Revista de Gestão & Tecnologia

ISSN 2358-3126

INFORMATION SECURITY AND ISO 27001

Felipe Souza Pinheiro, email: felipe.pinheirosouza@gmail.com
Waldir Ribeiro Junior, email: ribeiro.waldir2@gmail.com

Abstract*. This article aims to disseminate a totally contemporary subject matter, and of great interest by companies / organizations; this comes talk about information security and the ISO who understands. This work also seeks to show some settings on the treaty issue, and ISO implementation methodology. ISO 27001 focuses on information security, and comes to establish procedures and structures to be taken by a company to achieve a high level of quality, safety and commitment to its products and services.*

Keywords*: security, information, ISMS, ISO.*

1. INTRODUCTION

The security of information is shown essentially and even critical in some cases, so that the consistency of the systems is not affected, ensuring reduction in risks of fraud, errors, leaks, theft and misuse of information (ABREU, 2011). When managed properly it allows you to operate with confidence. Information security management gives you the freedom to grow, innovate and expand its portfolio of customers, knowing that all your confidential information will remain so.

To preserve documents to digital heritage, the system must demonstrate reliability (THOMAZ and SOARES, 2004). Currently it is perceived that a network implies the ability to work and trust each other, then there is a new scenario of the preservation of digital archives management.

The objective of this article is to strengthen the dissemination of an ISO little used in the national environment, thus a bibliographic study was performed in order to provide details on the implementation and methodology of this ISO.

As a result of this work is expected strengthen and integration of information security with the business goals of the organization, using the only international language through family standards of ISO 27000 (RIBAS, 2010).

2. INFORMATION SECURITY

The concept of information security according to ABNT NBR ISO/IEC 17799:2006 is the protection of itself from various types of threats to ensure business continuity, minimize risk and maximize return and business opportunities. Thus we have the view that the information security interferes directly in the company's results. The ABNT (2006) also indicates in standard that the information needs to be protected appropriately in order to maintain its confidentiality, integrity and availability and the lack of compliance with these requirements may lead to negative results.

The applications of an Information Security Management System second the NBR ISO/IEC 27001 adopts as a process of approach the PDCA model (Plan-Do-Check-Act).

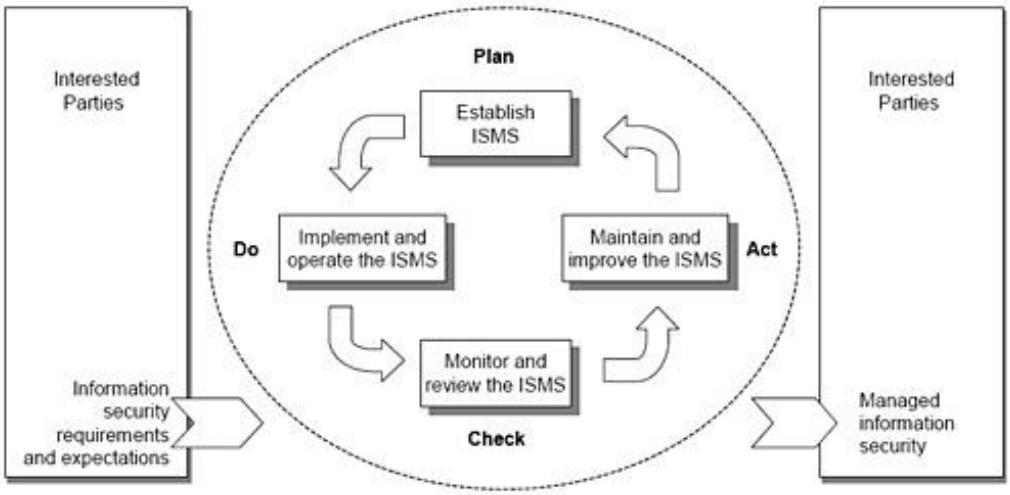

Figure 1. PDCA model applied to ISMS processes.
Source: NBR ISO/IEC 27001

PLAN (Establish ISMS)	**Establish ISMS policy, objectives, processes and procedures relevant to managing risk and improving IS to deliver results in accordance with an organization's overall policies and objectives.**
DO (Implement and operate ISMS)	**Implement and operate ISMS policy, controls, processes and procedures.**
CHECK (Monitor and review ISMS)	**Asses, and where applicable, measure process performance against ISMS policy, objectives and practical experience and report the results to management for review.**
ACT (Maintain and Improve ISMS)	**Take corrective actions, based on the results of the internal audit and management review or other relevant information, to achieve continual improvement of ISMS.**

