.8.1.1]	10	50	€ 1000	4 days	Yes
	70	Poor quality of service	Inappropriate capacity of the infrastructure	40	Mitigate	Deploy an SMTP server for ADETTI separately from ISCTE [A.9.4.6]	15	25	€ 1000	4 days	Yes
						Establish user practices to enable a more efficient and professional use of email [A.6.1.1]	5	35	€ 0	3 days	Yes
IT service	71	Inappropriate IT support	Lack of defined procedures	15	Accept	NA	NA	NA	NA	NA	NA
Courier	72	Lost of a document	Inappropriate transportation of documents	10	Accept	NA	NA	NA	NA	NA	NA
	73	Lost of integrity of a document	Deliberate action/Inappropriate transportation of	10	Accept	NA	NA	NA	NA	NA	NA

			documents								
	74	Lost of the confidentiality of a document	Deliberate action/Inappropriate transportation of documents	10	Accept	NA	NA	NA	NA	NA	NA
AUM/AUE1	75	Staff (AUM or AUE1) unavailability	Absence / Insufficient staff	30	Mitigate	Train AUE2 to be a backup for the financial process [A.6.2.1]	10	20	€ 0	2 days	Yes
	76	Total staff unavailability (both AUM and AUE1)	Impossibility to work for a long period (more than a one week)	25	Accept	NA	NA	NA	NA	NA	NA
	77	Misuse or unauthorised use of the assets	Unintentional actions of absent mind employees	30	Mitigate	Develop an information security policy [A.3.1.1]	5	25	€ 0	3 days	Yes
						Train and create awareness of security issues [A.6.2.1]	10	20	€ 0	4 days	Yes
	78		Discontent Administrative Unit employee	20	Accept	NA	NA	NA	NA	NA	NA
AUE2	79	Staff (AUE2) unavailability	Absence / Insufficient staff	24	Accept	NA	NA	NA	NA	NA	NA
	80	Misuse or unauthorised use of assets	Unintentional actions of absent mind employees	24	Accept	NA	NA	NA	NA	NA	NA
	81		Discontent Administrative Unit employee	8	Accept	NA	NA	NA	NA	NA	NA

In total the selected countermeasures enable an estimated reduction of 17% in the sum of the risk scores of the risks deemed as not acceptable. In fact, the sum of those risks, before the application of mitigation measures, was 1243 and due to those safeguards this total decrease to 1031 (as discussed in 6.2.5. of the dissertation text).

6. Define security processes and controls

6.1 Requirements

Inputs		Practices and techniques	Output(s)
T06.1	• BSI requirements of an ISMS • Existing security management practices (from T05.2) • Risk Treatment Plan (from T05.4)	• Definition of security norms	• Documentation: ISMS documentation • Activities: Security processes • Organizational: tasks and responsibilities

6.1.1 Required activities, controls and documentation

An ISMS requires the standardisation of security practices, which entails that existing practices be agreed, defined, documented and controlled. In order to accommodate these requirements it is necessary to define a number of practices in a documented support.

Abiding by the interpretation of three layers of processes in an ISMS (made in section 5.2 of the dissertation), in the present phase it was identified which processes, in ADETTI, were required to define in order to attain the compliance with BSI.

After we list the required activities for a security management system, we will define the document support of these activities.

6.1.2 List of required activities

6.1.2.1 Operational process

In ADETTI, it was decided to restrict the security management to the process of financial reporting, thus this process constitutes the operational process, according to the classification proposed in section 5.1 of the dissertation text.

The existence of a process description of the operational activities under the scope can be deemed as a requirement of BSI under the “ISMS scope”.

The activities included in the scope were described in a previous phase of this methodology, in the scope definition [see phase 2 in section 2 of the present document], and will be further addressed in the following step: Work_Deliverable05: Scope management.

6.1.2.2 Mandatory processes

BSI requires that some particular activities related to management control are performed in any security management system (in 5.1 of the dissertation text).

Mandatory BSI clauses	**Proposed process**	**Interpretation**	**Required output**
4 ISMS requirements 4.1 General requirements 4.2 Establishing and managing the ISMS 4.2.1 Establish the ISMS	ISMS scope	Process used to establish the scope and context of the ISMS	Work_Deliverable05: Scope management
	ISMS policy	Develop, publish and maintain a policy which reflects business concerns and proposes a direction for security management.	Work_Deliverable01: Information security policy
	Risk management	Establish the assets under the scope and then identify, assess and treat risks in a continuous manner.	Work_Deliverable04: Asset management Work_Deliverable06: Risk management
4.2.2 Implement and operate the ISMS	Security incidents management	Detection and response to security incidents.	Work_Deliverable07: Human resource management
4.2.3 Monitor and review the ISMS	Performance monitoring	Enable management to determine whether the security activities delegated to people or implemented by information technology are performing as expected.	Work_Deliverable14: Compliance and continual improvement management
4.2.4 Maintain and improve the ISMS	Procedures to support security processes	Documented procedures needed by the organization to ensure the effective planning, operation and control of its information security processes.	Work_Deliverable03: Supporting process of security norms
4.3 Documentation requirements 4.3.1 General 4.3.2 Control of documents 4.3.3 Control of records	Document control	Documents and records required by the ISMS shall be protected and controlled.	
5 Management responsibility 5.1 Management commitment 5.2 Resource management 5.2.1 Provision of resources 5.2.2 Training, awareness and competency	Organization of security management	Security management activities must be defined, conducted and monitored.	Work_Deliverable02: Organization of security management
	Human resource management	Human resource management includes: - job description, - training needs assessments, - training in security competences and - awareness raising activities.	Work_Deliverable07: Human resource management

6 Management review of the ISMS 6.1 General 6.2 Review input 6.3 Review output 6.4 Internal ISMS audits	Internal audit	The responsibilities and requirements for planning and conducting audits, and for reporting results and maintaining records shall be defined in a documented procedure	Work_Deliverable14: Compliance and continual improvement management
7 ISMS improvement 7.1 Continual improvement 7.2 Corrective action 7.3 Preventive action	Corrective and preventive action	Corrective and preventive actions are activities that are taken to address potential or actual nonconformities and make improvements.	

Table R.3: Mandatory clauses of BSI

The above table shows the mandatory requirements of BSI and a possible interpretation of the processes and their associated work deliverables of the proposed methodology which could be associated.

The clauses 4 to 7 of BSI can be interpreted as defining the following requirements:

1. ISMS scope
2. ISMS policy
3. Risk management
4. Security incidents management
5. Performance monitoring
6. Procedures to support security processes
7. Document control
8. Organization of security management
9. Human resource management
10. Internal audit
11. Corrective and preventive action

These mandatory requirements can be attained by the following 8 processes:

- Work_Deliverable01: Information security policy (attains ISMS policy requirement)
- Work_Deliverable02: Organization of security management (complies with the organization requirement)
- Work_Deliverable03: Supporting process of security norms (related to the procedures to support security and document control requirement)
- Work_Deliverable04: Asset management (related to the risk management requirement)
- Work_Deliverable05: Scope management (attains ISMS scope requisite)
- Work_Deliverable06: Risk management (risk management requirement)

- Work_Deliverable07: Human resource management (attains the requirements of human resource and incident management)
- Work_Deliverable14: Compliance and continual improvement management (this process fulfils the internal audit, performance monitoring and corrective and preventive action requirement)

6.1.2.3 Selective processes and controls

The British Standards encompass a group of selective safeguards, which are assembled in an Annex of the British Standard (Annex A).

These safeguards are grouped in 10 domains, as discussed in Annex B. The following domains were applied in the project, due to the selection of countermeasures integrated in those domains:

- Work_Deliverable08: Information classification
- Work_Deliverable09: Physical and environmental management
- Work_Deliverable10: Communications and operations management
- Work_Deliverable11: Access control management
- Work_Deliverable13: Business continuity management

All of these 5 domains include controls, which were selected. However the following domain did not have any risk associated with him, and therefore did not have any output:

- Work_Deliverable12: System development and maintenance management

The output of these selections was:

- a number of procedures (for the controls which prescribed activities and therefore could be described in processes) as:
    - 2.8 Document Classification Procedure
    - Physical caveats integrated in “Recommended Security Practices”, a supporting document of “2.6 Human Resource Manag. Procedure”
    - 2.12 IT Operations Procedure
    - 2.11 Access Control Procedure
    - 2.13 Business Continuity Framework Procedure

- A number of “Detailed Risk Treatment Plans” for risks classified with a score higher than 100 or for risks with controls which are not activities but are technological (the template “Detailed Risk Treatment Plans” is included in Annex E). The following 4 controls are in this last circumstance:

    - Install a surveillance camera at the office lobby [A.7.1.1]
    - Update malicious code software (from McAffe 7.0 to McAffe 8.0) [A. 8.3.1]
    - Implementing access control from ADETTI network to the ISCTE network (reinforce firewall policies) [A.9.4.6]
    - Deploy an SMTP server for ADETTI separately from ISCTE [A.9.4.6]

6.1.3 List of required documentation by BSI (BS 77799-2:2002)

BSI demands the existence of three types of documentation in an ISMS: policies, procedures and records, as shown in the next Figure.

Documentation requisites
Policies
Procedures
Records

Figure R.10: Documentation requirements by BSI

The British Standard explicitly refers to the following documents in order to attain the BS 7799-2 certification:

- Security policy statements
- ISMS Scope
- Risk assessment report [the present document]
- Risk treatment plan
- Documented procedures, such as:
    - detection of and response to security incidents
    - monitoring procedure
    - control of documents
    - audit
    - corrective and preventive action
- Records required by the British Standard
- Statement of Applicability

The following stages intended to produce the aforementioned documentation. The decisions regarding the documentation are made in Work_Deliverable03: Supporting process of security norms.

6.2 Develop the supporting documentation (T06.1)

6.2.1 Work_Deliverable01: Information security policy

Requirement type	Mandatory requirement for BSI
Risk measures applicable [from the risk Treatment Plan]	Develop an information security policy [A.3.1.1] - Risk77
Purpose	The first document to be produced was the "Information Security Policy Statement", which is the Work_Deliverable01 or simply WD_01. According to BSI (*cf.* 3.3.2 in the dissertation text) and ISO (*cf*. Annex B.2.2) is the primary source of all security documents.
Existing practices in ADETTI	Inexistence of formal security norms (A.3.1.1 in 5.3.2 of this document)
Methodology	**a) Decide the policy structure** Before defining the content of a strategic security policy, the structure of this document was defined by the implementation advisor, following the recommendations of several authors - [BSI03a], [Barman02], [Woods02], [Guel01], [Purser04]: a) Purpose – states the main purpose of the ISMS in ADETTI. b) Objectives – clarifies the management objectives for security management. c) Applicable legal requirements – states ADETTI compliance with all applicable legal requirements. d) Applicability - states the coverage or the audience of the policy. e) Responsibilities - who is accountable for what actions. f) Enforcement - asserts the possibility of disciplinary action against the violators. g) Ownership and revision – establishes who is the policy owner and the circumstance for a regular or unplanned revision of the document. It was decided also to add a glossary and a document control mechanism in order to clarified the meaning of any concept and control the document's revisions, respectively. **b) Compose the Strategic Information Security Policy** The first draft of the document was composed by the implementation advisor and then was revised and approved by steering committee.
Outcome	"Information Security Policy Statement", integrated in the Security Manual (Annex D).

6.2.2 Work_Deliverable02: Organization of security management

Requirement type	Mandatory requirement for BSI
Risk measures applicable	None
Purpose	All security activities must be planned, coordinated, controlled and audited by nominated management structures (as demanded by BSI in its Annex A). ISO (*cf*. Annex B.3.2 a) recommends that SM should be supported on: (1) a security forum and (2) a security officer. With these two structures, the executive responsibility of SM is assigned to the security officer, while the security committee acts as a board of stakeholders, approving the major decisions and supervising all actions of SM.
Existing practices in ADETTI	Inexistence of a formal security management with defined responsibilities (A.4.1.3 in section 5.3.2 of the present document).
Methodology	**a) Decide the organization model of security management (SM)** The implementation advisor developed the following guideline principles, which were revised and approved by the Steering Committee. Three management levels were defined: (1) Strategic management should be entrusted to a security forum. It was decided that this forum would gather senior management (President of ADETTI), managers of units integrated in the evaluation scope (Administrative Unit Manager) and the security officer. (2) Tactical security responsibilities, as incident management for instance, would be assigned to specific employees and coordinated by the security officer. (3) Operational security tasks which are part of the daily tasks, as performing backups, would be assigned to specific employees, under the supervision of their respective field managers. **b) Identify requirements to operate security management (SM)** This task involved the identification of the requirements to ensure that the SM will be able to plan, organize, coordinate, control and audit all security activities. In this process, it was established: ▪ (1) the position of the security officer in ADETTI structure: a staff role reporting directly to the executive committee; ▪ (2) the SM responsibilities of the existing managers and specialised workers: theses responsibilities were defined in the ADETTI´s Policy Manual; ▪ (3) the relationship of the security officer and security forum with managers involved in the scope: for this purpose specific communication and cooperation mechanism were defined in the security procedures of ADETTI; ▪ (4) the budget and resource allocation for SM: the funding for SM will be provided by the general budget of ADETTI.

	c) Define the norms of security organization The activity of the security management structure will be delimited with these normative documents: ▪ general management responsibilities defined in the Policy Manual ▪ “Security Management Planning and Review” SMP02 in Annex E **d) Security management nomination** The SM structure is formed by: ▪ Security Forum – which assembles the President of ADETTI, managers of the units integrated in the evaluation scope (Administrative Unit Manager) and the security officer [see Security Procedure 2 - Security Management Planning and Review]. ▪ Security Officer – no decision was made about who will fulfil this position. ▪ Managers and employees of ADETTI – their new security responsibilities are defined in the Policy Manual and, in some cases, detailed by its supporting procedures.
Outcome	“Security Responsibility”, integrated in the Policy Manual (Annex D) “Security Management Planning and Review Procedure”, in Annex E

6.2.3 Work_Deliverable03: Supporting process of security norms

Requirement type	Mandatory requirement for BSI
Risk measures applicable	None
Purpose	Security norms crystallize security requirements for an organization at a specific point in time. Nevertheless, security requisites evolve through time. Therefore, it is required a continuous process to produce, publish, communicate to employees, enforce and revise the security norms.
Existing practices in ADETTI	No procedure to update security norms (see A.3.1.2 in section 5.3.2 of this document)
Methodology	**a) Decide the hierarchy of security norms** BSI demands - at least - the existence of two security regulations categories (policies and procedure). However, an organization is free to adhere to this model or adopt additional layers of security norms. [2] For a matter of simplicity, it was decided in ADETTI to define only two categories of security norms: policies and procedures. **b) Decide the ISMS documentation hierarchy** The documentation of ISMS is structured by a defined hierarchy, formed by different layers of documentation [BSI03a]. In ADETTI it was applied the following levels, as recommend by [BSI03a]: ▪ Tier 1 = formed by the strategic documents, i.e. policies statements compiled in the Policy Manual (Annex D). ▪ Tier 2 = ISMS supporting procedures, grouped in the Information Security Handbook. ▪ Tier 3 = Documents employed to collect, analyse or report data required by the security procedure. Examples report templates, audit plan template. ▪ Tier 4 = records of the execution of the security management tasks. This includes previous audit plans or reports of incidents. This hierarchy is depicted in the Policy Manual in page 15. In tier 1 and 2 appear two documents respectively entitled as Policy Manual and Information Security Handbook. These deliverables are the offspring of these decisions (which abide by the recommendations of other management systems implementers [Clements96], and [Seaver03]): - group all policies in a “security manual”. - assemble the procedures and other documents in a “security handbook”.

[2] In this context, an organization has at its disposal - for example - (1) the three layer norms suggested by ISO (policies, standards and procedures); or (2) the four level model of NIST (policies, standards, guidelines and procedures), as studied in Annex B.2.2.

c) Decide the structure of security documents

The structured of the previous established documents follow these guidelines:

- The Policy Manual adopts the structure recommended by [NHSWales04], [BSI03a], [AEXIS04]. Those authors recommend an organization that mimics the structure of the text of the BS 7799-2, as show next:
  - Introduction
  - Scope statement [product of 6.3.5 - Work_Deliverable05] Information Security Policy Statement [product of 6.3.1 Work_Deliverable01]
  - ISMS Approach
  - Security Responsibility [product of 6.3.2 - Work_Deliverable02]
  - ISMS Improvement [product of 6.3.13 - Work_Deliverable13]
- The Information Security Handbook, which is formed by the procedures and forms.
  - The procedures were viewed as the description of the sequences of actions performed by specific agents [Clements96]. Due to this concept, the procedures are composed by a flowchart, illustrating the tasks and the entities responsible for them. In each procedure, it was defined who is the process owner, responsible for supervising the practical conductance of the procedure.
  - The forms are the documents to register the conductance of the activities prescribed in the procedures. These templates were based on [Aceituno04], [Brainthwaite02], [BSI02] and [BSI03a].

d) Define the activities supporting the security norms life cycle

The activities related to development, production, publication, communication and revision of security norms and their related documents are described in ISMS Documentation Control Procedure.

In this context, it was decided that security norms would be:

- (1) composed by the implementation advisor, with the help of the actual managers and operatives involved in the actions that the norm covers,
- (2) approved by the steering committee,
- (3) publish and communicated to all employees covered by the norm (records must exist of this communication for legal reasons) [3] and
- (4) maintained and revised by a policy owner (who may act as the official interpreter of the norms, in case doubts in the application arise).

Each norm would be revised, at least, annually (as BSI establishes [BSI02]). The owner of policies is the Executive Board of ADETTI. Procedures are owned by or the S. Officer or by the Administrative Unit Manager (the operational manager with authority over the scope).

[3] Under the Portuguese law, citizens cannot justify an illegal act with the lack of knowledge of law; however the internal regulations of organizations are not covered by the law ignorance principle (Portuguese Civil Code [CódigoCivil00]). Therefore, an employee cannot be subjected to a disciplinary process, with the allegation of violating an internal regulation, if he proves that he was not informed of that particular directive. For this reason, the organization must maintain records of participation on training sessions, as well as written agreements of security regulations acceptance.

Outcome	"ISMS Documentation Control Procedure" integrated in the Information Security Handbook (Annex E) Policy Manual structure (illustrated in page 15 of Annex D

6.2.4 Work_Deliverable04: Asset management

Requirement type	Mandatory requirement for BSI
Risk measures applicable	None
Purpose	As new assets are added or changed, the inventory, developed in T04.2 (4.3 - Asset inventory) must be updated. The purpose of resource management is to establish an ongoing process to support the asset inventory.
Existing practices in ADETTI	A register of IT systems (as servers, desktops, laptops, communication devices among others) exists. Other types of assets associated with information systems as file cabinet are not inventoried. (see A.5.1.1 in section 5.3.2 of the present document).
Methodology	**a) Define norms for asset management** The Steering committee decided to follow the guidelines regarding asset management defined in the implementation process (which are described in the present document). This guidelines are established in the "Risk Management Procedure – SMP05" integrated in the Security Handbook (Annex E).
Outcome	"Risk Management Procedure" integrated in the Security Handbook (Annex E)

6.2.5 Work_Deliverable05: Scope management

Requirement type	Mandatory requirement for BSI
Risk measures applicable	None
Purpose	Process used to establish the scope and context of the ISMS
Existing practices in ADETTI	The operational procedure is described in the section 2.3.2 of this document.
Methodology	**a) Define the operational process under the scope** The organizational process existing in ADETTI, which was selected to be the scope of the security evaluation is the financial reporting. At this moment is reproduced as a formal procedure, the process depicted in the evaluation definition phase of the methodology [see phase 2 in section 2 of the present document]. **b) Define norms for scope management** As the scope is a part of ADETTI, its boundaries must be established and maintain as processes and assets change. To help to maintain the scope description updated the following documents were developed:

	• ISMS scope statement – a top level outline of the scope, which intends to do required constant amendments or updated; • Technological diagrams [included in the Implementation Report] • Physical diagrams [included in the Implementation Report] • Scope Management Procedure, which described the activities and responsibilities to maintain these documents are in the "integrated in the Security Handbook (Annex E).
Outcome	- "ADETTI financial reporting process" – which is the operational process, integrated in the Security Handbook (Annex E) - "ISMS Scope Statement", integrated in the Security Manual (Annex D) - "Scope Management Procedure" integrated in the Security Handbook (Annex E)

6.2.6 Work_Deliverable06: Risk management

Requirement type	Mandatory requirement for BSI
Risk measures applicable	None
Purpose	Establish the assets under the scope and then identify, assess and treat risks in a continuous manner.
Existing practices in ADETTI	No practice of risk management was found in ADETTI.
Methodology	**a) Define norms for risk management** The Steering committee decided to follow the guidelines regarding risk management defined in the implementation process (which are described in the present document). This guidelines are established in the "Risk Management Procedure – SMP05" integrated in the Security Handbook (Annex E). These procedures were applied in ADETTI and suffer several revisions: • The first version of this procedure started in the risk identification activity, then was decided to include the asset identification (to prevent developing another procedure just for asset management). • The second amendment was the inclusion of the legal compliance activity (identification of legal requisites). Because of this fact, it was reviewed the legal requirements defined in 3.3.1. • The third change was the inclusion of the "Detailed Risk Treatment Plan" to support the monitoring the application of controls (see this template in Annex E).
Outcome	- "Statement of Applicability", integrated in this document - "Security Responsibility", integrated in the Policy Manual (Annex D) - "Risk Management Procedure" integrated in the Security Handbook (Annex E)

6.2.7 Work_Deliverable07: Human resource management

Requirement type	Mandatory requirement for BSI
Risk measures applicable	Train and create awareness of security issues [A.6.2.1] - Risk 21, Risk77 Establish user practices to enable a more efficient and professional use of email [A.6.1.1] - Risk70, Train AUE2 to be a backup for the financial process [A.6.2.1] - Risk75
Purpose	ISO mandates security requirements to be tackled in human resources management (*cf.* Annex B.5.2): (1) incorporate security functions in job definition, (2) verify credentials of recruiters, (3) confidentiality agreements, (4) train employees and (5) define disciplinary procedures. Apart from these personnel issues, incidents management is considered by ISO as part of the human resource domain, therefore they are addressed in the present stage.
Existing practices in ADETTI	The following security practices were not found in ADETTI: job descriptions which include security responsibilities, verification of credentials, confidentiality agreements, security training and awareness or even incident reporting (A.6 in section 5.3.2 of the present document).
Methodology	**a) Define norms for human resource management** The several human resource management activities in ADETTI were depicted in a process approach in the human resource management procedure. In relation to the existing activities in ADETTI, the following actions were added or changed: • Development of a job description for the Security Officer [as available in Annex E] • Credential verification in recruitment [task added to the HR process, as show in Annex E] • Confidentiality agreements [available in Annex E] • Employees training and awareness procedure [template of training plan available in Annex E] • Disciplinary process definition This task required the involvement of human resource management of the organization to accommodate and adapt these security requirements into the existing personnel management practices. **b) Define norms for incident management** In ADETTI there was no procedure for the reporting of security incidents (see A.6.3.1 in section 5.3.2 of this document). The activities regarding incident management are addressed in the procedure SMP07.
Outcome	- “Security Responsibility”, integrated in the Policy Manual (Annex D) - “Human Resource Management Procedure” in the Information Security Handbook (Annex E) - “Incident Report Management Procedure” in Annex E

6.2.8 Work_Deliverable08: Information classification

Requirement type	Optional requirement for BSI
Risk measures applicable	Produce an Information labelling and handling procedure [A.5.2.2] - Risk54, Risk57
Purpose	One particular type of assets, the information resource, must be further classified in terms of security (see information classification).
Existing practices in ADETTI	There is no information classification procedure in ADETTI. (see A.5.2.2 in section 5.3.2 of the present document).
Methodology	**a) Define norms for information classification** An information classification norm establishes why and how a piece of information will be classified with a certain security category (*cf.* Annex B.4.3). Based on the CIA requirements of the several information types, identified in the asset registry it was established: • Only financial documents produced by the Administrative Unit to support the final financial report of the research projects and external documents received by the administrative unit, which are considered relevant by them, will be subject to security classification. • These documents will be classified by ADETTI´s personnel according to its confidentiality degree. • As a classification scale, in ADETTI will be employed three security levels: o Confidential o Internal o External • Documents classified will receive a security label (identifying labels to be used in the documentation). [4] • Based on these categorizations, particular procedures to handle information were defined. These questions are detailed in the “Document Classification Procedure”.
Outcome	“Document Classification Procedure” integrated in the Information Security Handbook (Annex E)

[4] An explicitly security label associated with documents has the advantage of facilitate the use by employees. However, it has the drawback to expose documents to the natural curiosity of someone who sees a document with a top-secret classification. In consequence, it is advisable to use a classification not explicitly, as showed in Data Classification Procedure.

6.2.9 Work_Deliverable09: Physical and environmental security management

Requirement type	Optional requirement for BSI
Risk measures applicable	Define norms for the physical security of the office and its equipment [A.7.1.3] - Risk06 Install a surveillance camera at the office lobby [A.7.1.1] - Risk06
Purpose	Protect the facilities and resource of ADETTI against physical and environmental risks.
Existing practices in ADETTI	The Administrative Unit employees of ADETTI have several physical security practices. As showed in A.7.1 there is a high conformity level of ADETTI with BSI requirements in this area.
Methodology	**a) Define norms for physical and environmental security** Although physical security practices were identified in ADETTI (e.g. "Every time the last staff member exits the room, it closes it down" documented in A.7.1 in section 5.3.2 of this document); the risk of robbery was deemed as unacceptable, and two countermeasures are proposed: - Install a surveillance camera at the office lobby [A.7.1.1] - Define norms for the physical security of the office and its equipment [A.7.1.3] In relation to first issue (surveillance camera) it was decided to implement in a time frame outside the present academic project. According to the defined in 6.1.2.3, it was develop the "Detailed Risk Treatment Plan". In relation to the second aspect physical practices were defined as "Recommended Security Practices"
Outcome	Integration of practices in "Recommended Security Practices", which is a supporting document of the "Human Resource Management Procedure" in the Information Security Handbook (Annex E)

6.2.10 Work_Deliverable10: Communications and operations management

Requirement type	Optional requirement for BSI
Risk measures applicable	Update malicious code software (from McAffe 7.0 to McAffe 8.0) [A. 8.3.1]– Risk19, Risk23 Develop IT maintenance procedure [A.8.1.1] - Risk29 Develop procedures for regular IT maintenance for the systems that support the SMTP service [A.8.1.1] - Risk69 Develop a procedure to test and backups [A.8.4.1] - Risk32
Purpose	This domain addresses an organization's ability to ensure the correct and secure operation of its assets (*cf*. Annex B.7.2). The various areas of this domain are conducted by the IT service provider.
Existing practices in ADETTI	In the following issues it was found nonconformities in ADETTI (A.8 in section 5.3.2 of the present document): i. Capacity planning ii. System acceptance iii. Controls against malicious software iv. Information back-up v. Operator logs
Methodology	**a) Define norms for communications and operations security** Due to the risks (Risk29, Risk69, Risk32) relating to the lack of denied procedures in IT operations it was defined: ▪ a group of maintenance tasks, with fixed frequency, to be performed by the IT Service Provider; ▪ a reporting mechanism for all IT operations (task not dealt in the previous group of task).
Outcome	"IT Operations Management Procedure" integrated in the Information Security Handbook (Annex E)

6.2.11 Work_Deliverable11: Access control management

Requirement type	Optional requirement for BSI
Risk measures applicable	Implementing access control from ADETTI network to the ISCTE network (reinforce firewall policies) [A.9.4.6] - Risk 20, Risk24, Risk26, Risk28, Risk38 Deploy an SMTP server for ADETTI separately from ISCTE [A.9.4.6] – Risk69, Risk70 Develop access control procedure [A.9.2.2] Risk27, Risk59
Purpose	This domain aims to ensure the management of access control, preventing the unauthorised access to information and supporting IT resources.
Existing practices in ADETTI	There are no formal access control procedures. Permissions are granted in a “Need to Know” basis. For example only the ADU manager has administrator credentials in the BSCW software (A.9. in section 5.3.2 of the present document).
Methodology	**a) Define access control norms** In order to counter the risks of inadequate access control management (related to Risk27 and Risk59) it was decided to develop a registration and authorization mechanism of all access request from: - a new employee of the Administrative Unit; - a existing employee of ADETTI who needs to access the final financial reports - a existing employee of ADETTI who needs to use laptops, which is property of ADETTI - an new or existing partner who needs to access the financial statements integrated in the final financial report. In this procedure, the S. Officer will authorize or reprove the requests and register the accesses granted. **b) Identify mechanisms to segregate the ADETTI from ISCTE network** It was identified by a number of risks (Risk20, Risk24, Risk26, Risk28, Risk38, Risk69, Risk70) the need to isolate ADETTI network from ISCTE. To attain this objective two measures were proposed: ▪ Deploy an SMTP server for ADETTI separately from ISCTE ▪ Reinforce the access control applying more stringent firewall policy at the point of connection between ADETTI network and ISCTE. This firewall policy will block all traffic, except SMTP, HTTP from ISCTE gateway. All other traffic from ISCTE will be blocked. The application of these two measures requires an assessment of the network and applications dependencies of ADETTI resources on the ISCTE infrastructure, which was not performed during this case study.
Outcome	“Access Control Management Procedure” integrated in the Information Security Handbook (Annex E)

6.2.12 Work_Deliverable12: System development and maintenance management

Requirement type	Optional requirement for BSI
Risk measures applicable	None
Purpose	To ensure that security is built into the several life cycle phases of a system: development or acquisition, implementation, maintenance and disposal (see Annex B.9.3).
Existing practices in ADETTI	It was found in ADETTI (A.10 in section 5.3.2 of the present document): ▪ Encryption is not employed to protect business data under the scope. The only encrypted data found was the Windows user database. Digital signatures are not used. ▪ There is no formal security assessment of the acquired system.
Methodology	As any of the identified safeguard was related to this security domain, no process or control was defined.
Outcome	None

6.2.13 Work_Deliverable13: Business continuity management

Requirement type	Optional requirement for BSI
Risk measures applicable	Develop a Business Continuity Management that includes fire situations [A.11.1.3] – Risk02, Risk04 Train fire procedures under the BCM framework [A.11.1.5] - Risk02
Purpose	This domain is concerned with the definition of the steps and responsibilities to ensure the analysis, planning, testing and maintenance of Business Continuity. The established process should follow the sequence of phases of a BC process, defined by ISO (in Annex B.10.2).
Existing practices in ADETTI	Previously, in the vulnerability assessment performed in ADETTI the following was noticed: I. Business continuity concerns were found in ADETTI, but not structured as a managed process (define, plan, write, test, revise a plan). II. An informal assessment of the most critical data in case of a disaster was performed. This assessment did not include resources to ensure continuity of services. III. It was not found evidences of planned actions to be performed in the event of a major disaster.
Methodology	**a) Define the general framework for business continuity management** To initiate the development of BC plans, it was composed a procedure, which was based on the "Seven-Step Business Continuity Planning Model" from Disaster Recovery Institute, 2003.
Outcome	"Business Continuity Framework" in Annex E

6.2.14 Work_Deliverable14: Compliance and continual improvement management

Requirement type	Mandatory requirement for BSI
Risk measures applicable	Develop procedure that includes the verification of legal compliance –[A.12.1.4] – Risk61
Purpose	An ISMS, as any management system, must have in place mechanisms to ensure an continuous improvement of its effectiveness and to assure compliance with the BSI, legal and business requirements.
Existing practices in ADETTI	There is no formal identification of legal requirements related to the information handled by ADETTI. However, ADETTI has a contracted service of legal counselling that ensures that the activities of the Association are compliant with the Law. A not written procedure is followed to protect software copyrights. All software is registered in a software inventory. The licenses are maintained in a defined file cabinet. Source: A.12 in section 5.3.2 of this document
Methodology	**a) Define norms for compliance and continual improvement management** To ensure a stance in the organization of security *kaisen* (continual improvement), it was established a process to collect improvements measures, plan, implement and control its application. This process is the Security Management Planning and Review Procedure – SMP02. The revision of the ISMS accepts inputs from: - Follow-up actions from the previous reviews - Status of corrective and preventive actions (this is a output of an specific audit procedure) - Audits results (which is the output of an specific audit procedure) - Revision of risk management (made by the Security Officer, every 6 months) - Revision of policies and procedures (policies and procedure are review annually) - Opportunities for the improvement (suggestions made by employees) All these data is collected in the “Management Review Input Report”, a document made by the Security officer. The outcome of this step is: - the principles defined as the ISMS Improvement policy (in Policy Manual) - the procedure to conduct regular audit to assess the ISMS effectiveness - the process to identify, apply and monitor actions to prevent and correct nonconformities. - the process to carry out a management review of the ISMS All these decisions are compiled in the “Management Review Output”, as detailed in Security Management Planning and Review Procedure” in the Information Security Handbook.

b) Compose the Statement of Applicability (SoA)

The structure of Statement of Applicability follows the recommendations of Kadam [03], as discussed in section 3.9.3 in the dissertation text. The document is formed by the following sections:

- Number - Clause number of BS-7799-2
- Clause - BSI Control Objective of BS-7799-2
- Applied - Yes or No
- Rationale - Reasons for the selection or exclusion of controls
- Risk Reference - A code for each risk identified by the organization
- ISMS Document Reference - An identification for controls adopted by the organization

The control objectives are selected if:

- one or more of the controls corresponds to the identified risks;
- some of the controls are applied by the mandatory security procedures.

Outcome

- "ISMS Improvement" integrated in the Security Manual (Annex D)
- "Security Management Planning and Review Procedure" in the Information Security Handbook
- "ISMS Audits", in the Information Security Handbook (Annex E)
- "Corrective and Preventive Actions Procedure" in the Information Security Handbook (Annex E)
- Statement of Applicability (in this document)

Statement of Applicability

1. Controls selected

N.	Clause	Applied	Rationale	Risk reference	ISMS document reference
A.3 Security policy					
A.3.1 Information security policy Control objective: To provide management direction and support for information security.					
A.3.1.1	Information security policy document	Yes		R77	1.1 Policy Manual
A.3.1.2	Review and evaluation	Yes			2.4 ISMS Documentation Control
A.4 Organizational security					
A.4.1 Information security infrastructure Control objective: To manage information security within the organization.					
A.4.1.1	Management information security forum	Yes			1.1 Policy Manual
A.4.1.2	Information security coordination	Yes			1.1 Policy Manual 2.2 Security Management Planning and Review
A.4.1.3	Allocation of information security responsibilities	Yes			1.1 Policy Manual
A.4.1.4	Authorization process for information processing facilities	Yes			2.11 Access Control
A.4.1.5	Specialist information security advice	No	ADETTI has internal expertise.		
A.4.1.6	Cooperation between organizations	No	ADETTI has internal expertise.		

A.4.1.7	Independent review of information security	Yes			2.9 ISMS Audits
A.4.2 Security of third-party access Control objective: To maintain the security of organizational information processing facilities and information assets accessed by third parties.					
A.4.2.1	Identification of risks from third-party access	Yes			2.11 Access Control
A.4.2.2	Security requirements in third-party contracts	No	It is not possible to include security requirements in the existing contracts.		
A.4.3 Outsourcing Control objective: To maintain the security of information when the responsibility for information processing has been outsourced to another organization.					
A.4.3.1	Security requirements in outsourcing contracts	No	It is not possible to include security requirements in the existing contracts.		
A.5 Asset classification and control					
A.5.1 Accountability for assets Control objective: To maintain appropriate protection of organizational assets.					
A.5.1.1	Inventory of assets	Yes			2.5 Risk Management
A.5.2 Information classification Control objective: To ensure that information assets receive an appropriate level of protection.					
A.5.2.1	Classification guidelines	Yes			2.8 Document Classification
A.5.2.2	Information labelling and handling	Yes			2.8 Document Classification
A.6 Personnel security					
A.6.1 Security in job definition and resourcing Control objective: To reduce the risks of human error, theft, fraud or misuse of facilities.					
A.6.1.1	Including security in job responsibilities	Yes		R70	2.6 Human Resource Management

A.6.1.2	Personnel screening and policy	Yes			2.6 Human Resource Management
A.6.1.3	Confidentiality agreements	Yes			2.6 Human Resource Management
A.6.1.4	Terms and conditions of employment	Yes			2.6 Human Resource Management
A.6.2 User training Control objective: To ensure that users are aware of information security threats and concerns, and are equipped to support organizational security policy in the course of their normal work.					
A.6.2.1	Information security education and training	Yes		R77,	2.6 Human Resource Management
A.6.3 Responding to security incidents and malfunctions Control objective: To minimize the damage from security incidents and malfunctions, and to monitor and learn from such incidents.					
A.6.3.1	Reporting security incidents	Yes			2.7 Incident Report Management
A.6.3.2	Reporting security weaknesses	Yes			2.7 Incident Report Management
A.6.3.3	Reporting software malfunctions	Yes			2.7 Incident Report Management
A.6.3.4	Learning from incidents	Yes			2.7 Incident Report Management
A.6.3.5	Disciplinary process	Yes			2.7 Incident Report Management
A.7 Physical and environmental security					
A.7.1 Secure areas Control objective: To prevent unauthorized physical access, damage and interference to business premises and information.					
A.7.1.1	Physical security perimeter	Yes		R06	2.6 Human Resource Management
A.7.1.2	Physical entry controls	Yes			2.6 Human Resource Management
A.7.1.3	Securing offices, rooms and facilities	Yes		R06	2.6 Human Resource Management
A.7.1.4	Working in secure areas	Yes			2.11 Access Control Management
A.7.1.5	Isolated delivery and loading areas	No	It was not identified risks related with delivery areas.		
A.7.2 Equipment security Control objective: To prevent loss, damage or compromise of assets and interruption to business activities.					

A.7.2.1	Equipment siting and protection	No			
A.7.2.2	Power supplies	No			
A.7.2.3	Cabling security	No			
A.7.2.4	Equipment maintenance	Yes			2.12 IT Operations Management
A.7.2.5	Security of equipment off-premises	No	There is no equipment being used off-premises, therefore this control is not applicable.		
A.7.2.6	Secure disposal or re-use of equipment	No			
A.7.3 General controls Control objective: To prevent compromise or theft of information and information processing facilities.					
A.7.3.1	Clear desk and clear screen policy	Yes			2.6 Human Resource Management
A.7.3.2	Removal of property	No	There is no property removed from the ADETTI office of during the normal work processes.		
A.8 Communications and operations management					
A.8.1 Operational procedures and responsibilities Control objective: To ensure the correct and secure operation of information processing facilities.					
A.8.1.1	Documented operating procedures	Yes		R69	2.12 IT Operations Management
A.8.1.2	Operational change controls	No			
A.8.1.3	Incident management procedures	Yes			2.7 Incident Report Management
A.8.1.4	Segregation of duties	No			2.12 IT Operations Management
A.8.1.5	Separation of development and operational facilities	No	Not applicable to the area under evaluation.		
A.8.1.6	External facilities management	No	Not applicable to the area under evaluation.		

A.8.2 System planning and acceptance Control objective: To minimize the risk of systems failure.					
A.8.2.1	Capacity planning	No	Not applicable to the area under evaluation.		
A.8.2.2	System acceptance	No	Not applicable to the area under evaluation.		
A.8.3 Protection against malicious software Control objective: To protect the integrity of software and information from damage by malicious software.					
A.8.3.1	Controls against malicious software	Yes		R19, R23	2.12 IT Operations Management
A.8.4 Housekeeping Control objective: To maintain the integrity and availability of information processing and communication services.					
A.8.4.1	Information back-up	Yes		R32	2.12 IT Operations Management
A.8.4.2	Operator logs	Yes			2.12 IT Operations Management
A.8.4.3	Fault logging	Yes			2.12 IT Operations Management
A.8.5 Network management Control objective: To ensure the safeguarding of information in networks and the protection of the supporting infrastructure.					
A.8.5.1	Network controls	Yes			Apply more stringent firewall policies
A.8.6 Media handling and security Control objective: To prevent damage to assets and interruptions to business activities.					
A.8.6.1	Management of removable computer media	Yes			2.12 IT Operations Management
A.8.6.2	Disposal of media	Yes			2.12 IT Operations Management
A.8.6.3	Information handling procedures	Yes			2.8 Document Classification
A.8.6.4	Security of system documentation	Yes			2.8 Document Classification
A.8.7 Exchanges of information and software Control objective: To prevent loss, modification or misuse of information exchanged between organizations.					

A.8.7.1	Information and software exchange agreements	No	Not applicable.		
A.8.7.2	Security of media in transit	No	Not applicable.		
A.8.7.3	Electronic commerce security	No	Not applicable.		
A.8.7.4	Security of electronic mail	No	Not applicable.		
A.8.7.5	Security of electronic office systems	No	Not applicable.		
A.8.7.6	Publicly available systems	No	Not applicable.		
A.8.7.7	Other forms of information exchange	No	Not applicable.		
A.9 Access control					
A.9.1 Business requirement for access control Control objective: To control access to information.					
A.9.1.1	Access control policy	Yes			1.1 Policy Manual
A.9.2 User access management Control objective: To ensure that access rights to information systems are appropriately authorized, allocated and maintained.					
A.9.2.1	User registration	Yes			2.11 Access Control
A.9.2.2	Privilege management	Yes			2.11 Access Control
A.9.2.3	User password management	Yes			2.11 Access Control

A.9.2.4	Review of user access rights	Yes			2.11 Access Control
A.9.3 User responsibilities Control objective: To prevent unauthorized user access.					
A.9.3.1	Password use	Yes			2.6 Human Resource Management
A.9.3.2	Unattended user equipment	Yes			2.6 Human Resource Management
A.9.4 Network access control Control objective: Protection of networked services.					
A.9.4.1	Policy on use of network services	Yes			2.6 Human Resource Management
A.9.4.2	Enforced path	No	Deemed as not required.		
A.9.4.3	User authentication for external connections	Yes	Already implemented (see section 5.3.2).		
A.9.4.4	Node authentication	No	Deemed as not required.		
A.9.4.5	Remote diagnostic port protection	No	ADETTI does not manage the Internet gateway. The switches have this port disabled.		
A.9.4.6	Segregation in networks	Yes		R20, R24, R28, R38	- Apply more stringent firewall policies - Deploy an SMTP server for ADETTI separately from ISCTE
A.9.4.7	Network connection control	No			
A.9.4.8	Network routeing control	No			
A.9.4.9	Security of network services	No			
A.9.5 Operating system access control Control objective: To prevent unauthorized computer access.					

A.9.5.1	Automatic terminal identification	No	ADETTI does not manage the Internet gateway. The switches have this port disabled.		
A.9.5.2	Terminal log-on procedures	No	ADETTI does not manage the Internet gateway. The switches have this port disabled.		
A.9.5.3	User identification and authentication	No	ADETTI does not manage the Internet gateway. The switches have this port disabled.		
A.9.5.4	Password management system	No	ADETTI does not manage the Internet gateway. The switches have this port disabled.		
A.9.5.5	Use of system utilities	No	ADETTI does not manage the Internet gateway. The switches have this port disabled.		
A.9.5.6	Duress alarm to safeguard users	No	This control is not necessary in the ADETTI. The risk assessment has not identified any situation making this control necessary.		
A.9.5.7	Terminal time-out	No	ADETTI does not provide terminals outside their office facilities, where such a control would be required.		
A.9.5.8	Limitation of connection time	No	ADETTI does not provide any connection types where this control would make sense.		
A.9.6 Application access control Control objective: To prevent unauthorized access to information held in information systems.					
A.9.6.1	Information access restriction	Yes			2.11 Access Control
A.9.6.2	Sensitive system isolation	No	All users need to access the same data, no system isolation.		