Figure 2. PDCA Activity.
Source: NBR ISO/IEC 27001

It is essential the role of the Information Security Manager in this context, and this one should have maximum autonomy and authority as possible to develop, deploy, and maintain processes in order to increase the chances of success in information protection (FONTES, 2012). The same author points out that even with this freedom, the information manager should be subject to regulations and controls indicated in the policy.

2.1. Information Security Principles

We must protect the assets from threats of all kinds, in order to guarantee the three basic principles of information security that are (ABNT ISO 177799, 2006):

- Confidentiality: The information must be known only by individuals holding the access permissions.
- Integrity: the information should be kept in their original state, without changes.
- Availability: Access to all data when needed for use.

2.2. Threats

By threats it is understood the elements that are able to exploit vulnerabilities and cause severe problems to the assets of a company (MODULO, 2007). Assets are continually exposed to existing threats that may endanger the three principles of information security. We can cite the following threats:

- Natural;
- Intentional;
- Involuntary.

2.3. Vulnerability

Vulnerability is the deficiency of various origins, which often are not identified in time or even when it occurs, are not properly addressed in order to prevent an attack (NAKAMURA, 2002).

The vulnerabilities could come from various sources, such as (SEMÔLA, 2002):

- Natural agents;
- Hardware;
- Software;
- Storage Media;
- Media;
- Human.

2.4. Risks

It can be said that are the possibilities of threats to exploit the vulnerabilities, causing damage or data loss, providing damage to the company's business and which ultimately affect the principles of confidentiality, integrity and availability (MODULO, 2007).

2.5. Attackers

Attackers are the individuals who carry out an attack on a computer system by exploiting their vulnerabilities, which may or may not succeed (NAKAMURA, 2002). The attackers are better known as hackers, however, there are a variety of attackers, among them are:

- Preackers;
- Scrip kiddies;
- Carders;
- Insiders.

2.6. Attacks

These can occur when vulnerabilities are not treated to contain or even correct known problems. Collect competitive information of the types of attacks is a necessary step to initiate an information security action plan (HATCH, 2003). Some examples of common attacks are

- Attack at the application level;
- Attack on the web server;
- Buffer-overflow;
- Exploit;
- SQL-Injection;
- Trojan;
- Worm;
- Physical attack;
- Denial of Service;
- Packet Sniffing;
- Scan.

2.7. Tools for Information Security

Tools for information security are the set of software, hardware and techniques that are mainly intended to combat the attacks (CHESWICK, 2005). They are found to cross-platform operating systems such as Microsoft Windows (MICROSOFT WINDOWS SERVER 2003) and Linux (LINUX, 2008). Many of these tools are used together to thereby provide greater security.

Here are some tools for information security:

- Firewall;
- Packet filter;
- Proxy;
- Personal Firewall;
- Reactive Firewall.

2.8. Information Security Standards

The standards play an essential role in the development of an information security plan (KARABACAK, 2006). They provide a systematic approach of management to adopt the best practices in controls, quantify the acceptable level of risk and implement appropriate measures to protect the confidentiality, integrity and availability of information (DEY, 2007).

The 27000 series of ISO/IEC standards focuses on requirements, security controls and orientation for implementing an ISMS in the organization (McGee, 2007).

3. ISO 27001

The ISO "International Organization for Standardization" is an organization based in Switzerland (ABNT ISO 27001, 2006). The ISO abbreviation originated from the word Isonomy, and its function is to develop and promote standards that can be used equally in all countries. Brazil is represented by the Brazilian Association of Technical Standards - ABNT.

ISO 27001 has emerged based on the British standard BS7799 and ISO/IEC 17799 (FENZ, 2007). It was prepared to provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a system of information security management (NBR ISO/IEC 27001: 2006).