A.9.7 Monitoring system access and use Control objective: To detect unauthorized activities.					
A.9.7.1	Event logging	Yes			2.12 IT Operations Management
A.9.7.2	Monitoring system use	Yes			2.12 IT Operations Management
A.9.7.3	Clock synchronization	Yes	Computers clocks are synchronized in ADETTI. The maintenance of this situation depends on procedure 2.12.		2.12 IT Operations Management
A.9.8 Mobile computing and teleworking Control objective: To ensure information security when using mobile computing and teleworking facilities.					
A.9.8.1	Mobile computing	Yes			2.11 Access Control
A.9.8.2	Teleworking	Yes			2.11 Access Control
A.10 System development and maintenance					
A.10.1 Security requirements of systems Control objective: To ensure that security is built into information systems.					
A.10.1.1	Security requirements analysis and specification	No	In the Administrative Unit systems are standard and do not require security specification.		
A.10.2 Security in application systems Control objective: To prevent loss, modification or misuse of user data in application systems.					
A.10.2.1	Input data validation	No	The risk assessment has not shown any need to apply this control.		
A.10.2.2	Control of internal processing	No	The risk assessment has not shown any need to apply this control.		

A.10.2.3	Message authentication	No	The risk assessment has not shown any need to apply this control.		
A.10.2.4	Output data validation	No	The risk assessment has not shown any need to apply this control.		
A.10.3 Cryptographic controls Control objective: To protect the confidentiality, authenticity or integrity of information.					
A.10.3.1	Policy on the use of cryptographic controls	No	There are no cryptographic controls in the scope.		
A.10.3.2	Encryption	No	There are no cryptographic controls in the scope.		
A.10.3.3	Digital signatures	No	There are no cryptographic controls in the scope.		
A.10.3.4	Non-repudiation services	No	There are no cryptographic controls in the scope.		
A.10.3.5	Key management	No	There are no cryptographic controls in the scope.		
A.11 Business continuity management					
A.11.1 Aspects of business continuity management Control objective: To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters.					
A.11.1.1	Business continuity management process	Yes	BC plans will be develop in the future according to procedure 2.12		2.12 Business Continuity Framework
A.11.1.2	Business continuity and impact analysis	Yes	BC plans will be develop in the future according to procedure 2.12		2.12 Business Continuity Framework
A.11.1.3	Writing and implementing continuity plans	Yes	BC plans will be develop in the future according to procedure 2.12	R02, R04	2.12 Business Continuity Framework
A.11.1.4	Business continuity planning framework	Yes	BC plans will be develop in the future according to procedure 2.12		2.12 Business Continuity Framework

A.11.1.5	Testing, maintaining and re-assessing business continuity plans	Yes	BC plans will be develop in the future according to procedure 2.12	R02	2.12 Business Continuity Framework
A.12. Compliance					
A.12.1 Compliance with legal requirements Control objective: To avoid breaches of any criminal and civil law, statutory, regulatory or contractual obligations and of any security requirements.					
A.12.1.1	Identification of applicable legislation	Yes	Risk Management Procedure includes identification and application of legal requirements.		2.5 Risk Management
A.12.1.2	Intellectual property rights (IPR)	Yes	Legal compliance is verified by management review (procedure 2.2) and proper software copyright is follow in IT operations (2.12)		2.2 Security Management Planning and Review 2.12 IT Operations Management
A.12.1.3	Safeguarding of organizational records	Yes	This control already exists in ADETTI (includes identification and application of legal requirements).		2.5 Risk Management
A.12.1.4	Data protection and privacy of personal information	Yes	This control already exists in ADETTI, will be reinforced by the Risk Management Procedure (includes identification and application of legal requirements).	R61	2.5 Risk Management
A.12.1.5	Prevention of misuse of information processing facilities	Yes			2.11 Access Control
A.12.1.6	Regulation of cryptographic controls	No	Not applicable within the scope.		
A.12.1.7	Collection of evidence	Yes	Legal compliance in the evidence collection is followed in procedure 2.7		2.7 Incident Report Management
A.12.2 Reviews of security policy and technical compliance Control objective: To ensure compliance of systems with organizational security policies and standards.					
A.12.2.1	Compliance with security policy	Yes			2.2 Security Management Planning and Review

A.12.2.2	Technical compliance checking	Yes			2.9 ISMS Audits
A.12.3 System audit considerations Control objective: To maximize the effectiveness of and to minimize interference to/from the system audit process.					
A.12.3.1	System audit controls	Yes			2.9 ISMS Audits
A.12.3.2	Protection of system audit tools	Yes			2.9 ISMS Audits
A.12.3.1	System audit controls	Yes			2.9 ISMS Audits

2. Conclusions from the Statement of Applicability

1. In total, 70 controls were regarded as applied, 49 controls deemed as not necessary and 8 not applicable. Some ISO measures were applied because they correspond to BSI mandatory requirements (e.g. the control A.3.1.1 - Information security policy document is fulfilled by the “Policy Manual”)

2. Some ISO measures were applied because they correspond to BSI mandatory requirements (e.g. the control A.3.1.1 - Information security policy document is fulfilled by the “Policy Manual”)

7. Time consumption

7.1 Time consumption in the implementation project (present case-study)

Task	Activities	Resource								Total
		Implementation advisor	President of ADETTI	Scope			Functions			
				AUM	AUE1	AUE2	IT	HR *	Purchase *	
T01.1	Project management model	4 hours	0,5 hour	1 hour						6
	Steering Committee informed	8 hours	0,5 hour	1 hour						10
T02.1	Decision criteria for scope selection	4 hours	0,5 hour	1 hour						6
T02.2	Scope selection	8 hours	0,5 hour	1 hour						10
	Process description	8 hours	0,5 hour	2 hours	2 hours					13
	Organizational structure	4 hours	0,5 hour			1 hour				5
	Physical description	8 hours				1 hour				9
	Technological description	16 hours	0,5 hour	1 hour			4 hours			24
T02.3	Interfaces and dependencies of the ISMS	8 hours	0,5 hour	2 hours		2 hours				13
T03.1	List of business requirements for SM	4 hours	0,5 hour	1 hour		2 hours				8
T03.2	List of legal requirements for SM	8 hours				1 hour				9
	List of contractual requirements for SM	8 hours		1 hour						9
T04.1	Asset inventory structure	8 hours	0,5 hour	1 hour						10
T04.2	Asset inventory completed	24 hours	0,5 hour	1 hour	1 hour	3 hours				30
T05.1	Risk calculation formula	8 hours	0,5 hour	1 hour						10
T05.2	Identification of threats	6 hours	0,5 hour	1 hour			2 hours			10
	Identification of vulnerabilities	16 hours		1 hour	2 hours	3 hours	3 hours			25
	List of risk	32 hours	1 hour	1 hour	1 hour	4 hours	1 hour			40
T05.3	Risk acceptance criteria	2 hours	0,5 hour	1 hour						4
T05.4	Risk Treatment Plan	16 hours	1 hour	2 hours			1 hour			19
T06.1	Work_Deliverable01: Information security policy	24 hours	0,5 hour	1 hour						26
	Work_Deliverable02: Organization of security management	8 hours	0,5 hour	1 hour				1 hour		11

	Work_Deliverable03: Supporting process of security norms	16 hours	0,5 hour	1 hour						18
	Work_Deliverable04: Asset management	6 hours	0,5 hour	1 hour						8
	Work_Deliverable05: Scope management	6 hours	0,5 hour	1 hour						8
	Work_Deliverable06: Risk management	24 hours	0,5 hour	1 hour						26
	Work_Deliverable07: Human resource management	8 hours	0,5 hour	1 hour				2 hours		12
	Work_Deliverable08: Physical and environmental management	8 hours	0,5 hour	1 hour						10
	Work_Deliverable09: Communications and operations management	8 hours	0,5 hour	1 hour						10
	Work_Deliverable10: Access control management	8 hours	0,5 hour	1 hour						10
	Work_Deliverable11: System development and maintenance mgn	0 hours	0,5 hour	0 hour						0
	Work_Deliverable12: Business continuity management	8 hours	0,5 hour	1 hour						10
	Work_Deliverable13: Compliance and continual improvement mgn	32 hours	0,5 hour	1 hour						10
Total hours		356 hours	15 hours	32 hours	6 hours	7 hours	11 hrs	1 hour	0 hour	440
Total days		45 days	2 days	4 days	1 day	2 days	1 day	1day	0 day	56 days

This case study required, broadly, 45 days from the implementation advisor and 11 days from ADETTI personnel, in a total of 56 days.

* - Performed by AUM.

ANNEX D

POLICY MANUAL

The present document is required by BSI for organizations to attain the security certification.

This document is an output of the phase 6 of the implementation methodology proposed in Annex C. The structure and content of the present document is discussed in Annex C, section 6.2.3 - Work_Deliverable03: Supporting process of security norms.

POLICY MANUAL

Label: 1.0
Version: 03.100804
Approved by: José Miguel Dias on 11/08/04

Completion of the following signature blocks signifies the review and approval of this document (signed copy held in safe)

Participants

Name	Name	Signature	Date
Authored by:	Paulo Alves Coelho		30/05/2004
Reviewed by:	José Miguel Dias		11/08/2004
Approved by:	José Miguel Dias		11/08/2004

Version Table

Version	Author	Reason	Date
01.100804	Paulo Coelho	Initial document version	30/05/2004
02.100804	Paulo Coelho	Incorporation of new components (procedures). Modifications in scope statement and Strategic Information Security Policy.	14/07/2004
03.100804	Paulo Coelho	Final document version	10/08/2004

TABLE OF CONTENTS

0. Introduction

0.1 Objective

The present document "Policy Manual" is the foundation stone of the Information Security Management System (ISMS) of the Associação para o Desenvolvimento das Telecomunicações e Técnicas de Informática (ADETTI).

The present Manual provides a top-level description of the information security management system designed for ADETTI during the case study.

0.2 Compliance with the British Standard 7799-2:2002 (BSI)

ADETTI, in order to achieve the certification of its ISMS, must present evidence that its security management processes were designed in order to provide an adequate and proportionate level of protection against the organization's overall risks and taking into account the requirements of ADETTI's management, employees, partners and other interested parties.

In light of this requisite, the present Manual compiles the policies developed by ADETTI in order to demonstrate the compliance of the ISMS of ADETTI with the requirements of British Standard 7799-2:2002 or simply BSI.

0.3 Revision

The present document can be revised in a global level or altered in each of its constituent documents.

In case of a global revision, the version number of all documents must be incremented (adding a unit to the number at left of the point).

All amendments derived from a revision must be recorded in the Version Table, as illustrated in page 3 of this document.

After each revision, the new printout sheets must be provided to all authorised holders of this document.

The revision process of this document is established by the Security Management Procedure 4 - ISMS Documentation Control.

0.4 Distribution

Holder	Format	
	Paper Number of copies	Electronic
President of ADETTI	1	
Administrative Unit Manager	1	
Security Officer	1	X

0.5 Definitions, acronyms and abbreviations

ADETTI
Associação para o Desenvolvimento das Telecomunicações e Técnicas de Informática

Availability
Ensuring that authorized users have access to information and associated assets when required [BS ISO/IEC 17799:2000]

Asset
Anything that has value to an organization [Humphreys02b:p.13].

Confidentiality
Ensuring that information is accessible only to those authorized to have access [BS ISO/IEC 17799:2000]

Continual improvement
Recurring process of enhancing the security management system.

Corrective Action
Action to eliminate the cause of a detected nonconformity or other undesirable situation.

Countermeasure
The same as a security control (see below).

Degree of assurance
Level of protection of an asset required by business needs.

Evaluation area
The organization's area subject to the security evaluation process. This area is defined by its activities, resources, locations and types of information.

Evaluation criteria
The same as risk acceptance criteria: the group of criteria used by organizations to classify risks as acceptable or unacceptable.

Information
The meaning that is currently assigned to data by means of the conventions applied to that data [Humphreys02b:p.14]. Information can be stored in an electronic format or by any means. An example is intellectual information, which is stored in people's minds.

Information security
Preservation of confidentiality, integrity and availability of information

ISMS
Information Security Management System - That part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security NOTE The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.

Integrity
Safeguarding the accuracy and completeness of information and processing methods [BS ISO/IEC 17799:2000].

Impact
The result of an unwanted incident [ISO96] in an organization [AS99].

Preventive Action
Action to eliminate the cause of a potential nonconformity or other undesirable potential situation.

Process	Set of interrelated or interacting activities which transforms inputs into outputs.
PDCA	Plan, Do, Check, Act
Risk acceptance	Decision to accept a risk [ISO Guide 73]
Risk analysis	Systematic use of information to identify sources and to estimate the risk [ISO Guide 73]
Risk assessment	Overall process of risk analysis and risk evaluation [ISO Guide 73]
Risk evaluation	Process of comparing the estimated risk against given risk criteria to determine the significance of risk [ISO Guide 73]
Risk management	Coordinated activities to direct and control an organization with regard to risk [ISO Guide 73]
Risk treatment	Treatment process of selection and implementation of measures to modify risk [ISO Guide 73]
Statement of applicability	Document describing the control objectives and controls that are relevant and applicable to the organization’s ISMS, based on the results and conclusions of the risk assessment and risk treatment processes
Security Plan	Documents specifying which procedures and associated resources shall be applied by whom and when.
SOA	Statement of Applicability
S.Officer	Security officer
S. Forum	Security forum
Security control	A practice, procedure or mechanism that mitigates security risk [Humphreys02b:p.14].
Security control catalogue	A list of recommended security controls. Examples studied in this research are ISO [ISO00a], GMITS [ISO00b] COBIT [ISACA00] and NIST Handbook [NIST95].
Threat	A potential cause of an unwanted incident [ISO96], which affects the CIA dimensions of security and results in harm to an organization.
Vulnerability	A weakness of an asset, a flaw in the organizational policies or worker’s actions, that allows a threat to cause harm [ISO96], [Alberts02].

1. ISMS Scope

1.1 Scope statement

The management of information security in ADETTI covers the protection of the financial information of the final reports of the funded scientific research projects.

1.2 Scopes dimensions

1.2.1 Types of information covered by the scope

The scope involves (1) all financial documents, which may represent an income or an expenditure of a specific project, (2) the accounting data of a specific project (3) working documents used to produce the financial component of the project's final report.

All of this information may reside in electronic or paper format.

The financial information of projects which ended more than 5 years ago may not be considered as included in the scope.

1.2.2 Activities covered by the scope

The activities conducted to collect, prepare, stored and retrieve the financial information submitted in the final report of projects fall under the scope of security management. These activities were depicted as forming a process, as described in the Financial Reporting Procedure - SMP01 [Annex E].

1.2.3 Organizational scope

The mentioned activities are carried out by the administrative unit of ADETTI with the support of the project leader of each project.

1.2.4 Assets included in the ISMS

The scope covers the resources deemed as critical for the protection of financial information, including:

- the administrative unit manager;
- the projects and accounting file cabinets;
- the ADETTI financial application;
- the BCSW server (where reports are kept in electronic format);
- IT systems and other resources employed in the execution of the activities related to information type regarded as business critical.

The relationships between these assets and other resources outside the scope are enumerated in this document in section 1.3.

A detailed breakdown of the assets included in the ISMS can be found in the Asset Inventory, in Annex C [section 4.3].

1.2.5 Physical location

The activities included in the ISMS are conducted in the administrative room, in the ISCTE building.

1. 3 ISMS interfaces

1.3.1 Interfaces

The organizational process under the ADETTI ISMS interfaces with the following entities:

Type of entities	**Name of the entities**	**Relationship with the scope**	**Role in the process**
Funding organizations	European Commission and *Fundação da Ciência e Tecnologia*	External organization	Client of the process deliverable (to whom the reports are submitted)
Project leaders	Project Leader1, Project Leader2, etc.	ADETTI members outside the scope	Owner of the process under the scope (who supervise the overall process of the report composition)
Accountant		External organization	Service provider (keeps all the records and audits all the financial statement)
Courier company		External organization	Service provider (transport all financial documentation to the accountant)
Research partners (if applicable)		External organization	
ISCTE	ISCTE	Partner organization	Service provider (internal data networking services)
Communication providers	Portugal Telecom FCCN (ISCTE)	External organization	Service provider (Portugal Telecom for voice communication and FCCN, which provides Internet access for ISCTE)
IT services provider		External organization	Service provider (maintains the ICT environment)
Utilities	EDP EPAL	External organization	Service provider (provide electricity – EDP - and water – EPAL - to the ISCTE compound)

1.3.2 Interdependency

The ADETTI ISMS is dependent on the following from the external services:

- Timely delivery of the financial documentation of the project by the project leader to allow the correct reservations and bookings to be made;
- Timely and accurate provision of accountant services;
- Ensuring that the mail service is running, secure and accessible to authorised users at all times;
- Ensuring that the desktops and laptops of the Administrative Unit are in conditions to function;
- Reliable provisioning of electricity, water services for the office.

1.4 Process conducted to define the ISMS scope

The ISMS scope was selected according to the procedure described in the Implementation Report [Annex C].

2. Information Security Policy Statement

2.1 Purpose

The purpose of Information Security Management in ADETTI is to ensure the continuity and protection of the financial reporting process of the scientific research projects conducted by ADETTI.

2.2 Objectives

The Information Security Management of ADETTI intends to ensure:

- Confidentiality of the deliverables of research projects (information is not disclosed to unauthorised persons through deliberate or careless action).
- Integrity of the deliverables of research projects through protection from unauthorised modification.
- Availability of the deliverables of research projects to authorised users when needed.
- Minimize the impact of security incidents on the operation of ADETTI.
- Compliance with the legislation, regulation and contractual obligations applicable to ADETTI.

2.3 Applicable legal requirements

ADETTI complies with the laws, regulations and contractual obligations which are applicable to the organization in general and in particular to its ISMS. From the applicable legislation the following legal requirements may be drawn:

a. Protect the privacy of personal information according to (1) European Commission's Data Privacy Directive (Directive 95/46/EC), (2) Portuguese Data Privacy Law (*Lei de Protecção de Dados Pessoais*, law number 67/98 from 26th October) and (3) Rulings from the Portuguese National Forum of Data Protection (*Comissão Nacional de Protecção de Dados*).

b. Protect software rights according to Portuguese legislation on software licensing (1) *Código dos Direitos de Autor e dos Direitos Conexos* - law number 144/91, (2) *Regime de Protecção Jurídica das Bases de Dados* - law number 252/94 and (3) *Protecção Jurídica das Bases de Dados* - law number 122/00).

c. Ensure the confidentiality and availability of the project documentation during three years after the project finish due to requirements from the funding intuitions (European Commission and *Fundação da Ciência e Tecnologia*).

d. Comply with other applicable Portuguese legislation.

e. Comply with all obligations derived from the contracts with ISCTE, research partners, between others.

2.4 Applicability

This policy applies to all members of staff, suppliers or partners, under a contact, who have any access to or involvement with the information assets covered by the scope of the Information Security Management System (financial information of the final report of the scientific research projects).

2.5 Responsibilities

ADETTI management is responsible to ensure that all activities required to implement, maintain and review this policy are performed.

All personnel, regarded as included in the ISMS scope, must comply with this policy statement and its related security responsibilities defined in the ISMS policies and procedures that support the present policy.

All personnel, even if not included in the ISMS scope, have a responsibility for reporting security incidents and any identified weaknesses and to contribute to the protection of the information and resources of ADETTI.

2.6 Enforcement

ADETTI holds the right to monitor the compliance of its personnel with this policy. Members of staff who fail to comply with this policy may be subjected to disciplinary actions.

2.7 Ownership and revision

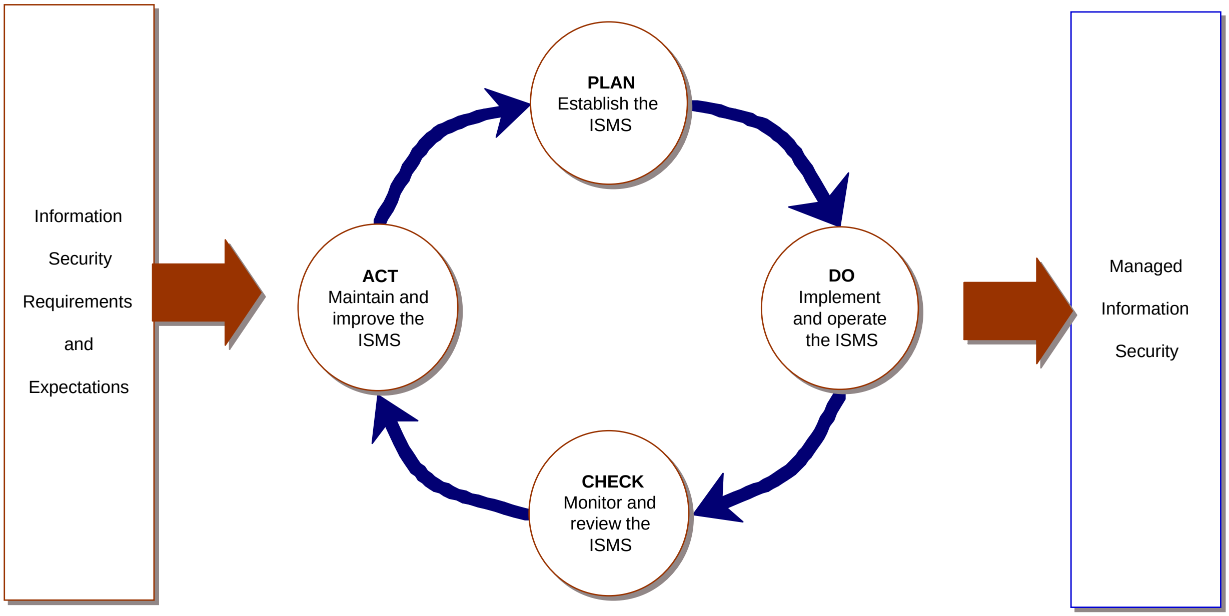
This policy statement is owned by the Executive Board of ADETTI who has delegated this task to Security Officer.

This policy is revised on an annual basis by the Security Officer and every time that the Executive Board of ADETTI of ADETTI or the Security Forum decides to do so.

3. ISMS Approach

3.1 Plan, Do, Check, Act model

ADETTI adopted as a framework to develop, implement, maintain and continually improve its ISMS, the Plan, Do, Check, Act (PDCA) model.


Information Security Requirements and Expectations
PLAN
Establish the ISMS
DO
Implement and operate the ISMS
CHECK
Monitor and review the ISMS
ACT
Maintain and improve the ISMS
Managed Information Security

Plan (establish the ISMS)

Definition	Establish security policy, objectives, targets, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organisation's overall policies and objectives.
Compliance of the ISMS	ADETTI to comply with this requisite has conduct the following actions: a) define the scope of its ISMS. b) define its ISMS policy, according to the specifications of BS 7799:2002. c) identify and apply a systematic risk assessment approach, which is described in SMP05 - Risk Management [Annex E].

Do (implement and operate the ISMS)

Definition	Implement and operate the security policy, controls, processes and procedures.
Compliance of the ISMS	The Risk Treatment Plan [in the Implementation Report, Annex C] reflects the decisions made in the Plan phase and identifies the actions, responsibilities and timelines to manage security management.

Check (monitor and review the ISMS)

Definition	Assess and, where applicable, measure process performance against security policy, objectives and practical experience and report the results to management for review.
Compliance of the ISMS	ADETTI undertakes reviews of the ISMS on a regular basis to ensure that the system remains adequate and effective in the protection of the scope, state in the SMP02 - Security Management Planning and Review [in Annex E].

Act (maintain and improve the ISMS)

Definition	Take corrective and preventive actions, based on the results of the management review, to achieve continual improvement of the ISMS.
Compliance of the ISMS	ADETTI performs appropriate corrective and preventive actions in accordance with the SMP10 - Corrective and Preventive Actions Procedure [in Annex E].

3.2 Documentation

3.2.1 Documentation structure

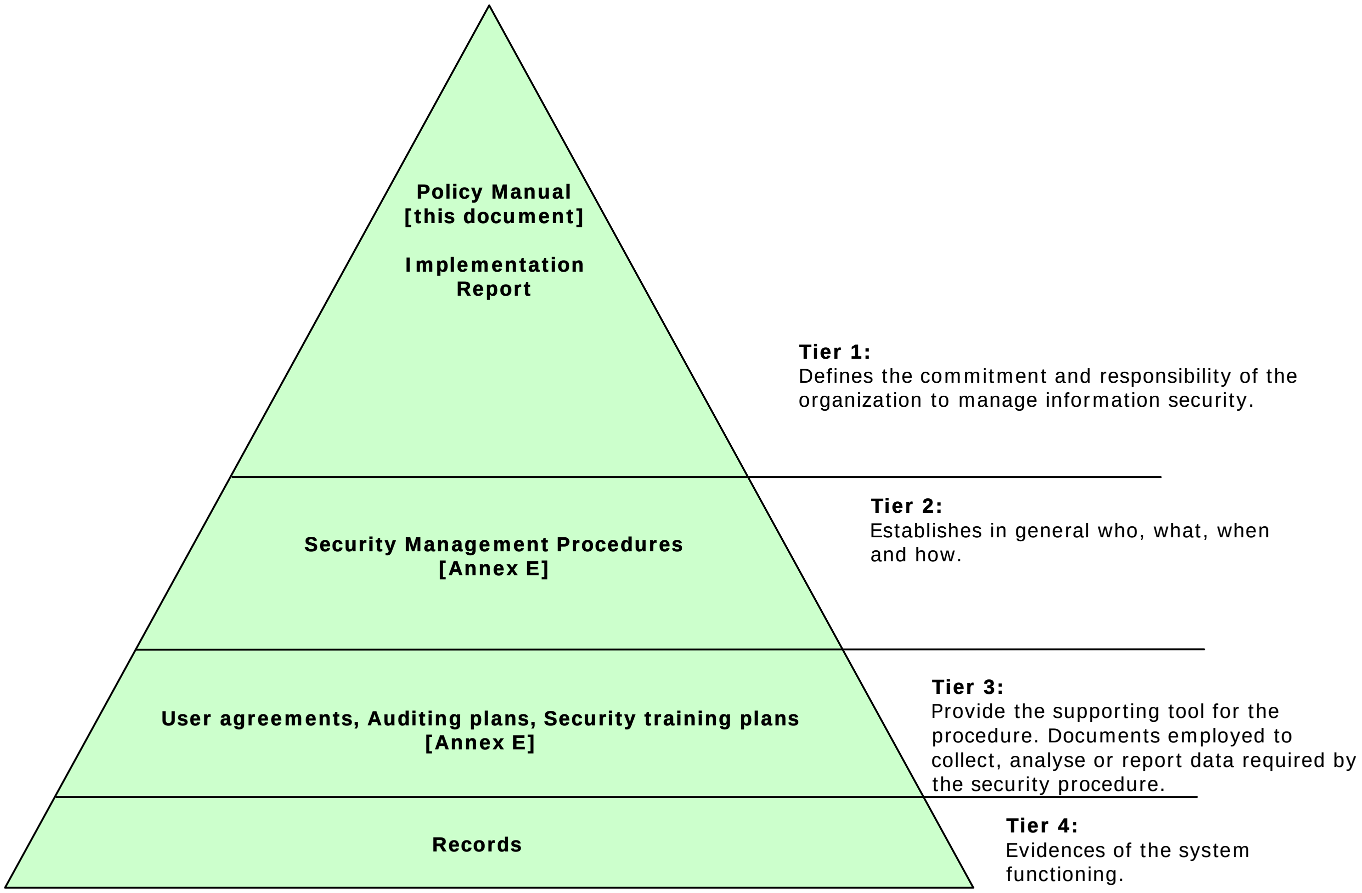
The documentation of ISMS includes the present Manual and the corresponding referenced procedures and other documents and records necessary to meet the requirements of BS 7799:2002. The documentation is organized in four tiers, illustrated in Figure I.

Tier 1 is formed by the documents that define the objectives of security management and the overall mechanisms that support it. All the documents compiled in this Manual are included at this hierarchical level.

In tier 2 we will find the ISMS supporting procedures, which describe how the policies are implemented.

The tier 3 documentation provides a written support for the execution of the tasks required by the security procedures.

Tier 4 is the records of the execution of the security management tasks. This includes previous audit plans or reports of incidents.


Policy Manual
[this document]
Implementation
Report
Security Management Procedures
[Annex E]
User agreements, Auditing plans, Security training plans
[Annex E]
Records

Tier 1:
Defines the commitment and responsibility of the organization to manage information security.

Tier 2:
Establishes in general who, what, when and how.

Tier 3:
Provide the supporting tool for the procedure. Documents employed to collect, analyse or report data required by the security procedure.

Tier 4:
Evidences of the system functioning.

Figure I: ISMS documentation layers

3.2.2 Documentation control

Documentation required for the ISMS is controlled per Security Management Procedure 04 [in Annex E]. This procedure establishes the required actions for documents to be:

a. approved by authorised personnel and reviewed for adequacy prior to use;
b. reviewed, updated as necessary and re-approved documents, ensuring that the changes and the current revision status of documents are identified;
c. ensured that relevant versions of applicable documents are available at points of use, and that those documents remain legible and readily identifiable with the purpose of preventing the unintended use of obsolete documents, and to apply suitable identification to them if they are retained for any purpose.

3.2.3 Control of records

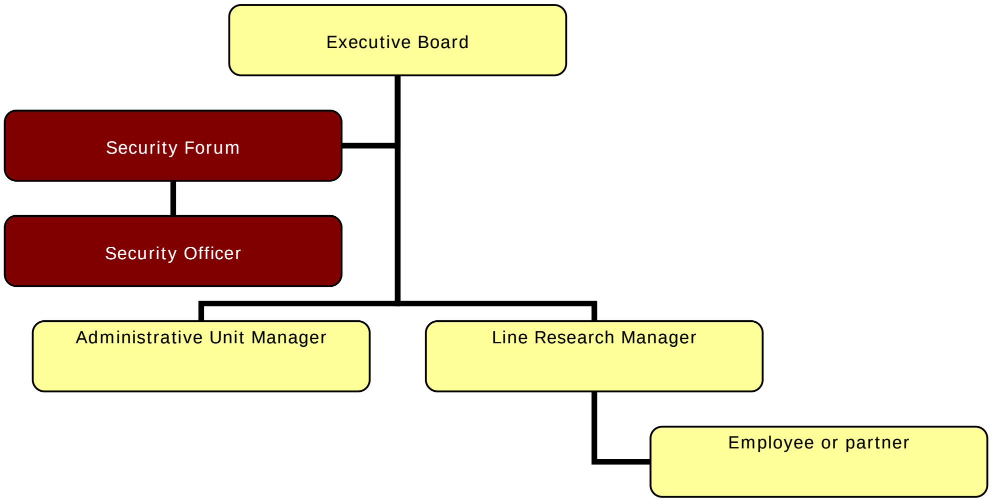
ADETTI maintains records necessary to demonstrate conformity to the requirements of BS 7799-2:2002. Records that provide evidence of the performance of the security process as well as all occurrences of security incidents shall be identified and maintained. The Security Management Procedure 04 [in Annex E] defines the controls needed for the identification, storage, protection, retrieval, retention time and disposition of records in order to ensure that records:

a. remain legible, readily identifiable and retrievable.
b. protected against unauthorised access, modification or unavailability.
c. maintained during a period of time complaint with any relevant legal and business requirements.
d. are disposal in order to prevent the inappropriate disclosure of information of ADETTI.

4. Security Responsibility

4.1 Security Management Organization

This policy establishes the organization of the information security management and the allocation of information security responsibilities within the ADETTI management and staff.



Executive Board

The Executive Board of ADETTI is the ultimately responsible to ensure the appropriate conditions for the establishment, implementation, operation, monitoring, review, maintenance and improvement of the ISMS.

The Executive Board champions the security management system in ADETTI and supports this effort through the following actions:

a. approval of ADETTI´s Information Security Policy Statement.
b. approval of ADETTI´s security objectives and plans.
c. assistance in determining and approval of the responsibilities for information security;
d. facilitation of the communication to the organization of the importance of information security management for ADETTI.
e. provision of the adequate resources and funding to operate and maintain the ISMS.
f. conduct management reviews of the ISMS.
g. review and approval of the risk tolerance level.
h. provision of input into and support improvements in the ISMS of ADETTI.

Security Forum

The forum is responsible for supervising the implementation of Information Security within ADETTI. This forum is responsible for:

a. planning the resource to support security management, according to SMP02 [in Annex E].
b. supervise security actions in ADETTI, according to SMP02 [in Annex E].

Security Officer

This person is responsible to conduct the required actions to support security management and controlling the security actions of other employees, according to SMP02 [in Annex E].

Administrative Unit Manager

Administrative Unit Manager should ensure that the Information Security policy and procedures are implemented and maintain suitable in relation to the activities and resources under the scope of evaluation.

Line research manager

Line research manager should ensure that the ADETTI Security policy is understood and, in the applicable cases, followed by the employees within their area of responsibility.

Employees

All members of staff, suppliers or partners, under a contact, who have any access to or involvement with the information assets covered by the scope of the Information Security Management System (financial information of the final report of the scientific research projects) must:

a. Comply with the ISMS security policies and procedures.
b. Protect the information defined by ADETTI as critical.
c. Protect the assets of ADETTI.
d. Report suspected or actual non-conformities, incidents or security weaknesses using SMP07 - Incident Report Management [in Annex E].

5. ISMS Improvement

5.1 Continual improvement

ADETTI plans and manages the processes necessary for the continual improvement of the security management system. The facilitation of the continual improvement of the security system involves the following instruments:

a. Verifying the compliance of the actual information security policy with the existing legal and business requirements of ADETTI.
b. Evaluate in what extend the defined security objectives ensure the push forward of ADETTI to the attainment of the purpose of its information security policy.
c. Assess the audit results and the effectiveness of the corrective actions taken to eliminate possible nonconformities.
d. Analyse the data provided by the monitoring mechanisms of security events.
e. Examine the data from corrective and preventive actions taken by ADETTI.
f. Assess the input and output data provided by management review.

5.2 Corrective action

ADETTI performs corrective actions, in accordance with the Security Management Procedure 10 [in Annex E], to determine the cause of nonconformities and to implement the appropriate actions which will prevent the recurrence of the nonconformity.

5.3 Preventive action

ADETTI performs preventive actions, in accordance with the Security Management Procedure 10 [in Annex E], to determine the required action to guard the organization against future nonconformities, preventing their occurrence.

ANNEX E

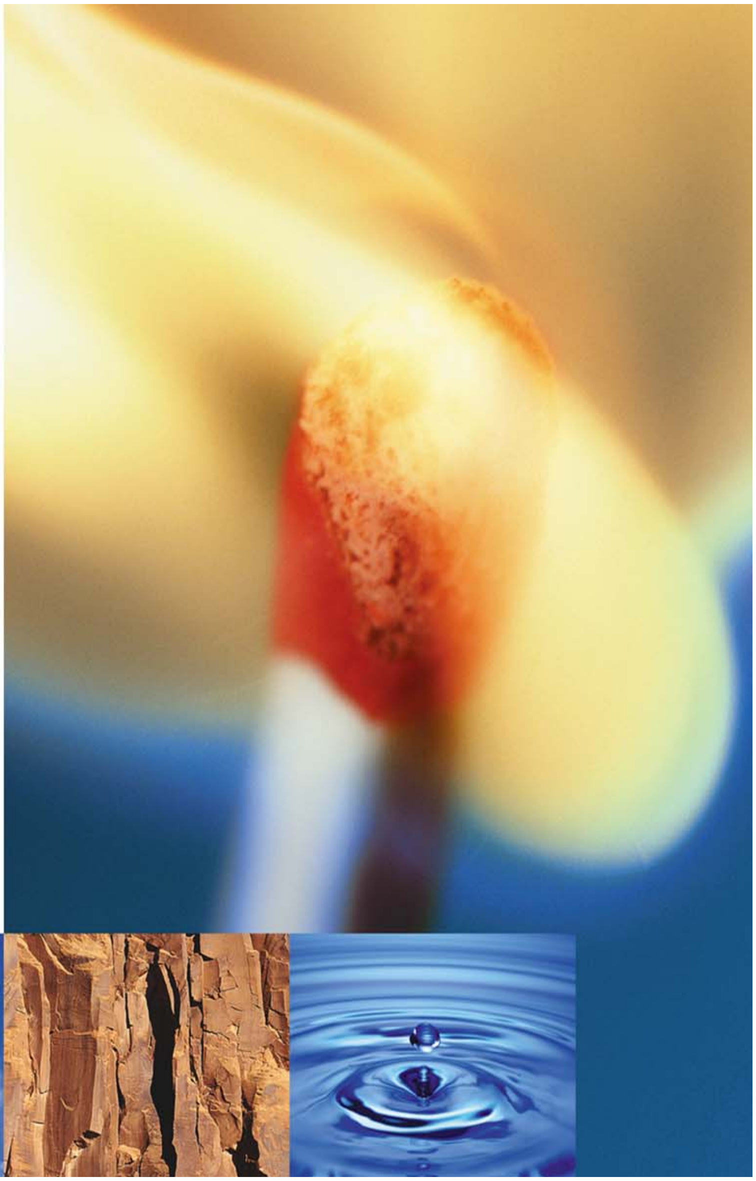
SECURITY HANDBOOK

The present document is required by BSI for organizations to attain the security certification.

This document is an output of the phase 6 of the implementation methodology proposed in Annex C. The structure and content of the present document is discussed in Annex C, section 6.2.3 - Work_Deliverable03: Supporting process of security norms.

Security Handbook

adetti



Label: 1.0
Version: 03.100804
Approved by: José Miguel Dias on 11/08/04

TABLE OF CONTENTS

ISMS Level II documentation: Procedures

ISMS Level III documentation: Forms

Part I
ISMS level II documentation: Procedures

Security Management Procedure - SMP01

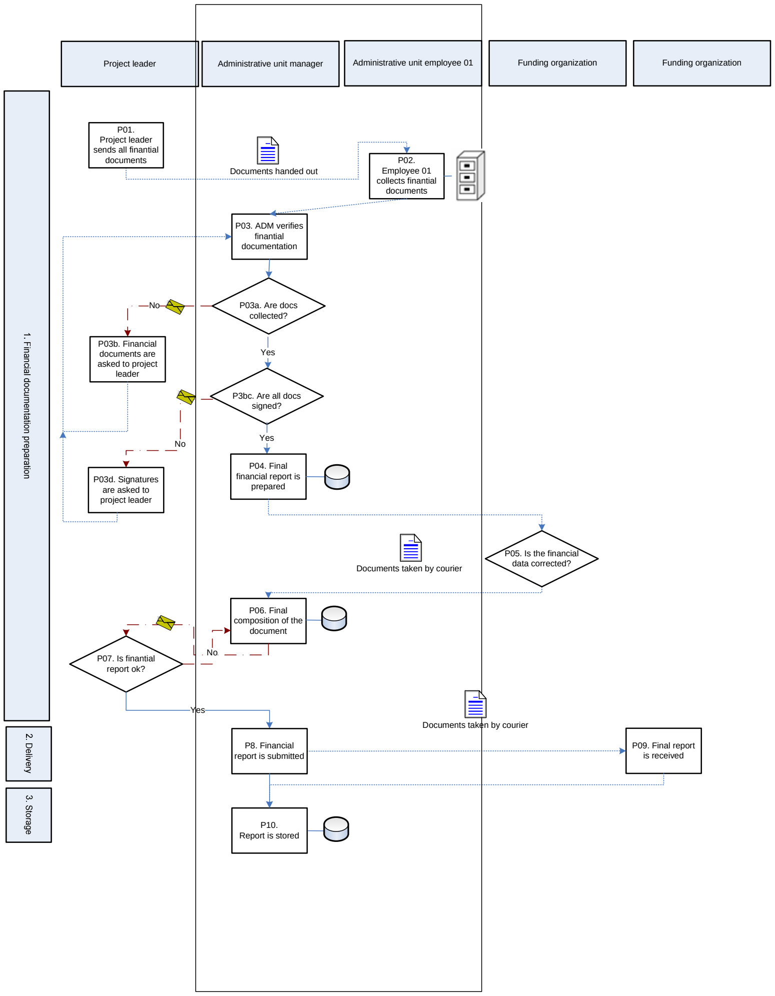
Financial Reporting

(organizational process selected as the scope for the security evaluation)

Page: 1 of 1	ISMS document: 2.1	Code: 0010101
		Label: <1.0>

1. Objective Preparation, delivery and storage of the financial data of final report of the research projects

2. Process


Project leader
Administrative unit manager
Administrative unit employee 01
Funding organization
Funding organization
1. Financial documentation preparation
2. Delivery
3. Storage
P01. Project leader sends all finantial documents
Documents handed out
P02. Employee 01 collects finantial documents
P03. ADM verifies finantial documentation
No
P03a. Are docs collected?
P03b. Financial documents are asked to project leader
Yes
P3bc. Are all docs signed?
No
Yes
P03d. Signatures are asked to project leader
P04. Final financial report is prepared
Documents taken by courier
P05. Is the financial data corrected?
P06. Final composition of the document
No
P07. Is finantial report ok?
Yes
Documents taken by courier
P8. Financial report is submitted
P09. Final report is received
P10. Report is stored

1 - The project leader sends all financial documents to the ADUE01.

2 - ADUE01 fills this documentation in the respective folder, which is stored in the project file cabinet.

3 - The Ad Unit manager (ADM) verifies if the financial documentation is colleted and properly signed by a project responsible. This verification is performed by checking if the collected documents are consistent with the financial budget of the project and with the requirements of the funding institution. If a document is missing or is not signed the ADM asks by e-mail to the project leader, who then sends the document in missing or goes to the AD office to sign the document.

4 - The Ad Unit manager (ADM) prepares the final financial report, which is placed at the BSCW server at the project's folder, with restrict access to the project leader, research line leader and members of the Administrative Unit. Once the report is finished, the report and the supporting documents are send to the accountant who audits the data in the report. This transportation is done by courier or by hand (an employee from the accountant office goes to ADU office). Copies of all documents which are sent to accountant are maintained at the project folder.

5 - The Accountant sends the audited report to Ad Unit manager (ADM) through courier.

6 - The ADU finishes the report and then sends an email to the project leader notifying him that the financial report is ready for approval.

7 – The project leader approves the financial report and then informs by email the ADU.

8 – The ADU submits the financial report to the funding organization, employing a courier, registered letter or in even some cases by fax.

9 – A notification of reception is signed by the funding organization.

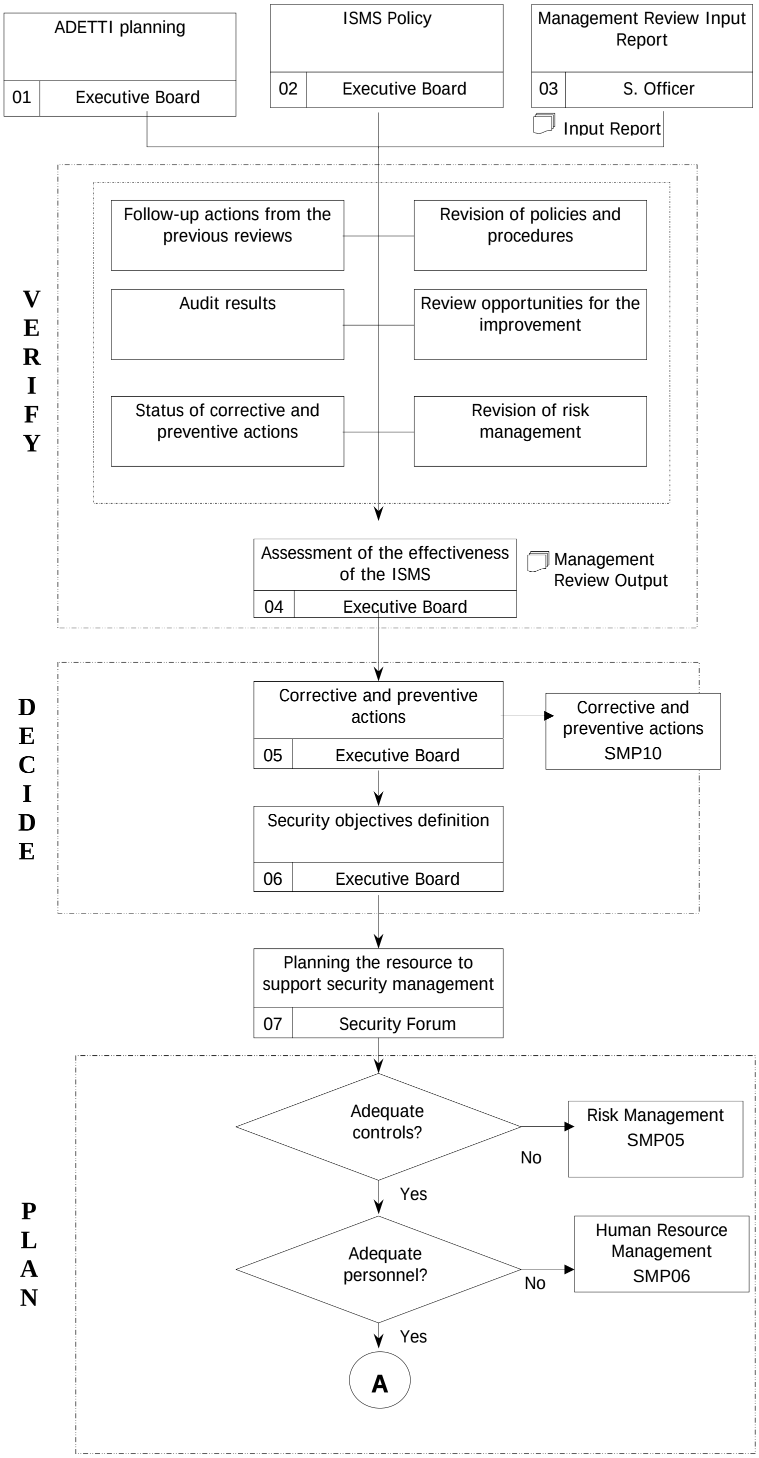
10 – The ADU stores the financial report in BSCW and the project file cabinet, closed by lock.