The ISO 27001 standard (ABNT ISO 27001, 2006) provides features and requirements so that the organization can structure an information security management system (ISMS).

It incorporates a risk escalation process and value-oriented assets for analysis and identification of risks and the implementation of controls to minimize them (ABNT ISO 27001, 2006). The degree to which the system is arranged and contains structured processes will facilitate the replication of a system from one location to another. A company can implement ISO 27001 at its headquarters and then replicate it in their branches.

This standard is the first in information security related with the family of standards ISO/IEC (FENZ, 2007). The table below shows the chapters of the standard.

Clause	Name	Description
0	Introduction	Presentation of the standard
1	Scope	Scope of the standard
2	Normative References	Other necessary standards for ISMS
3	Terms and Definitions	Terms and definition of information security
4	Information Security Management System	Information on the establishment, implementation, monitoring and improvement of an ISMS
5	Responsibilities of the direction	Management commitment, training and provision of resources for the ISMS.
6	Internal ISMS audits	Internal audits carried out by trained and committed staff with the ISMS
7	Critical analysis of the ISMS	Analysis conducted by the organization's direction about the actions taken by the ISMS.
8	ISMS Improvements	Corrective and preventive actions carried out by the ISMS

Figure 3. Descriptions of ISSO 27001 chapters.
Source: NBR ISO/IEC 27001

3.1. Requirements

According to the standard of ABNT ISO 27001, 2006.

Requirements No. 1, 2 and 3 refer respectively to Scope, Normative Reference and Terms and Definitions, being all informative.

The Requirement No.4 deals with the creation, implementation, monitoring and improvement of the ISMS, it is through this requirement that define the participating members of the ISMS, the necessary documents and records which we must maintain.

In Requirement No. 5 is presented the responsibility of the direction which is referred to the allocation of the ISMS responsibilities such as provision of training and resources necessary for the ISMS.

The Requirement No. 6 deals with internal audits and defines which areas should be audited, the frequency of them and who may be responsible auditors. Regarding this last point, we note that the auditor should not assess processes for which it is responsible.

In Requirement No. 7 of critical ISMS analysis shows the need of direction to check the actions taken by the ISMS, acting as a single control element.

And finally Requirement No. 8 deals with the improvement of ISMS. The ISMS is a committee that has a dynamic that, through internal audits and critical analyses of management, can improve their actions and thus take care of information security.

Item	Requirement	Description
1	Scope	Scope of the standard
2	Normative Reference	Document that serves as a reference for application of ISO 27001
3	Terms and Definitions	Terms and definitions used in the standard
4	Information Security Management System	Requirements for creating, implementing, monitoring, improvement, documentation and registration of ISMS information.
5	Responsibilities of the direction	Definition of responsibilities, training and provision of ISMS resources.
6	Internal Audits	Internal audits to determine whether the objectives of ISMS are being achieved.
7	Critical analysis of the ISMS	Analysis carried out by the organization's direction in verifying the actions of the ISMS
8	ISMS Improvements	Continuous improvement of the effectiveness of the ISMS

Figure 4. ISO 27001 requirements.
Source: NBR ISO/IEC 27001

Three central pillars were identified for this certification: organization, technology and management (THOMAZ, 2004).

Organization: certifies the obligation, the scope, the objectives, the financial availability and the commitment of an organization to engage in digital preservation (THOMAZ, 2004).

Technology: certifying the fitness of the technical infrastructure of the organization and its ability to meet demands of management and of the digital objects (THOMAZ, 2004). It involves hardware, software, storage media, networks, security measures, workflow managers, protocols, documentation and skills.

Management: ensures the functions, processes and procedures required to manage the actual digital objects (THOMAZ, 2004).

3.2. Implementation of ISO 27001

The author Marcos Sêmola (SÊMOLA, 2002) suggests a series of measures, but only makes suggestions that we can find in their own ISO standards. It then developed a method in order to provide a logical framework for implementing information security (SOUZA, Ranieri Marinho, 2007).