The present procedure is owned by the Administrative Unit Manager and must be review every year, according to the SMP04.

adetti	Security Management Procedure - SMP02	
Security Management Planning and Review		Label: <1.0>
Page: 1 of 2	ISMS document: 2.2	Code: 0010101

1. Objective Planning and review of the security management system

2. Process



ADETTI planning
01
Executive Board
ISMS Policy
02
Executive Board
Management Review Input Report
03
S. Officer
Input Report
V E R I F Y
Follow-up actions from the previous reviews
Revision of policies and procedures
Audit results
Review opportunities for the improvement
Status of corrective and preventive actions
Revision of risk management
Assessment of the effectiveness of the ISMS
04
Executive Board
Management Review Output
D E C I D E
Corrective and preventive actions
05
Executive Board
Corrective and preventive actions SMP10
Security objectives definition
06
Executive Board
Planning the resource to support security management
07
Security Forum
P L A N
Adequate controls?
No
Risk Management SMP05
Yes
Adequate personnel?
No
Human Resource Management SMP06
Yes
A

1, 2 – Based on the business objectives of ADETTI, the "Information Security Policy Statement" is defined/revised by the Executive Board.

3 – The "Management Review Input Report" is prepared by the S. Officer and revised by the Executive Board. This report is reported every 6 months. This document covers the following issues:

- Follow-up actions from the previous reviews
- Audit results
- Status of corrective and preventive actions
- Revision of policies, procedures and controls
- Revision of risk management
- Review opportunities for the improvement

This document follows the structured defined in the Template "Management Review Input Report".

This Security Officer is responsible to conduct the required actions to support security management and controlling the security actions of other employees.

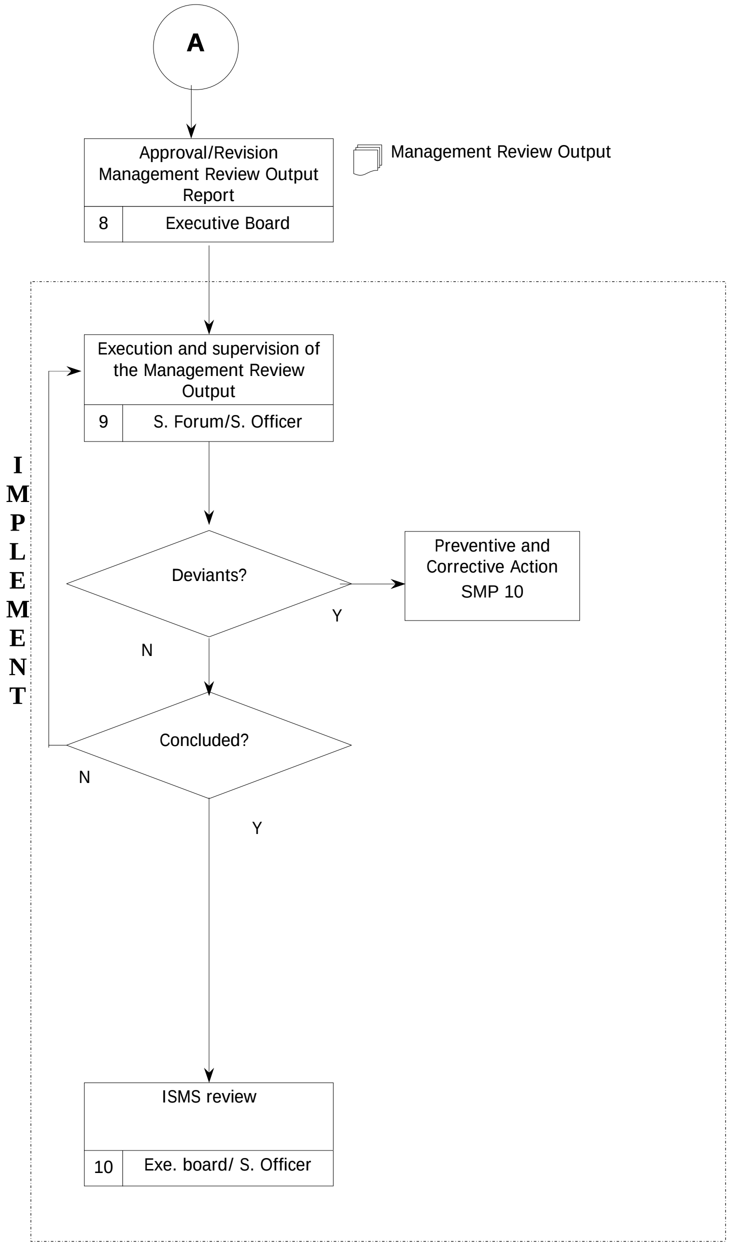
4 – The Executive Board reviews the ISMS, at least once per year, to ensure its continuing suitability, adequacy and effectiveness. The results of this assessment are recorded in the "Management Review Output".

5 – In case of necessity, corrective and preventive actions are defined, in accordance with SMP10.

6 – At least annually, the Executive Board defines security objectives, employing for that the "Management Review Output".

7 – The established objectives in the previous step must be attainable by the resources, which are or will be, in support of security management. The Security Forum, with the assistance of the S. Officer must assess if:

- the existing controls are adequate, if not, SMP05 Risk Management will be required.
- the personnel is adequate, if not SMP06.


A
Approval/Revision Management Review Output Report
8
Executive Board
Management Review Output
I M P L E M E N T
Execution and supervision of the Management Review Output
9
S. Forum/S. Officer
Deviants?
Y
Preventive and Corrective Action SMP 10
N
Concluded?
N
Y
ISMS review
10
Exe. board/ S. Officer

The Security Forum is formed by the President of ADETTI, managers of the units integrated in the evaluation scope (Administrative Unit Manager) and the security officer. This forum meets every month in order to supervise security management in ADETTI.

8 – The needs identified in the previous step are defined in the “Management Review Output”.

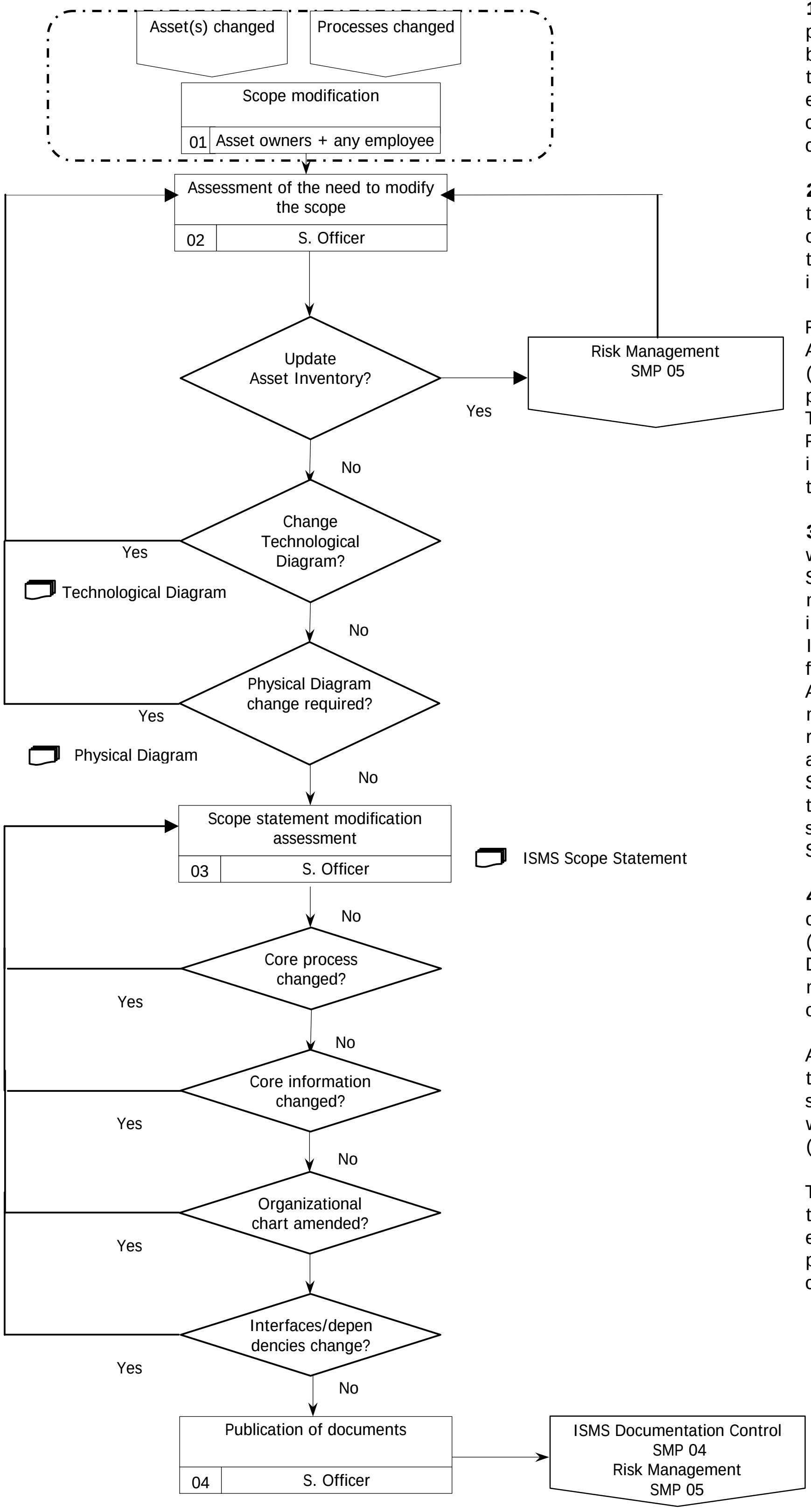
9 – The S. Officer must, monthly, verify the execution of the actions planned. The results of this verification are discussed in the monthly meetings of the S. Forum. Every time, a deviant is identified, a corrective or preventive plan must be issued.

10 – The results of the actions performed will be used as data for future ISMS reviews. An ISMS review must be conducted, at least, every year.

The present procedure is owned by the Executive Board and must be review every year, according to SMP04. This procedure must be, at least, conducted every 6 months.

1. Objective To define the boundaries of the organizational area subjected to security management.

2. Process



1 - Changes in the assets or/and processes included in the ISMS should be communicated to the S. Officer by the asset or/and process owner or even by any employee. This communication can be done by any channel (e.g. e-mail, oral speech).

2 – The S. Officer will assess the need to amend the ISMS documentation in order to accommodate the changes in the assets or on the process included in the ISMS.

Firstly, it should be decided if the Asset Inventory should be updated (the applicable modification procedures are described in SMP 05). Then the Technological Diagram and Physical Diagram should be considered in terms of amendment required by the asset.

3 – A significant change in the scope will require a modification in the ISMS Statement. Qualifying changes are (1) modification in the process and type of information which is the aim of the ISMS protection. (2) Changes in the functional organization of the Administrative Unit may result in modifications in the activities or its responsibilities and therefore must be adequately reproduced in the Scope Statement. (3) Relevant changes of the interfaces and dependencies of the scope should be reflected in the Scope Statement.

4 - If the S. Officer considers that any of these documents need to change (ISMS Scope Statement. Technological Diagram and Physical Diagram), he must apply the publication procedure of security norms (SMP04).

Additionally, if the scope was deemed to be changed, the risks affecting the scope may also have changed, which will require a new risk assessment (SMP05).

The present procedure is owned by the S. Officer and must be review every year, according to SMP04. This procedure must be, at least, conducted every 6 months.

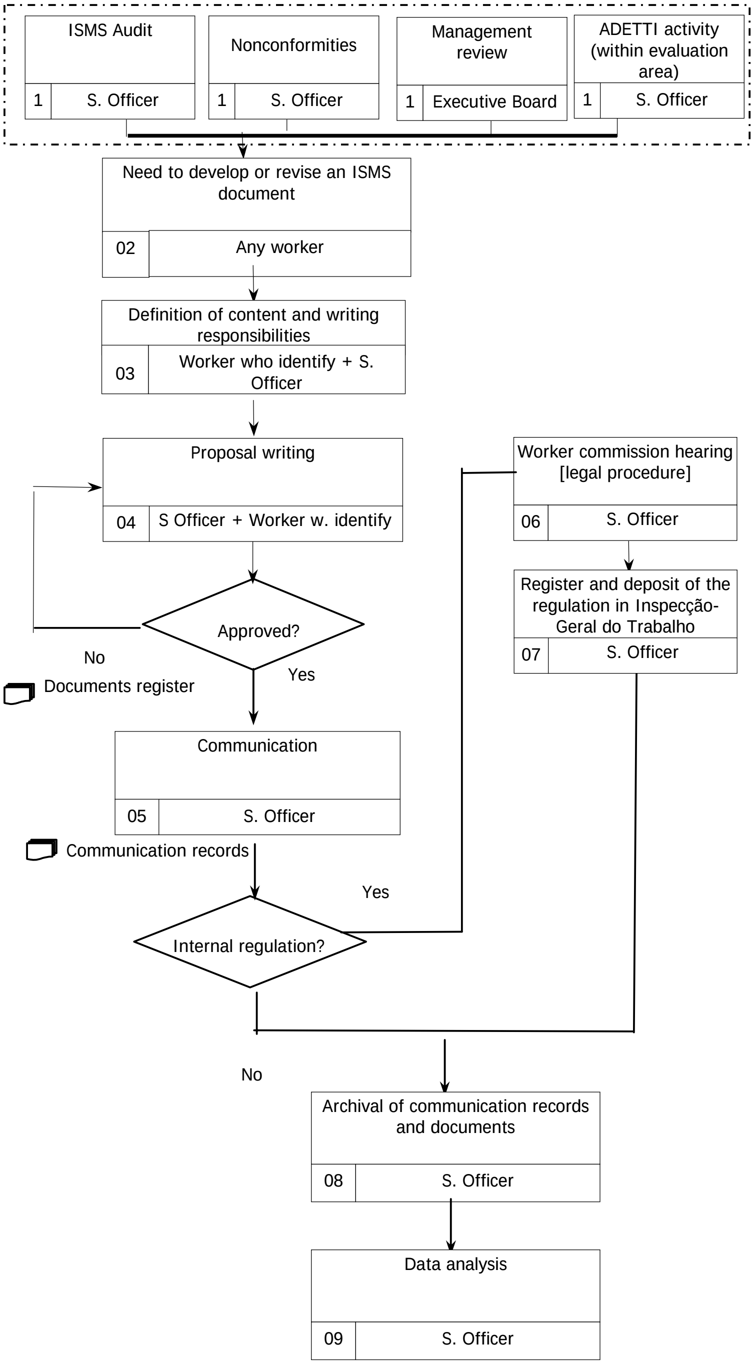
Security Management Procedure - SMP04

ISMS Documentation Control

		Label: <1.0>
Page: 1 of 3	ISMS document: 2.4	Code: 0010101

1. Objective Management of the security norms and its supporting documentation

2. Process


ISMS Audit
1
S. Officer
Nonconformities
1
S. Officer
Management review
1
Executive Board
ADETTI activity (within evaluation area)
1
S. Officer
Need to develop or revise an ISMS document
02
Any worker
Definition of content and writing responsibilities
03
Worker who identify + S. Officer
Proposal writing
04
S Officer + Worker w. identify
Approved?
No
Yes
Documents register
Communication
05
S. Officer
Communication records
Internal regulation?
Yes
No
Worker commission hearing [legal procedure]
06
S. Officer
Register and deposit of the regulation in Inspecção-Geral do Trabalho
07
S. Officer
Archival of communication records and documents
08
S. Officer
Data analysis
09
S. Officer

1 - Develop or revise an supporting document of the ISMS (i.e. an Policy, or Procedure) or any other document included in the scope may be found necessary, in result of an audit, in the nonconformities treatment, management review or simply result from the normal and daily activity of ADETTI (within evaluation area).

2, 3 – In case of an ISMS supporting document the need to develop or amend the document is reported to the S. Officer by mail who, together with the worker who identify the need, defines the what is to develop/revise (content) and who is going to writing the document (responsibilities).

4 – The S. Officer or who was assigned with this responsibility in the previous phase develops a draft, which is revised and approved by the S. Officer and, if this was the case, with the worker who identify the need. All approved documents must be identified in the ISMS document register.

5 – Every time a norm is approved, it must be properly communicated to his audience. The communication process is organized by the S. Officer and can involve, training sessions, written communication and other means. For probation reasons, records of the communication to employees must be kept.

The S. Officer assess if the security norm must have the legal statute of an internal regulation.

6 – If the security norm must be enacted as an internal regulation, then the commission of workers must be heard (this commission does not exist in ADETTI at the moment).

7 – The security norm is then submitted to the Inspecção-Geral do Trabalho (for some norms, a previous submission to the CNPD is required).

8 – Records of communication to employee of security norms must be kept for prosecution reasons.

9 – The S. Officer is assigned with the task of analysing the records and documents in order to evaluate the results of the communication process.
The present procedure is owned by the S. Officer and must be review every year. The procedure must be carry out every year (at least).

3. Description

3.1 Document content

This section defines the content, distribution and archival of the ISMS documents of ADETTI. It applies to the Security Policies (SP), Security Management Procedures (SMP) and Security templates (T).

3.1.1 Security Management Procedure

The procedure is written in a template with the following items:

In the header:

- ADETTI logo
- Identification of the type of the ISMS documentation
- Title
- "Label" which identifies the security classification of the document according to the Data Classification Procedure – SMP08;
- "Pages" indicates the number of the current page and the number of total pages;
- "ISMS document" the number showed refers to the list of deliverables defined in ISMS document 3.2 – ISMS Document Register;
- "Code" this number results from the documental classification scheme adopted by this procedure, see 3.2. Documentation numbering schema.

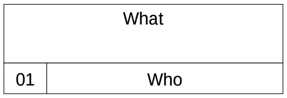
In the footer:

- Version
- Approval
- Date

The document is structured in the following sections:

1. Objective
2. Process (flowchart and text description)

Flowcharts employs the following symbols:

Symbols	Description
	Activity, action or operation
◇	Step where a decision is required
○	Continuation

3. Description (continuation)

3.2. Documentation numbering schema

All documents (and templates for records) covered by this Procedure shall have a unique reference number for identification of the document version (identified as “Code”).

The version code comprises of 7 digits, as shown below:

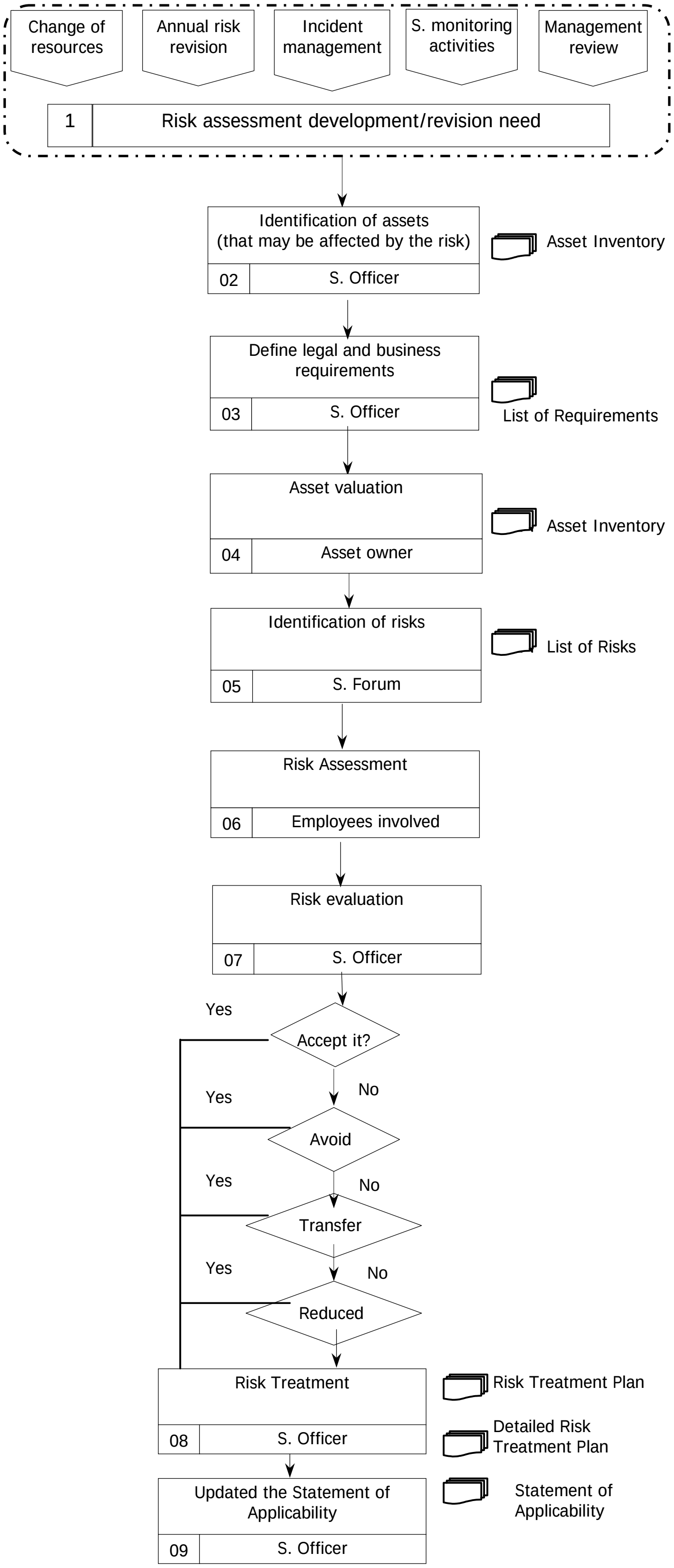
0010101

The first 3 digits show the ‘major revision’, the subsequent two digits are ‘minor revision’ and the last ‘simple update’.

adetti	Security Management Procedure – SMP05	
Risk Management		Label: <1.0>
Page: 1 of 3	ISMS document: 2.5	Code: 0010103

1. Objective Risk assessment and treatment methodology applied in ADETTI

2. Process



1 - Risk assessment is an ongoing activity in ADETTI. Any asset included in the ISMS scope must be inventoried and its risks identified and assessed. The assessment process can be initiated by a number of activities as:

- Any change in the assets included in the scope, especially prior to the introduction of any new information system, it should be communicated to the S. Officer.