Follows the model proposed by Ranieri Marinho de Souza (SOUZA, Ranieri Marinho, 2007):

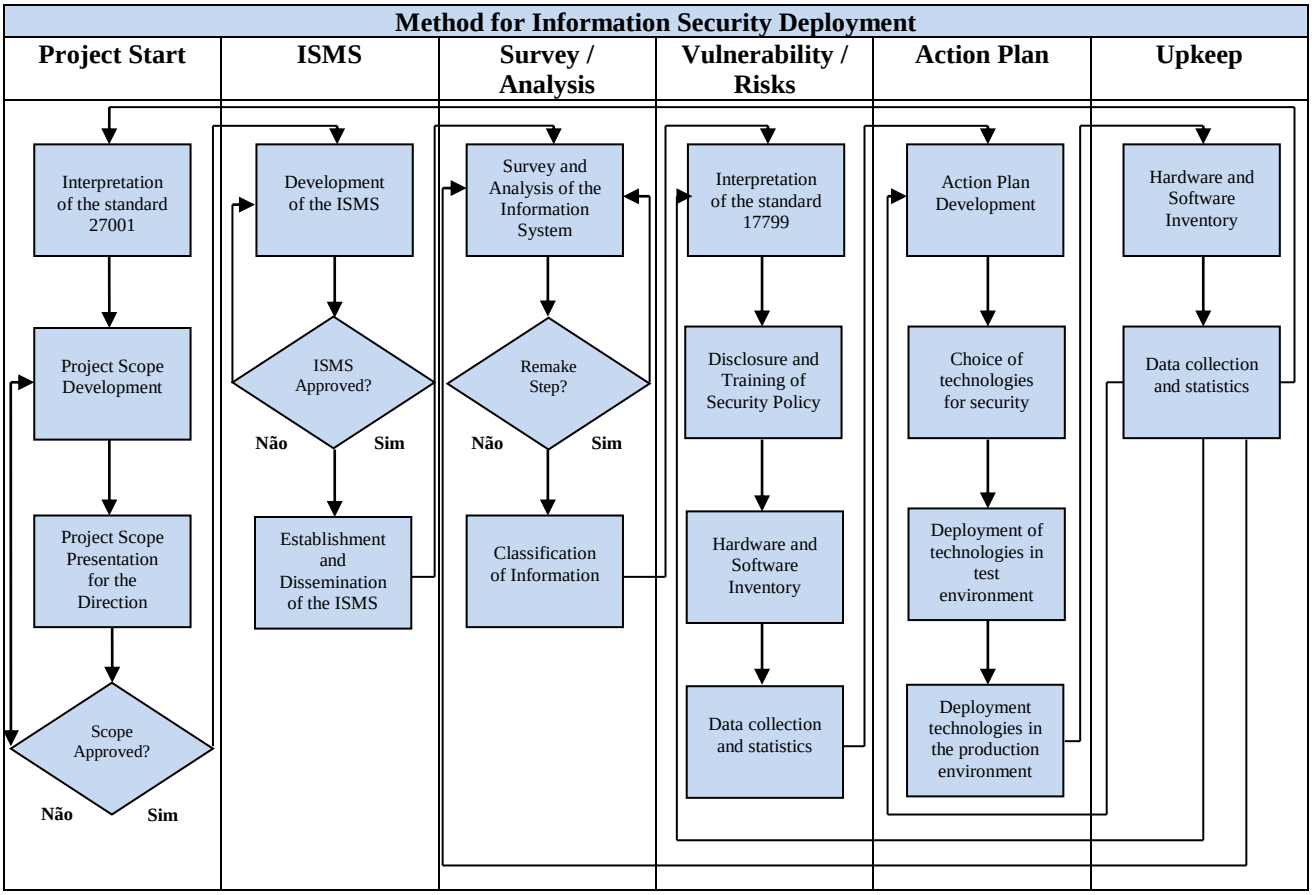

Figure 5. Method flow chart for the implementation of Information Security.
Source: SOUZA, Ranieri Marinho, 2007.

3.3. Cost of Implantation

We cannot tell the exact amount immediately, it depends on the size of your organization or business unit that will be included in the scope of ISO 27001, on the degree of importance of information (e.g., information on banks are considered most critical and require more protection), on the technology used by the organization (e.g., data centers tend to have higher cost because of its complex systems), and on the requirements of legislation (in general, financial and government sectors are highly regulated concerning information security) (KOSUTIC, 2011). It is impossible to calculate the exact costs before you know what level of protection you need. Before, it must be performed a risk assessment, as this analysis indicates the necessary security measures.