- The S. officer will conduct an annual revision of the risk assessment process in order to review and identify new risks that may have appeared in the meanwhile, which implies the update of the risk assessment report and risk treatment plan.

- The analysis of results of incident management (SMP07).

- The analysis of s. monitoring activities as internal audit (SMP09).

- The management may decide to alter the degree of assurance (forcing the modification of the required level of protection of an asset). Management review is performed in accordance with SMP02.

2 - Resources included in the scope (defined according to SMP01) should be identified using the following categories:

- information assets (includes paper documents and electronic information databases)
- software assets (e.g. application, system, development tools, utilities)
- physical assets (such as rooms, file)
- services (e.g. telecommunications, heating)

Assets are registered using the “Asset Inventory”.

3 –The legal and business requirements should be defined using the “List of requirements”.

4 - The asset owner (employee nominated by the S. Forum as responsible for the asset) defines the value of each asset. The asset evaluation formula is based on 4 factors: confidentiality, integrity, availability and business value. For the first three items, the asset is valuated in terms of the possible business impact that the loss of confidentiality, integrity and availability could caused on ADETTI. The last factor measures the asset in terms of business relevance, depicting the business and legal requirements for that asset. Each of the four items is graded in a scale of 1 to 5 (being 5 the highest score).

The resulting values of the four classifications are divided by 4 to ensure that the final asset value reproduces the average value from all the different four aspects. The perceived value is rated using a numerical scale of 1 to 5 (being 5 the highest score).

5 – Risks are identified based on their internal factors: threats and vulnerabilities. According to BSI recommendations, threats and vulnerabilities are identified sequentially. The S. Officer can employ any method to identify threats and vulnerabilities. The identified risks are revised by the S. Officer. Risks are identified in the List of Risks.

6 – All risks are assessed with the following risk formula: the asset value (1 to 5) is multiplied by the probability (1 to 5) and by the impact (1 to 5). The probability is estimated based on a series of descriptions:

Probability

How likely is it that an incident could occur, taking account of the controls in place and their adequacy?

5	Almost certain	Likely to occur with some frequency
4	Likely	Will probably occur
3	Possible	Do not expect it to happen but it is possible
2	Unlikely	May occur occasionally
1	Rare	Can't believe that this will ever happen

Impact

The several levels of Impact were also described:

Level	**Description**	**Impact on the business**	**Impact on the legal requirements**	**Impact on the information security properties**		
				Confidentiality	**Integrity**	**Availability**
5	Very high	Risk most probably will cause an serious interruption or degradation of the business process (e.g. a funding organization cancelling a project)	Serious punitive measurement and litigation expected or certain	Any unauthorised access will cause an serious impact	Any data corruption will cause an serious impact	Serious impact of unavailability (e.g. any permanent loss of service)
4	High	Risk can cause an minor interruption or degradation of the business process	Minor punitive measurement and litigation expected or certain	Any unauthorised access will cause an minor impact	Any data corruption will cause an minor impact	Any unavailability will cause an minor impact
3	Medium high	The risk can indirectly cause a degradation of the business process.	Litigation possible but not certain. Potential for punitive measurement.	Any unauthorised access will cause negative consequences	Any data corruption will cause negative consequences	Noticeable impact of unavailability. It should be available within a 24 business hours.
2	Medium low	Minimal risk for ADETTI	Litigation unlikely. No punitive measurement.	Failure to meet legal obligations that may result in a departmental embarrassment	Data corruption with minimal impact	Unavailability would cause some minor impact. It should be available within a 48 business hours.
1	Low	No risk for ADETTI	Unlikely to cause litigation or any punitive measurement (as fines)	Failure to meet legal obligations that may result in a individual member of staff embarrassment	Minor data corruption with no risks	Not critical, it can be available within 72 business hours.

7 – All risks must be evaluated in terms of the following options: first risks are assessed if they are acceptable. If the risk is too dangerous to be tolerable, it is examined consequently in terms of avoidance, transference or mitigation. The risk to be acceptable must be below the defined risk acceptance level (a defined value in the scale of possible risk values, which differentiate the risks which are acceptable from the ones, which are not).

8 – After the decision is made, by the S. Officer and approved by the S. Forum, on what to do with each risk, the Risk Treatment Plan is developed. This document register for each risk, the following data, as show in the respective Template:

- Asset
- Threat
- Vulnerability
- Risk level
- Treatment option
- Applicable Controls
- Risk reduced
- Residual risk
- Cost
- Time
- Selected

All risk classified with a score higher than 100 must be addressed by a Detailed Risk Treatment Plan, which details:

- Risk priority
- Risk owner
- Risk description
- Risk Assessment
- Risk Indicators
- Control implemented

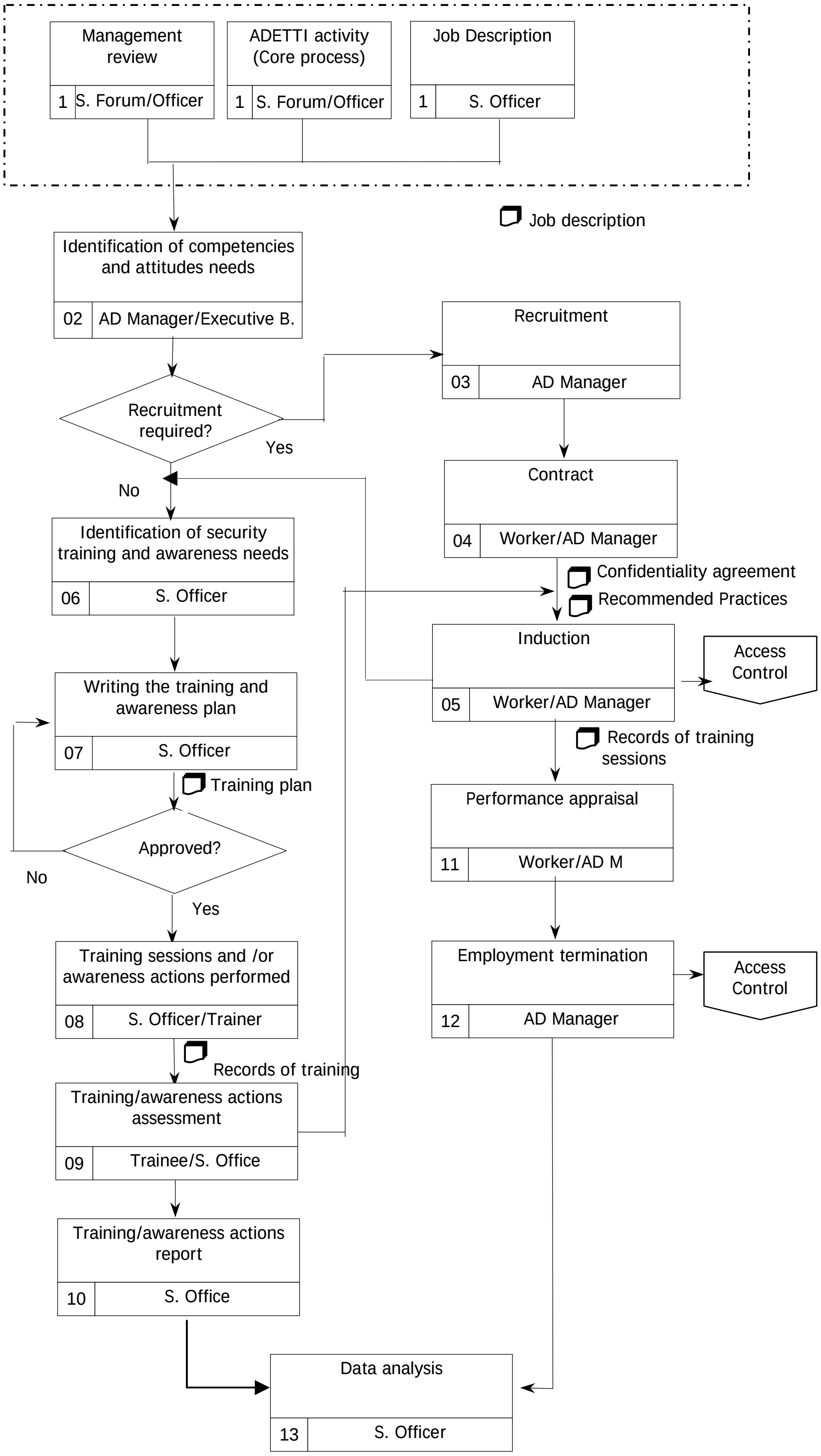
9 – The controls selected from ISO 17799 must be added to the Statement of Applicability.

The present procedure is owned by the S. Officer and must be review every year, according to SMP04. This procedure must be performed every 6 months (at least).

adetti	Security Management Procedure – SMP06	
Human Resource Management		Label: <1.0>
Page: 1 of 1	ISMS document: 2.6	Code: 0010101

1. Objective To ensure that ADETTI personnel have adequate training and awareness to perform security functions.

2. Process



1 - Derived from several activities the HR function collects data which is used in the HR management. The S. Officer establishes through Job Descriptions the group of requirements to perform the job positions pertained to security management.

2 - The AD manager and Executive Board decide which competencies are required for the Administrative area and security management.

3 - The recruitment of any employee for the Administrative area (AD) is conducted by the AD manager, who verifies the credentials of the selected candidate(s).

4 – The selected candidate(s) must sign a Confidentiality Agreement and must receive a copy of the Recommended Security Practices.

5 – During the induction process, the new worker must be subjected to security training sessions. For authorization of access rights, it must be employed SMP11 – Access Control.

6, 7 and 8 – The S. Officer must prepare, at least annually, a training plan in order to ensure that personnel are trained and aware of their security responsibilities.

9 - The attendance of training sessions as well as awareness actions is recorded. This record is maintained by the Security Officer.

10 - The training and awareness actions are reported by the Security Officer.

11 – In the performance appraisal of workers, the AD Manager must assess also the performance of security duties.

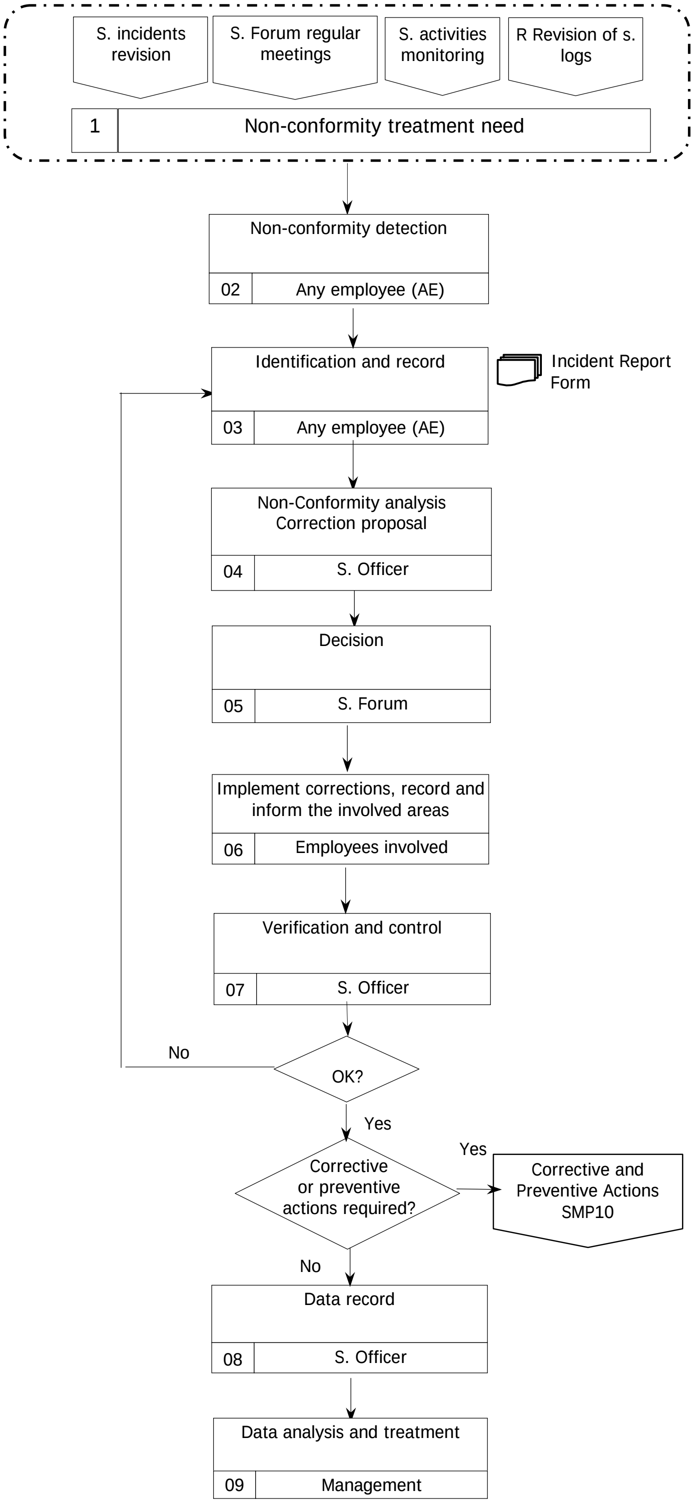
12 – In the moment of employment, it must be verified if the controls have been removed, according to SMP11 – Access Control.

13 - In this activity, the data collected (records) is analyzed, in order to provide input for the management planning and review process (SMP02) and, in case of applicability, initiate corrective or preventive actions, as described in SMP10. This procedure is owned by the S. Officer and must be review every year and carry out every 6 months (at least).

adetti	Security Management Procedure – SMP07	
Incident Report Management		Label: <1.0>
Page: 1 of 1	ISMS document: 2.7	Code: 0010101

1. Objective To ensure that incidents are promptly detected, reported and dealt in an appropriately manner.

2. Process


S. incidents revision
S. Forum regular meetings
S. activities monitoring
R Revision of s. logs
1
Non-conformity treatment need
Non-conformity detection
02
Any employee (AE)
Identification and record
03
Any employee (AE)
Incident Report Form
Non-Conformity analysis Correction proposal
04
S. Officer
Decision
05
S. Forum
Implement corrections, record and inform the involved areas
06
Employees involved
Verification and control
07
S. Officer
No
OK?
Yes
Yes
Corrective or preventive actions required?
Corrective and Preventive Actions SMP10
No
Data record
08
S. Officer
Data analysis and treatment
09
Management

1, **2** – For the purpose of this procedure, the concept of incident is similar to the notion of non-conformity. ADETTI employs several methods to identify incidents:

• Incidents are reviewed on a regular basis to determine if preventative action will prevent certain types of incidents re-occurring.
• Logs of access logons, URL access lists, malicious code infections and other security records are monitored to assist in detection of unusual trends and any unauthorized attempts to access ADETTI information processing facilities. This task is performed by the S. Officer.
• Regular reviews by the Security Forum.

Every employee of ADETTI can submit a security incident/non-conformity to be investigated.

3 – In every situation, the employee must report the situation to the S. Officer. The collection of evidences must be done according to the legal requirements.

4 – The cause of the identified non-conformities is determined by an investigation lead by the S. Officer, who involves all other members of staff regarded as necessary. Once the cause is identified, the appropriate proposal of actions to correct the non-conformity is composed.

5, **6** – The decision in relation to the non-conformities can be:

a) correct the incident/non-conformity;
b) accept the incident/non-conformity [this decision means that the S. forum acknowledges the situation and the risks involving it, but nothing can be done] .

7 – After the implementation of the agreed actions, the results will be monitored in order to ensure that the situation of non-conformity was eradicated. The elimination of the non-conformity must be recorded in the in Incident Report Form.

If the non-conformity situation persists, there is a need to perform corrective or preventive actions, in order to eradicate the cause and to prevent re-occurrence of the problem. In this case, SMP10 should be applied.

8, 9 – The S. Officer ensures the treatment of all data related to the detected non-conformities and claims in order to guarantee that all of them are used for the periodic monitoring of processes, performed in the S. Forum and Management meetings.

The present procedure is owned by the S. Officer and must be review every year, according to SMP04. This procedure must be performed every 6 months (at least).

Security Management Procedure – SMP08

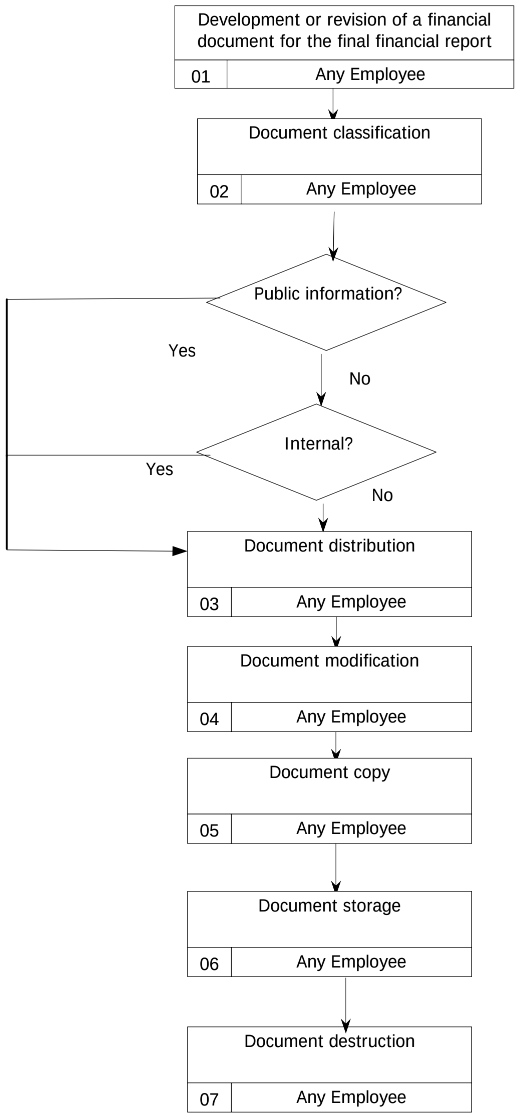
Document Classification

Label: <1.0>

Page: 1 of 2 | ISMS document: 2.8 | Code: 0010101

1. Objective To ensure that incidents are promptly detected, reported and dealt in an appropriately manner.

2. Process



1 – Financial documents produced by the Administrative Unit to support the final financial report of the research projects must be classified according to its confidentiality degree by ADETTI´s employees. External documents received by the administrative unit, which are considered relevant by them, are also classified.

2 - The documents should be classified as by their creators:

- Confidential is any information or material to which the unauthorised disclosure could be expected to cause exceptionally grave damage to the security of ADETTI or the privacy of its employees. An example is the disclosure of a research deliverable, which had a confidentiality requirement posed by its funding organization, which can result in loss of funding and other damages for ADETTI. Access to confidential information is strictly provided on a need-to-know basis.

- Internal is any information or material of which the loss, misuse, modification or unauthorised access might adversely affect ADETTI or the privacy of its employees. This type of information can be viewed only by ADETTI staff.

- External is any information or material that can be distributed to the public and poses no threat for ADETTI interests.