The implantation time of the standard varies with reality, maturity and size of the organization, as these depend on the implementation and adaptation of the requirements, policies, procedures, controls and practices required by ISO 27001 (SEMÔLA, 2002).

Ranking	Country	Amount
1º	Japan	3499
2º	India	494
3º	United Kingdom	444
4º	Taiwan	373
5º	China	362
6º	Germany	137
7º	Korea	106
8º	USA	96
9º	Czech Republic	85
10º	Hungary	71
11º	Italy	60
12º	Poland	56
13º	Spain	40
14º	Ireland	37
15º	Austria	35
16º	Thailand	34
17º	Hong Kong	31
18º	Australia	29
19º	Greece	27
20º	Malaysia	27
21º	Romania	26
22º	Mexico	24
23º	**Brazil**	**23**
24º	Turkey	21
25º	United Arab Emirates	19

Figure 6. List of countries with the highest number of certifications.
Source: www.iso27001certificates.com, accessed in 06/23/2010.

3.4. Benefits

Companies / organizations that have adopted this set of specifications, acquired certainly a range of benefits, such as (KOSUTIC, 2011):

_ Risk identification and definition of controls to manage them or eliminate them;
_ Flexibility to adapt the controls to all areas or selected areas of your company;
_ Earn the trust of stakeholders and customers, who know that their data is protected;
_ Demonstrate compliance and get the status of preferred supplier;
_ Meets most sensitive expectations, demonstrating compliance.

Name of the Organization	Country	Certificate Number	Certification Body	Standard BS 7799-2:2002 or ISO/IEC 27001:2005
Atos Origin Brasil Ltda	Brazil	IS 98429		ISO/IEC 27001:2005
Axur Information Security	Brazil	IS 509742		ISO/IEC 27001:2005
BT	Brazil	LRQ 4003984	LRQA	ISO/IEC 27001:2005
Cardif do Brasil Vida e Previdencia S/A	Brazil	IS 521855		ISO/IEC 27001:2005
CIP Camara Interbancaria de Pagamentos	Brazil	IS 96934		ISO/IEC 27001:2005
Fucapi-Fundacao	Brazil	IS 504391		ISO/IEC 27001:2005
IBM ITD Brazil	Brazil	62.691	Bureau Veritas Certification - Brazil	ISO/IEC 27001:2005
Módulo Security Solutions S/A	Brazil	IS 510466		ISO/IEC 27001:2005
Poliedro - Informática, Consultoria e Serviços Ltda.	Brazil	44121081309		ISO/IEC 27001:2005
Prodesp	Brazil	IS 512881		ISO/IEC 27001:2005
Promon Engenharia Ltda.	Brazil	IS 500248		ISO/IEC 27001:2005
Promon Tecnologia Ltda	Brazil	IS 500564		ISO/IEC 27001:2005
Samarco Mineração S/A.	Brazil	IS 524157		ISO/IEC 27001:2005
SERASA S.A.	Brazil	262326 ISMS		ISO/IEC 27001:2005
Serviço Federal de Processamento de Dados - SERPRO	Brazil	IS 515421		ISO/IEC 27001:2005
Superior Tribunal de Justiça	Brazil	IS 538457		ISO/IEC 27001:2005
Telefonica Empresas S/A	Brazil	IS 501039		ISO/IEC 27001:2005
Tivit Tecnologia da Informacao S.A.	Brazil	00017-2006-AIS-OSL-NA	DNV	ISO/IEC 27001:2005
TIVIT TERCEIRIZAÇÃO DE TECNOLOGIA E SERVIÇOS S.A.	Brazil	16203-2007-AIS-BRA-NA	DNV	ISO/IEC 27001:2005
T-Systems Brazil	Brazil	336227 ISMS		ISO/IEC 27001:2005
T-Systems do Brasil Ltda.	Brazil	341898 ISMS		ISO/IEC 27001:2005
UNISYS Global Outsourcing	Brazil	IS 97102		ISO/IEC 27001:2005
Zamprogna S/A Importacao	Brazil	IS 518855		ISO/IEC 27001:2005

Figure 7. List of organizations that are certified in Brazil.
Source: www.iso27001certificates.com, accessed in 06/21/2010.