3, 4, 5, 6 and 7 – The document distribution, modification, copy, storage and destruction complies with the rules established in the following table:

3. Description

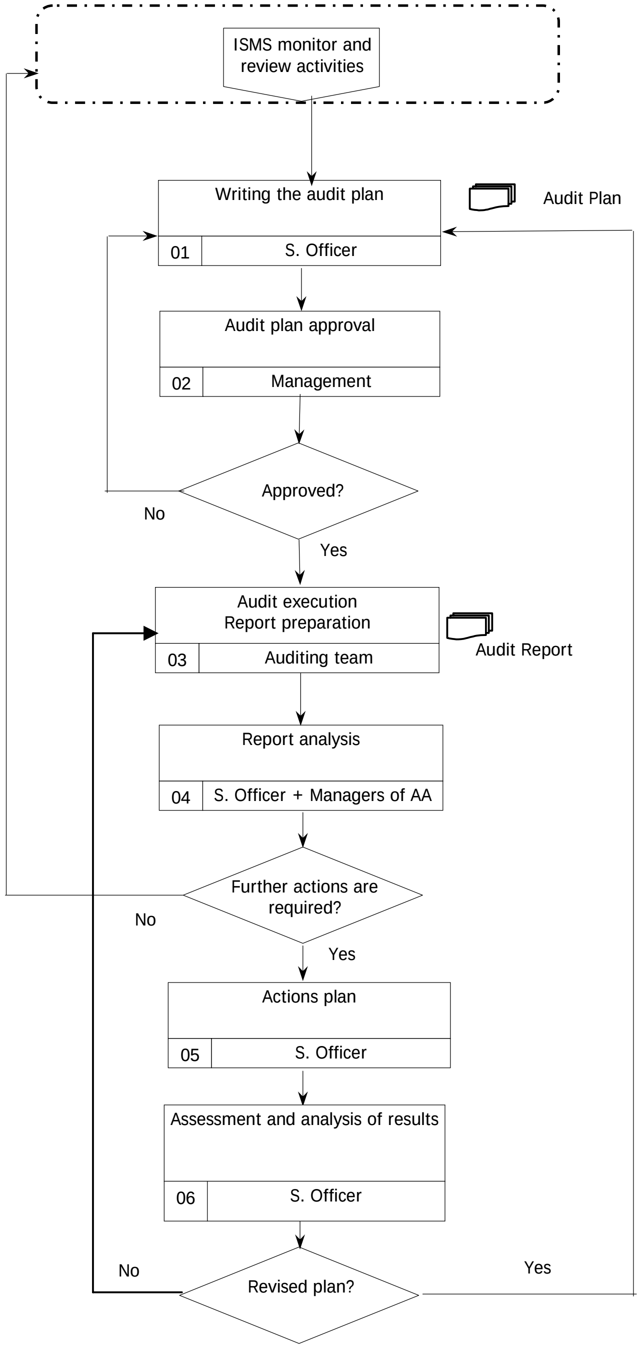
Confidentiality degree Handling tasks	External	Internal	Confidential
Label	(no label)	**A++**	**A-**
Document distribution	No procedure	The information recipients have to sign the document cover sheet.	The information recipients have to sign a non-disclosure statement.
Document modification	No procedure	All modifications are recorded in the document cover sheet.	All modifications are recorded in the document cover sheet.
Document copy	No procedure	All copies are recorded in the cover sheet of the document.	Every copy requires the authorisation in a written form by the Security Officer.
Document storage	No procedure	Information is kept in closed cupboard or in folder restricted to ADETTI personnel.	Information is kept in a closed safe or in a specific folder restricted to authorised individuals. Information is stored electronically encrypted.
Document destruction	No procedure	Paper documents are destroyed by shredder. Files are erased by selection of delete option in operating system.	Paper documents are destroyed by shredder. Files are erased by selection of delete option in operating system, temporary storage areas of these files (as Temp folder) are also empty.

The present procedure is owned by the S. Officer and must be review every year, according to SMP04. This procedure must be performed every 6 months (at least).

adetti	Security Management Procedure – SMP09	
ISMS Audit		Label: <1.0>
Page: 1 of 2	ISMS document: 2.9	Code: 0010101

1. Objective To ensure that ISMS audits are performed regularly in ADETTI.

2. Process



1,2 - The Security Officer conducts internal audits at planned intervals to determine whether the control objectives, controls, processes and procedures of the ISMS:

a) conform to the requirements of the British Standard 7799-2:2002 and relevant legislation or regulations;
b) conform to the identified information security requirements;
c) are effectively implemented and maintained;
d) perform as expected.

The audits are defined in an annual audit plan, prepared by the Security Officer and approved by ADETTI´s management. These audits are planned according to the organization objectives. An audit plan must be defined by the end of the month of October with the planned audits for the following twelve months period. At least an external audit must be performed in every twenty four months periods.

Each audit is performed by individuals who can not being the object of that particular audit.

These audits are based on random samples, however, should be planned to cover all aspects of the ISMS.

3 - The Auditing Team carries out the audit and issues the Report of the Audit with the evidence collected.

4 – The auditing report is analysed in a meeting of the Security Office with the managers of the audited areas (AA). In this meeting an assessment of the evidence collected is performed and, if applicable, corrective actions are identified.

5 – If the audit identifies an improvement action need an action plan is prepared indicating the actions to carry out, the responsibility for its concretization and the planned schedules. This plan is approved by the Security Officer. This plan is implemented in agreement with the defined in SMP 10.

6 – The Security Officer ensures the treatment of all data related to not conformities and observations detected in audits, in a way that this data may be used as input for the regular review of information security management processes, done in management meetings [addressed in SMP02]. When necessary corrective or preventive actions are done, in accordance with the planned in SMP1009. If necessary, the internal audit plan may be revised.

In addition to the annual audit, the subsequent issues required more regular checks:

- Internet Access – logging and monitoring of the accessed URL´s on an ongoing basis.
- E-mail – executable file attachments and viruses are checked an ongoing basis.

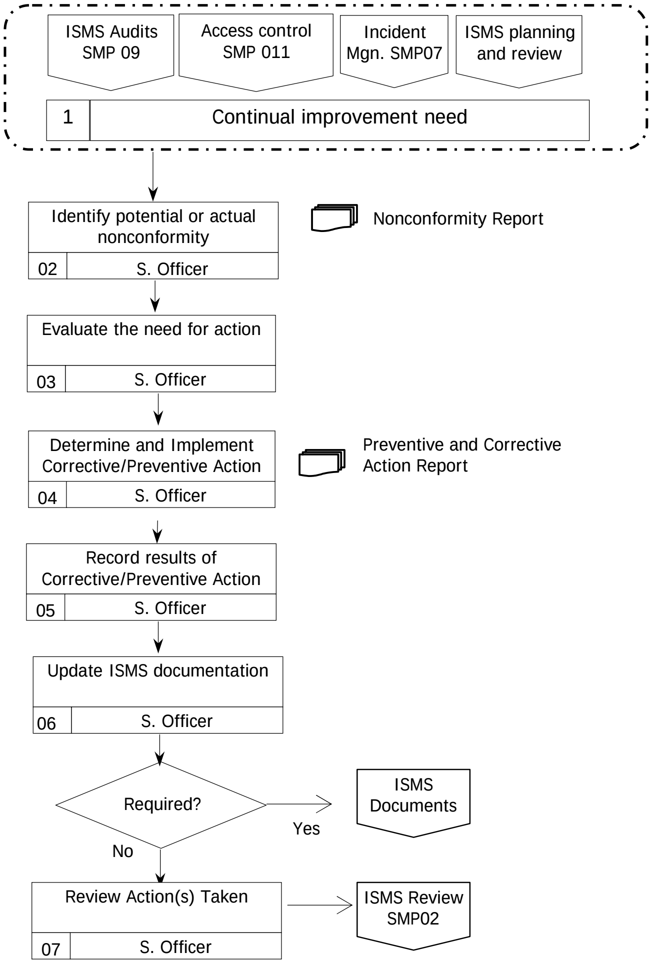
In addition to the above regular verifications, ad-hoc checks should be performed regularly to audit issues which had previously non conformities.

The present procedure is owned by the S. Officer and must be review every year, according to SMP04. This procedure must be performed every 6 months (at least).

adetti	Security Management Procedure – SMP10	
Corrective and Preventive Actions		Label: <1.0>
Page: 1 of 1	ISMS document: 2.10	Code: 0010101

1. Objective Investigation and correction of potential or actual nonconformities within the ISMS.

2. Process


ISMS Audits SMP 09
Access control SMP 011
Incident Mgn. SMP07
ISMS planning and review
1
Continual improvement need
Identify potential or actual nonconformity
02
S. Officer
Nonconformity Report
Evaluate the need for action
03
S. Officer
Determine and Implement Corrective/Preventive Action
04
S. Officer
Preventive and Corrective Action Report
Record results of Corrective/Preventive Action
05
S. Officer
Update ISMS documentation
06
S. Officer
Required?
Yes
No
ISMS Documents
Review Action(s) Taken
07
S. Officer
ISMS Review SMP02

1 – ADETTI employs various methods to identify situations which may require a corrective/preventive action:

- Regular ISMS audits (SMP09)
- Access rights are reviewed on a regular basis to ensure persons that have access to ADETTI information processing facilities are valid and appropriate (SMP11).
- Incidents are reviewed on a regular basis (SMP07).
- Security Management Planning and Review (SMP02).

2 - Once any potential or actual non-conformity is identified by the S. Officer, he must fulfil the Nonconformity Report.

3 - In the Nonconformity Report, the S. Officer must register the decision in relation to what to do with the nonconformity. The S. Officer must decide if a Corrective/Preventive Action is needed.

4 - Once corrective or preventive action is identified as being required, the appropriate action will be defined by the S. Officer. The person responsible for ensuring implementation of the agreed action will be identified and timescales for implementation will be agreed. The agreed action will then be implemented within the agreed timescales.

5 - For a period of 3 months after implementation of the corrective/preventive action, the results will be monitored and recorded in the Preventive and Corrective Action Report.

6 - If required, the appropriate ISMS document(s) will be amended accordingly and the change history of the document(s) will reflect the changes. For the document amendment SMP04 will be employed.

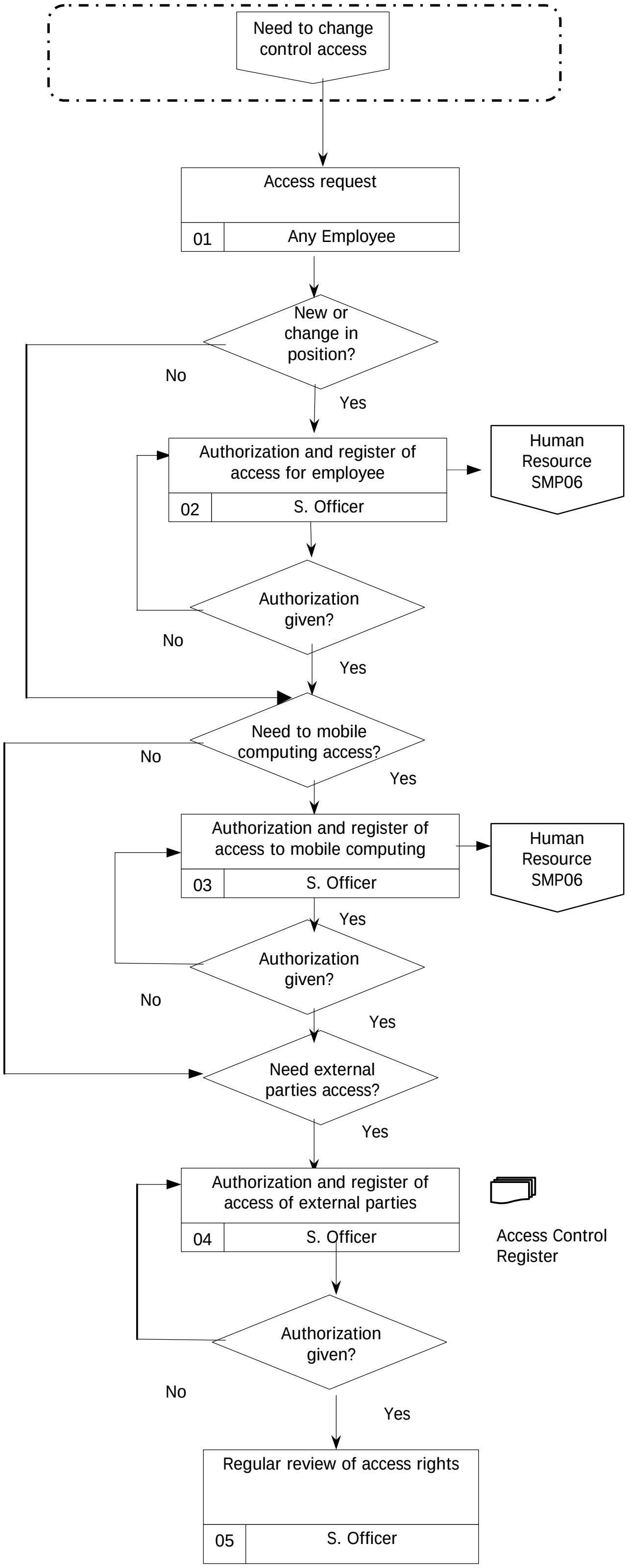
7 - Any corrective/preventive actions taken by ADETTI will be reviewed at the next ISMS review (SMP02) to confirm effectiveness. Any further actions identified as part of the review will be contained within the review report along with a suggested/recommended course of action.

The present procedure is owned by the S. Officer and must be review every year, according to SMP04.

adetti	Security Management Procedure – SMP11	
Access Control		Label: <1.0>
Page: 1 of 1	ISMS document: 2.11	Code: 0010101

1. Objective To control the process of providing access control to users.

2. Process



Need to change control access
Access request
01
Any Employee
New or change in position?
No
Yes
Authorization and register of access for employee
02
S. Officer
Human Resource SMP06
Authorization given?
No
Yes
Need to mobile computing access?
No
Yes
Authorization and register of access to mobile computing
03
S. Officer
Human Resource SMP06
Yes
Authorization given?
No
Yes
Need external parties access?
Yes
Authorization and register of access of external parties
04
S. Officer
Access Control Register
Authorization given?
No
Yes
Regular review of access rights
05
S. Officer

1 – There is a need to request access in the following situations:

- a new employee of the Administrative Unit;
- a existing employee of ADETTI who needs to access the final financial reports
- a existing employee of ADETTI who needs to use laptops, which is property of ADETTI
- an new or existing partner who needs to access the financial statements integrated in the final financial report.

The request must be submitted to the S. Officer, by any format, by the employee or by the ADETTI manager who is responsible for managing the relationship with the partner.

2, 3, 4 – The S. Officer will authorize or reprove the requests and register the accesses granted. The authorization decision will be based on the business need for the access. The S. Officer must verify if the employee, which is requesting the access, has signed the Confidentiality Agreement and received a copy of the Recommended Security Practices (according to the Security Management Procedure of Human Resources). The request authorized will be recorded in the Access Control Register.

5 – The S. Officer must every month review the access logs.

The present procedure is owned by the S. Officer and must be review every year, according to SMP04. This procedure must be performed every 6 months (at least).

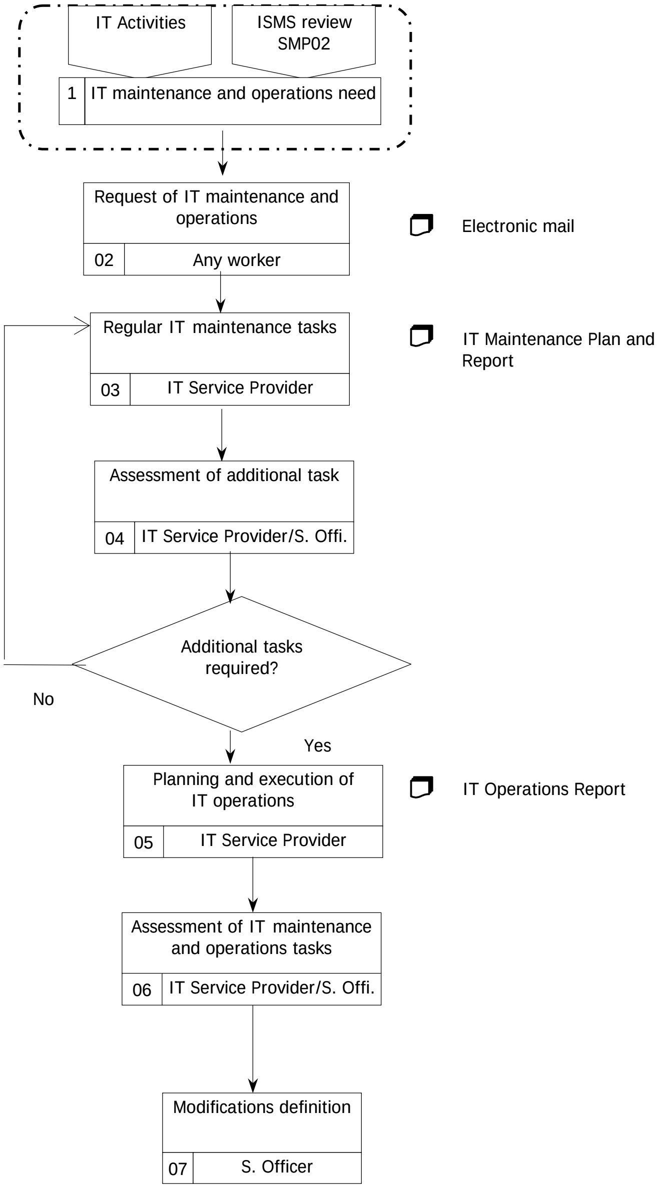
Security Management Procedure – SMP12

IT Maintenance and Operations

Page: 1 of 1	ISMS document: 2.12	Label: <1.0> Code: 0010101

1. Objective To protect IT resources

2. Process


IT Activities
ISMS review SMP02
1 IT maintenance and operations need
Request of IT maintenance and operations
02 Any worker
Electronic mail
Regular IT maintenance tasks
03 IT Service Provider
IT Maintenance Plan and Report
Assessment of additional task
04 IT Service Provider/S. Offi.
Additional tasks required?
No
Yes
Planning and execution of IT operations
05 IT Service Provider
IT Operations Report
Assessment of IT maintenance and operations tasks
06 IT Service Provider/S. Offi.
Modifications definition
07 S. Officer

1, 2 – A need of IT operations may be drawn from:

- IT activities;
- ISMS review - SMP02;

IT operations requests can be done by any employee by email.

3 – The IT service provider must conduct, with an established frequency, regular IT maintenance tasks. These tasks are defined and recorded in the IT Maintenance Plan and Report.

4 – The IT service provider with the S. Officer will assess, each week, if besides the maintenance tasks, further actions are required.

5 – All the tasks, which are not included in IT Maintenance Plan and Report, are regarded as IT operations. An IT operation can be the repair of hardware or buying a new system. The IT Service Provider, with the assistance of any other ADETTI employee if require, will accomplish these tasks.

6 – Each month the S. Officer and IT Service Provider will review all the IT tasks performed by the IT Service Provider and recorded in IT Maintenance Plan and Report and IT Operations Report.

7 – Based on the results of the security of the IT service, the S. Officer may define new maintenance tasks or any modification of the present procedure.

The present procedure is owned by the S. Officer and must be review every year, according to SMP04. This procedure must be performed every 6 months (at least).

Security Management Procedure – SMP13

Business Continuity Framework

Label: <1.0>

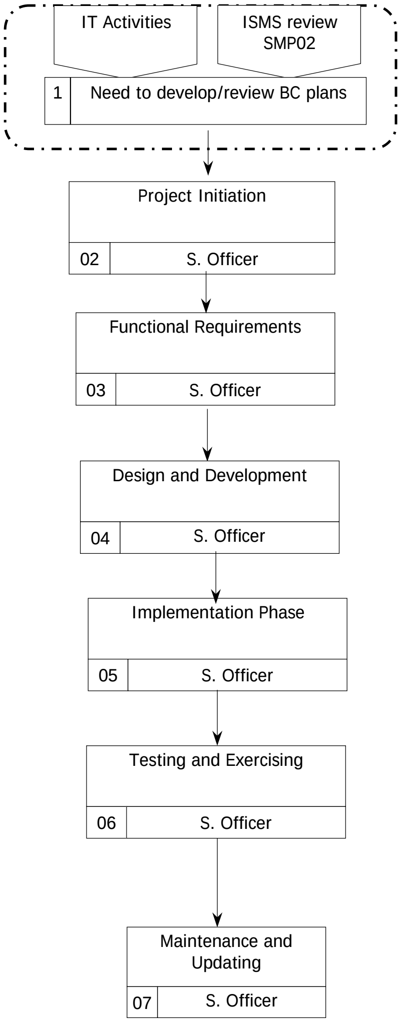
Page: 1 of 1

ISMS document: 2.13

Code: 0010101

1. Objective To ensure continuity of business operations in case of a major disaster

2. Process



1 – A need to develop or update an Business Continuity Plan may be drawn from:

- IT activities;
- ISMS review - SMP02;

2 – The S. Officer must initially define/review:

- Business Continuity Objective(s) and Requirements
- Scope and Cost of Business Continuity Project

3 – The S. Officer must collect data functional requirements from:

- Business Impact Analysis (BIA) and Time-Sensitive
- Alternative Business Continuity Strategy(ies)
- Cost-Benefit Analysis and Selected Strategy(Ies)

4 – The S. Officer must design plans in accordance with the following issues:

- Plan Scope and Objectives
- Business Recovery Organization (BRO) and
- Responsibilities (Recovery Team Concept)
- Escalation, Notification and Plan Activation
- Vital Records and Off-Site Storage Program
- Data Loss Limitations
- Plan Administration (general)

5 – The S. Officer must design plans for the following issues:

- Emergency Response Procedures (evacuation)
- Center (Crisis Management)
- Emergency Response Linkage to Business
- Recovery
- Detailed Resumption, Recovery and Restoration

6 – The S. Officer must test the plans according to:

- Exercise Plans, Scenarios and Actual Exercises
- Plan (Exercise) Evaluation
- Training, Corporate Awareness Program(s)

7 – The S. Officer must update the plans according to:

- Schedules and Budgets for Update and Maintenance
- Activities
- Software Tools for Update and Maintenance
- Review Criteria
- Program Status, Reporting and Audits
- Plan Distribution and Security

This procedure is based on the “Seven-Step Business Continuity Planning Model” from Disaster Recovery Institute, 2003.

The present procedure is owned by the S. Officer and must be review every year, according to SMP04. This procedure must be performed every 12 months (at least).

Part II
Level III documentation: Forms

adetti	Security Management Documentation	
Asset Inventory		Label: <1.0>
Page: 1 of 1	ISMS document: 3.1	Code: 0010101

Asset code	Asset general data				Asset evaluation							
	Asset name	Description	Location	Owner	CIA requirements	Legal requirements	Business requirements	C	I	A	B	T
[Assets type]												

[This template is developed in Annex C, section 4.3]

Version: 03.100804 Total Pages: 53
Approval: Issue date:
10/08/2004

This document list all documents included in the ISMS case study in ADETTI. The concepts employed in the below list are clarified in the ISMS Document Procedure.