4. ACKNOWLEDGEMENTS

First thank God for all health and will power granted to us; thank you also to all for whom we had the pleasure to live in an environment that has become almost familiar.

Thank you Mr. Teacher Lucio Garcia Veraldo Junior who knew with all attention and dedication help us in all tasks to be accomplished in this school matrix.

And last but not least we would like to thank our parents, who have always been at our side helping us, supporting, and especially for all the patience they had with us.

5. REFERENCES

ABNT ISO 27001, 2006. Brazilian Association of Technical Standards. Standard ABNT NBR ISO/IEC 27001: 2006 – Security Information Management System.

ABNT NBR ISO/IEC 27001:2006 “Security Information Management System – Requirements, 2006”.

ABREU, Leandro F.S.A., 2011, “Information Security in Social Networks”, Sao Paulo.

CHESWICK – W. ; Bellovin, S. M; Rubian A.D., “Firewalls e segurança na internet” 2ed. RS Bokman. 2005.

DEY, M., 2007, “Information security management – a practical approach In: Africon 2007”, 8th IEEE Africon Conference. p.1-6.

FENZ, S., Goluch G., Ekelhart A., Riedl B., Weippl E., 2007, “Information Security Fortification by Ontological Mapping of the ISO/IEC 27001 Standard In: PRDC 2007”, 13th Pacific Rim International Symposium on Dependable Computing, p.381-8.

FONTES, Edison Luiz Gonçalves, 2012, “Policies and Standards for information security”, 1.Ed. Rio de Janeiro: Brasport.

HATCH, Brian; LEE, James; KURTZ, George, “Security against Hackers”, SP: Futura, 2003.

KARABACAK, B. Sogukpinar, 2006, “A quantitative method for ISO 17799 gap analysis”, Computers & Security, 25(6);413-9.

KOSUTIC, Dejan, February, 8/2011, “27001 Academy-treinamentos”. Available in: < http://advisera.com/27001academy/pt-br/blog/2011/02/08/qual-e-o-custo-da-implementacao-da-iso-27001/>.

LINUX, Linus.org. 2008. Available in: <www.linux.org>.

NETWORK, Faculdade, 2013, “College Magazine of Information Systems”, n.1, PP. 77-86.

NEUBAUER, T., Ekelhart, A., and Fenz, S., 2008, “Interactive Selection of ISO 27001 Controls under Multiple Objectives”, vol. 278, Boston: Springer, pp. 477-491.

MARCIANO, João L. P., 2006, “Information Security - a social approach”, Brasília.

McGEE, AR Bastry FA, Chandrashekhar U, Vasireddy SR, Flynn LA, 2007, “Using the bell labs security framework to enhance the ISSO 17799/27001 information security management system”, Bell Labs Technical Journal, 12(3):39-54.

MICROSOFT WINDOWS SERVER, 2003. Version 2003, Microsoft Corporation. 2003, 1 CD-ROM.

RIBAS, Carlos Eduardo, 2010, “Information security management system in health care organizations”, Sao Paulo.

SÊMOLA, Marcos, 2002, “Information Security management: an executive view”, publishing company: Campus Elsevier, 2ª edition, pp. 43-73.

SOUZA, Ranieri Marinho, 2007, “Deployment tools and information security techniques in accordance with ISO 27001 and ISO 17799”, PUC – Minas.

THOMAZ, Katia P., jan/jun. 2007, “Trusted digital repositories and certification”, Rio de Janeiro, vol. 3, n.1, pp. 59-80.

THOMAZ, Katia P. e SOARES, Antonio José, fev. 2014. “Digital preservation and the reference model Open Archival Information System (OAIS). Data Grama Zero”, v. 5, n. 1. Available in:<http://www.dgz.org.br/fev04/F_I_art.htm>. Accessed in: July 23, 2007.

6. COPYRIGHT