ISMS document number	Description	Owner	Location of Master (illustrative)	Version
1.1	Policy Manual	Executive Board	F:\ISMS\Final_Version	0010101
2.1	Financial Reporting	AD Manager	F:\ISMS\Final_Version	0010101
2.2	Security Management Planning and Review	ADETTI President	F:\ISMS\Final_Version	0010101
2.3	Scope Management	Security Forum	F:\ISMS\Final_Version	0010101
2.4	ISMS Documentation Control	Security Officer	F:\ISMS\Final_Version	0010101
2.5	Risk Management	Security Officer	F:\ISMS\Final_Version	0010101
2.6	Human Resource Management	Security Officer	F:\ISMS\Final_Version	0010101
2.7	Incident Report Management	Security Officer	F:\ISMS\Final_Version	0010101
2.8	Document Classification	Security Officer	F:\ISMS\Final_Version	0010101
2.9	ISMS Audits	Security Officer	F:\ISMS\Final_Version	0010101
2.10	Corrective and Preventive Actions	Security Officer	F:\ISMS\Final_Version	0010101
2.11	Access Control	Security Officer	F:\ISMS\Final_Version	0010101
2.12	IT Maintenance and Operations	Security Officer	F:\ISMS\Final_Version	0010101
2.12	Business Continuity Framework	Security Officer	F:\ISMS\Final_Version	0010101
3.1	Asset Inventory	Security Officer	F:\ISMS\Final_Version	0010101
3.2	ISMS Documentation Register	Security Officer	F:\ISMS\Final_Version	0010101
3.3	Job Description	Security Officer	F:\ISMS\Final_Version	0010101
3.4	Confidentiality Agreement	Security Officer	F:\ISMS\Final_Version	0010101
3.5	Acceptable Use Agreement	Security Officer	F:\ISMS\Final_Version	0010101
3.6	Training plan	Security Officer	F:\ISMS\Final_Version	0010101
3.7	Recommended Security Practices	Security Officer	F:\ISMS\Final_Version	0010101
3.8	Incident Report Form	Security Officer	F:\ISMS\Final_Version	0010101
3.9	Preventive and Corrective Action Report	Security Officer	F:\ISMS\Final_Version	0010101
3.10	Nonconformity Report	Security Officer	F:\ISMS\Final_Version	0010101
3.11	Audit Plan	Security Officer	F:\ISMS\Final_Version	0010101
3.12	Audit Report	Security Officer	F:\ISMS\Final_Version	0010101
3.13	Management Review Input Report	Security Officer	F:\ISMS\Final_Version	0010101
3.14	Management Review Output Report	Security Officer	F:\ISMS\Final_Version	0010101
3.15	Training/Communication of Security Regulation	Security Officer	F:\ISMS\Final_Version	0010101
3.16	List of Requirements	Security Officer	F:\ISMS\Final_Version	0010101
3.17	List of Risks	Security Officer	F:\ISMS\Final_Version	0010101
3.18	Risk Treatment Plan	Security Officer	F:\ISMS\Final_Version	0010101
3.19	Detailed Risk Treatment Plan	Security Officer	F:\ISMS\Final_Version	0010101
3.20	Statement of Applicability	Security Officer	F:\ISMS\Final_Version	0010101
3.21	Access Control Register	Security Officer	F:\ISMS\Final_Version	0010101
3.22	IT Maintenance Plan and Report	IT Service	F:\ISMS\Final_Version	0010101

3.23	IT Operations Report	IT Service	F:\ISMS\Final_Version	0010101

Professional Profile	Job Title:	Security Officer
	Reference:	RF-008
	Unit:	Administrative unit
	Reports to:	President of ADETTI
	Job objective:	• Leading and conducting information security management, and providing consulting services to the organization’s management and staff.
	Main duties and responsibilities	• Identify protection goals, objectives and metrics consistent with corporate strategic plan. • Manage the development and implementation of security policy and procedures to ensure ongoing maintenance of security. • Physical protection responsibilities will include asset protection, workplace violence prevention, access control systems, video surveillance, and more. • Information protection responsibilities will include network security architecture, network access and monitoring policies, employee education and awareness, and more. • Maintain relationships with local law enforcement and other related government agencies. • Oversee incident response planning as well as the investigation of security breaches, and assist with disciplinary and legal matters associated with such breaches as necessary. • Work with outside consultants as appropriate for independent security audits.

Knowledge	**Education**	**Professional experience**
	• Higher education	• Must be an intelligent, articulate and persuasive leader who can serve as an effective member of the senior management team and who is able to communicate security-related concepts to a broad range of technical and non-technical staff. • Should have experience with business continuity planning, auditing, and risk management, as well as contract and vendor negotiation. • Must have strong working knowledge of pertinent law and the law enforcement community. • Must have a solid understanding of information technology and information security
		Languages
		• Portuguese, English

Confidentiality Agreement
Acordo de Confidencialidade [1]

Between:

ADETTI - Association for the Development of Telecommunications and Information Technology, with the number XXXXXXX, located in Av. Forças Armadas, Lisboa, represented by its President, José Miguel Dias, hereinafter referred to as EMPLOYEER.

And

(**Worker name and address**) hereinafter referred to as EMPLOYEE, agree to respect the present Confidentiality Agreement.

1st Clause

The EMPLOYEE will not, without the EMPLOYEER's prior written consent, disclose any information classified as confidential.

2 st Clause

The EMPLOYEE will employ its best endeavours to prevent the unauthorised publication or disclosure of any information classified as confidential.

3 st Clause

The EMPLOYEE may only divulge confidential information to those co-workers of the EMPLOYEER, with the proper clearance.

4 st Clause

The EMPLOYEE may not use the confidential information to any purpose other than for the permitted by the EMPLOYEER.

BY ADETTI **EMPLOYEE**

____________________ ________________________

[1] A copy in Portuguese language will be available.

Acceptable Use Agreement

Acordo de Utilização da Infra-estrutura da ADETTI [2]

Between:

ADETTI - Association for the Development of Telecommunications and Information Technology, with the number XXXXXXX, located in Av. Forças Armadas, Lisboa, represented by its President, José Miguel Dias, hereinafter referred to as EMPLOYEER.

And

(**Worker name and address**) hereinafter referred to as EMPLOYEE, agree to respect the present Confidentiality Agreement.

1st Clause

The EMPLOYEE accepts that information system of ADETTI is available for its researchers and staff to be used for the purpose of:

- research;
- personal educational development;
- administration and management of ADETTI business;
- consultancy work contracted to the ADETTI;
- reasonable use of computer facilities for personal correspondence, where not connected with any commercial activity, is at present regarded as acceptable.

ADETTI´s resources may not be used for any of the following:

- creation or transmission of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material;
- transmission of material that infringes the copyright laws applicable in Portugal;
- the transmission of unsolicited commercial or advertising material (such as spam or spim) to other organisations connected to ADETTI;
- deliberate unauthorised access to facilities or services accessible via ADETTI;
- deliberate activities that violate the privacy of users, disrupt or corrupts its work.

2 st Clause

The EMPLOYEE accepts that its general responsibilities as user of ADETTI infrastructure are:

- Only the registered holder shall use Usernames and other allocated resources. Users shall maintain a secure password to control access to their usernames on multi-user systems.

[2] A copy in Portuguese language will be available.

- No person shall by any wilful or deliberate act jeopardise the integrity of the computing equipment, its operating systems, systems programs or other stored information, or the work of other users, whether within the ADETTI or in other computing locations to which the facilities at the ADETTI allow connection. Such acts include the creation of network traffic high enough to significantly degrade network performance for other users, the use of tools to alter the behaviour of network devices, the scanning of ports on external computers and the unauthorised use of programs on central servers which consume such resources as significantly reduce the server's performance for other users.

- Users must secure ADETTI´s resources against theft and damage.

- Terminals which are not in use, should have user account locked.

- Data should be saved on a network drive.

- Laptops should not be left unattended in the office in plain sight.

- Users must comply with software copyright laws. Any employee found using unlicensed software will be forced to remove it and may be subject to disciplinary procedure.

- Users are obliged to comply with all ADETTI´s security policies and applicable Portuguese laws.

3 st Clause

The EMPLOYEE accepts that its responsibilities as Internet user in ADETTI infrastructure are:

- Internet browsing, which is not directly related to ADETTI, should be use rarely during working hours.

- Posted message on the Internet follow the same as rules as those for e-mail.

- The individual Internet usage should not cause a noticeable effect on the traffic rate of Internet for other users.

- Users cannot visit Web sites that display pornographic content.

4 st Clause

The EMPLOYEE accepts that its responsibilities as e-mail user in ADETTI infrastructure are:

- E-mail messages, which are not directly related to ADETTI, should be use rarely during working hours.

- The individual e-mail usage should not cause a noticeable effect on the e-mail traffic for other users.

- Users cannot send e-mails with pornographic content.

- The content of messages send or forward by ADETTI employees can not be interpreted as insulting or offensive by any other person or organization. On this definition is included any racial, religious, sportive slurs.

BY ADETTI **EMPLOYEE**

____________________ ________________________

Training sessions	Employees	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec

Sections	Definitions
1 Recommended practices	**1.1. Information systems acceptable use definition** Information system of ADETTI are available for its researchers and staff to be used for the purpose of: - research; - personal educational development; - administration and management of ADETTI business; - consultancy work contracted to the ADETTI; - reasonable use of computer facilities for personal correspondence, where not connected with any commercial activity, is at present regarded as acceptable. ADETTI´s resources may not be used for any of the following: - creation or transmission of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material; - transmission of material that infringes the copyright laws applicable in Portugal; - the transmission of unsolicited commercial or advertising material (such as spam or spim) to other organisations connected to ADETTI; - deliberate unauthorised access to facilities or services accessible via ADETTI; - deliberate activities that violate the privacy of users, disrupt or corrupts its work.
	1.2. General users responsibilities . - Only the registered holder shall use Usernames and other allocated resources. Users shall maintain a secure password to control access to their usernames on multi-user systems. - No person shall by any willful or deliberate act jeopardise the integrity of the computing equipment, its operating systems, systems programs or other stored information, or the work of other users, whether within the ADETTI or in other computing locations to which the facilities at the ADETTI allow connection. Such acts include the creation of network traffic high enough to significantly degrade network performance for other users, the use of tools to alter the behavior of network devices, the scanning of ports on external computers and the unauthorized use of programs on central servers which consume such resources as significantly reduce the server's performance for other users. - Users must secure ADETTI´s resources against theft and damage. - Every time the last staff member exits the room, it must close down the door - Terminals which are not in use, should have user account locked. - Data should be saved on a network drive. - Laptops should not be left unattended in the office in plain sight. - Users must comply with software copyright laws. Any employee found using unlicensed software will be forced to remove it and may be subject to disciplinary procedure. - Users are obliged to comply with all ADETTI´s security policies and applicable Portuguese laws

Sections	Definitions
1 Recommended practices	**1.3. Responsibilities for Internet usage** - Internet browsing, which is not directly related to ADETTI, should be use rarely during working hours. - Posted message on the Internet follow the same as rules as those for e-mail. - The individual Internet usage should not cause a noticeable effect on the traffic rate of Internet for other users. - Users cannot visit Web sites that display pornographic content.
	1.4. Responsibilities for e-mail usage - E-mail messages, which are not directly related to ADETTI, should be use rarely during working hours. - The individual e-mail usage should not cause a noticeable effect on the e-mail traffic for other users. - Users cannot send e-mails with pornographic content. - The content of messages send or forward by ADETTI employees can not be interpreted as insulting or offensive by any other person or organization. On this definition is included any racial, religious, sportive slurs, (for example any offensive remarks regarding Sport Lisboa & Benfica is prohibited).
2. Guidance principles	Information system is any computer or other type of resource that holds information or that is used in its processing.
3. Accountability	All researches and staff have a personal responsibility to ensure that they, and others who may be responsible to them, are aware of and comply with the present instructions.
4. Enforcement	ADETTI holds the right to apply disciplinary measures and criminally prosecute employees, which have been engaged in security violations.
5. Reference to ISO 17799	6. Personnel 9.2 User Access Management
6. Revision	This document should be revised by the Security Forum on an annual basis, according to the applicable security procedure.
7. Audience	All ADETTI staff members.
8. Glossary	Spam - unsolicited e-mail messages, generally with a commercial or advertising purpose Spim - unsolicited instant messages, generally with a commercial or advertising purpose

adetti	Security Management Documentation	
Incident Report Form		Label: <1.0>
Page: 1 of 1	ISMS document: 3.8	Code: 0010101

Incident Report number: _____________

1.General Data

Employee: _______________

Date: _______________

Time: _______________

2. Incident details

Description: ____
____
____
____

Was the issue resolved? If yes, how? _____________________________________
____
____

What further actions do you suggest? _____________________________________
____
____

Was the Incident reported to:

Security Officer □
Security Forum □
Other:____

Signature: ____________________________

3. Follow-up (for the security department)

Actions taken as follow-up (please indicate actions and who is accountable for each one):
____
____
____

Date of actions of follow-up completed: _______________________________

Signature: ____

Preventive and Corrective Action Report

Action: **Preventive** □ **Corrective** □

PROBLEM

DESCRIPTION:

SUBMITTED BY:	**APPOINTED WORKERS FOR THE PROBLEM ASSESSMENT:**	**DEALDINE:**
DATE: / /		**SIGNATURE:**

DETERMINING THE CAUSES OF THE PROBLEM AND ACTION PROPOSAL

CAUSE(S):

ACTION TO IMPLEMENT: **PROPOSED BY:** **DATE: DD/MM/YYYY**	**ACTION OBJECTIVES:**

APPROVED:	**APPROVAL DATE: DD/MM/YYYY**
EXECUTION RESPONSIBLE(S):	**EXECUTION DEALDLINE: DD/MM/YYYY**

IMPLEMENTATION AND FOLLOW UP ACTIONS

ACTION CONCRETIZATION (OBSERVATIONS):	**FINISHED IN: DD/MM/YYYY**
	SIGNATURE:

ACTION CONCLUTION

RESULTS:	**ANNEXES:** o REPORT ______________ o AUDIT ______________ o DATA ______________ o OTHERS ______________

EFFECTIVE ACTION? o YES o NO CLOSING DATE: DD/MM/YYYY	**COMMENTS:** SIGNATURE DATE: DD/MM/YYYY

adetti	Security Management Documentation	
Nonconformity Report		Label: <1.0>
Page: 1 of 1	ISMS document: 3.10	Code: 0010101

DETETION					
ISMS audits	□	**Access control review**	□	**Incident management**	□
ISMS Planning and Review	□	**Other:**	___		□

SECURITY REGUALTION (POLICY, PROCEDURE):

PROBLEM

DESCRIPTION:

DATE: / / SIGNATURE:

IDENTIFICATION / ASSESSMENT OF NONCONFORMITIES CAUSES

SIGNATURE:	SIGNATURE:

DECISION

○ **Accept** ○ **Open Corrective / Preventive Action Nº __________** ○ **________________________**	**Observations:** **Date: / / Signature:**

ACTION PLAN			**FOLLOW-UP PLAN**		
Action	**Responsible**	**Date**	**Performed**	**Controlled**	**Date**

CONCLUSION

○ **Action plan finished** ○ **Open Corrective / Preventive Action Nº__________** ○ **Close out process**	**Observations** **Date: / / Signature**

adetti	Security Management Documentation	
Audit Plan		Label: <1.0>
Page: 1 of 1	ISMS document: 3.11	Code: 0010101

ISMS	Auditor *	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Financial Reporting													
Security Management Planning and Review													
Scope Management													
ISMS Documentation Control													
Risk Management													
Human Resource Management													
Incident Report Management													
Document Classification													
ISMS Audits													
Corrective and Preventive Actions													

* - Assign auditors that do not have a conflict of interest with respect to the audited area or activity.

adetti	Security Management Documentation	
Audit Report		Label: <1.0>
Page: 1 of 3	ISMS document: 3.12	Code: 0010101

AUDIT SCOPE: ______________________________

AUDIT CRITERIA: BS 7799-2:2002

DATE:

AUDITORS:

AUDIT METHODS: ______________________________ ______________

NORMATIVE CLAUSE		NC Nº	Major NC Nº	Notes
4.1 GENERAL REQUIREMENTS				
4.2.1 ESTABLISHING THE ISMS				
4.2.2 IMPLEMENT AND OPERATE THE ISMS				
4.2.3 MONITOR AND REVIEW THE ISMS				
4.2.4 MAINTAIN AND IMPROVE THE ISMS				
4.3.1 GENERAL				
4.3.2 CONTROL OF DOCUMENTS				
4.3.3 CONTROL OF RECORDS				
5.1 MANAGEMENT COMMITMENT				
5.2.1 PROVISION OF RESOURCES				
5.2.2 TRAINING, AWARENESS AND COMPETENCY				
6.1 GENERAL				
6.2 REVIEW INPUT				
6.3 REVIEW OUTPUT				
6.4 INTERNAL ISMS AUDITS				
7.1 CONTINUAL IMPROVEMENT				
7.2 CORRECTIVE ACTION				

7.3 PREVENTIVE ACTION				
A.3 SECURITY POLICY				
A.4 ORGANIZATIONAL SECURITY				
A.5 ASSET CLASSIFICATION AND CONTROL				
A.6 PERSONNEL SECURITY				
A.7 PHYSICAL AND ENVIRONMENTAL SECURITY				
A.8 COMMUNICATIONS				
A.9 ACCESS CONTROL				
A.10 SYSTEM DEVELOPMENT				
A.11 BUSINESS CONTINUITY				
A.12 COMPLIANCE				

NOTES	DESCRIPTION

AUDIT SYNTHESIS

OBSERVATIONS AND IMPROVEMENT OPORTUNITIES

º	CLASULE	SEVERITY 1)	NONCONFORMITIES DESCRIPTION

1) Classification: Major Nonconformity **M**; minor nonconformity **m**.

Document structure:

Table of Contents
1. Introduction
2. ADETTI objectives
3. ADETTI Information Security Policy Statement
4. Security external constraints and trends
    4.1 Technological products supply
    4.2 Security service supply
    4.3 Legal requirements
    4.4 Outlook of the level of threats and vulnerabilities (based on reports such as the CSI/FBI Computer Crime and Security Survey [CSI04])
5. ISMS assessment
    5.1 Assessment of the Information Security Policy Statement
    5.2 Assessment of the support process (communication and revision) of the Information Security Policy Statement
    5.3 Assessment of the fulfilment of the security objectives
    5.4 Assessment of the information provided by interested parties (suggestions of partners, employees)
    5.5 Assessment of the information collected by the Security department of ADETTI
        5.5.1 Assessment of non-conformity data
        5.5.2 Assessment of corrective and preventive action
        5.5.3 Assessment of results of ISMS audits
        5.5.4 Assessment of results of previous management reviews
        5.5.5 Assessment of results of security incidents
        5.5.6 Assessment of the resources of the ISMS (human resources, technological and physical resources)
        5.5.7 Assessment of the ISMS processes (e.g. business continuity management)
        5.5.8 Assessment of the effectiveness of the ISMS
    5.6 Proposal of recommendations for improvement.

Date	DD/MM/YYYY	Agenda:	1. Review conclusions of the “Management Review Input Report” 2. Follow-up actions from the previous reviews (included in the “Management Review Input Report”) 3. Revision of policies, procedures and controls to respond to the modification of the internal or external protection requirements (e.g. new law and business strategies) and identified risks that may impact on the ISMS. 4. Review opportunities for the improvement of the effectiveness of the ISMS. 5. Establish security objectives (e.g. reduce security incidents due to malicious code infection in 30%).
Period to	From DD/MM/YYYY To DD/MM/YYYY (from the last management review to the present date)		
Participants (name & title):			

Security objectives established by this management review

Objective	**Measure (if applicable)**	**Previous Period**	**Previous Period Value**	**Next Target Period**	**Next Target Value**	**Status Next Mngmt Review**

Topic 1: Follow-up actions from previous managements reviews				
Item	**Description / Conclusions**	**Action**	**Assigned to**	**Due date**

Topic 2: Modification of policies, procedures and controls				
Item	**Description / Conclusions**	**Action**	**Assigned to**	**Due date**

Topic 3: Opportunities for the improvement of the ISMS				
Item	**Description / Conclusions**	**Action**	**Assigned to**	**Due date**

Training/Communication of Security Regulation

Label: <1.0>

Page: 1 of 1

ISMS document: 3.15

Code: 0010101

Employee name	Training or communication of the following security regulation	Employee signature	Date

Security Management Documentation

List of Requirements

Label: <1.0>

Page: 1 of 1 | ISMS document: 3.16 | Code: 0010101

Business requirements

ID	Strategic requirement	Underlying issue	Implications for security management

Legal requirements

Issues	Applicable legislation	Description	Implications in security management	Actions to ensure compliance
L1. Type of legislation				

Contractual requirements

ID	Organization	Supporting document	Type of relationship	Implications for security management

Security Management Documentation

List of Risks

Label: <1.0>

Page: 1 of 1 | ISMS document: 3.17 | Code: 0010101

Asset	A v	Threat	Vulnerability	Probability	P V	Impact	I V	Risk	Ref.
Type of assets									

Risk Treatment Plan

Asset	Threat	Vulnerability	Risk level	Treatment option	Applicable Controls	Risk reduced	Residual risk	Cost	Time	Selected
							NA	NA	NA	NA

Detailed Risk Treatment Plan

Risk priority:		**Risk:**
Risk owner:		
Risk description:		

Risk Assessment	**Risk value**	**Asset value**	**Vulnerability**	**Threat**
Risk Indicators				

Control implemented	**Risk reduced**	**Residual risk**	**Performance of risk indicators**	**Comments from last review**	**Status of actions**	**Done by**	**Date of next**

N.	Clause	Applied	Rationale	Risk reference	ISMS document reference

Security Management Documentation

Access Control Register

Label: <1.0>

Page: 1 of 1

ISMS document: 3.21

Code: 0010101

Employee name	Access control request	Authorized Yes or No	Employee signature	Observations	Date

IT Maintenance Plan and Report

Maintenance Task	Server or desktop name	Frequency	Performed Yes or No	Observations	Employee	Date
Daily full backup		Daily				
Offsite backup (copy of full backup in an tape to place off premises)		Weekly				
Testing and installing patches		Weekly				
Upgrading software		Weekly				
Deleting temporary files		Weekly				
‘Defragging’ the hard disk		Monthly				
Computer cleaning (remove dust near fans and power supplies)		Weekly				

IT Operations Report

Operation	Server or desktop name	Duration	Observations	Employee	Date