ISO/IEC 15504 BEST PRACTICES TO FACILITATE ISO/IEC 27000 IMPLEMENTATION

Antonia Mas, Antoni Lluís Mesquida, Esperança Amengual
Department of Mathematics and Computer Science, University of the Balearic Islands, Palma de Mallorca, Spain

Bartomeu Fluxà
Brújula Tecnologías de la Información S.A., Palma de Mallorca, Spain

Keywords: ISO/IEC 15504 (SPICE), ISO/IEC 27000, Information security, Software Process Improvement (SPI).

Abstract: In software development companies, as well as in any company, information must be adequately protected. Therefore, the implementation of information security standards has also become crucial in software organizations. Software companies involved in a process improvement initiative according to the ISO/IEC 15504 standard for process assessment and improvement are showing an increasing interest in the implementation of the ISO/IEC 27000 standard for information security management. With the intention of supporting these companies in the implementation of the ISO/IEC 27000 standard, our main goal is the development of a method which provides guidance on the application of both frameworks. As a first step of this work, in this article a mapping between ISO/IEC 27002 and ISO/IEC 15504-5 is presented.

1 INTRODUCTION

Nowadays information has become a very important asset for companies and, as well as other crucial assets, it requires special protection. In fact, information should be adequately protected independently of its format and transmission mode.

The main objective of information security is to properly protect information from unauthorized access, use, disclosure, disruption, modification and destruction.

The implementation of information security controls as those defined in ISO/IEC 27002 is a priority for companies to assure its continuity, minimise possible injuries and maximize the return of investment and business opportunities.

In software development companies in particular, information security is also fundamental. Within our environment a significant number of software companies, that have been or are currently involved in a process improvement programme according to ISO/IEC 15504, demand the implementation of ISO/IEC 27000 as a security standard.

In order to guide software organizations involved in process improvement programmes according to ISO/IEC 15504 in the implementation of the ISO/IEC 27000 standard, even obtaining a certification against ISO/IEC 27001, it is necessary to look for an efficient way of applying the ISO/IEC 27002 security controls.

During the last years, several initiatives relating quality and security best practices have emerged. (Barafort, Humbert and Poggi 2006) have developed a process reference model and a process implementation model which provide a framework for assessing and increasing process capability and organisational maturity in the field information security. (Valdevit, Mayer and Barafort 2009) propose a guide for a more affordable, easier and faster way to implement a vast majority of ISO/IEC 27001 in SMEs.

The Software Process Improvement (MiProSoft) research group is experienced in implementing ISO/IEC 15504 in software companies (Mas and Amengual, 2004), (Mas and Amengual, 2005), (Amengual and Mas, 2007), (Mas, Fluxà and Amengual, 2009) and using multiple standards in a combined way (Amengual and Mas, 2003) (Mesquida, Mas, and Amengual, 2009).

With the main intention of joining forces in the combined implementation of ISO/IEC 15504 and ISO/IEC 27000, in this article the possible relation

Mas A., Mesquida A., Amengual E. and Fluxà B. (2010).
ISO/IEC 15504 BEST PRACTICES TO FACILITATE ISO/IEC 27000 IMPLEMENTATION.
In *Proceedings of the Fifth International Conference on Evaluation of Novel Approaches to Software Engineering*, pages 192-198
DOI: 10.5220/0003001001920198

between ISO/IEC 15504-5 best practices and ISO/IEC 27002 security controls is analysed.

In section 2 both standards are introduced. Section 3 defines the process followed to perform the mapping between the two standards and summarizes the results of this mapping. In section 4 a discussion about the obtained results is offered. Finally, in section 5 the conclusions are presented.

2 BACKGROUND AND OVERVIEW

In this section, both standards ISO/IEC 27000 and ISO/IEC 15504 are introduced.

2.1 ISO/IEC 27000 Series

The ISO/IEC 27000 series, also known as the "ISMS Family of Standards", comprises information security standards jointly published. The series provides best practice recommendations on information security management, risks and controls within the context of an overall Information Security Management System (ISMS). At present, six of the standards in the series are publicly available while several more are under development. In order to conduct the research presented in this paper only two standards, ISO/IEC 27001 and ISO/IEC 27002, have been used.

The *ISO/IEC 27001:2005 Information technology - Security techniques - Information security management systems - Requirements* standard (ISO/IEC, 2005a) promotes the adoption of a process approach and specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented ISMS within the context of an organization. This standard can be used in order to assess conformance by interested internal and external parties. The requirements set out in ISO/IEC 27001 are generic and are intended to be applicable to all organizations, regardless of type, size and nature. The standard is aligned with ISO 9001:2000 and ISO 14001:2004 in order to support consistent and integrated implementation and operation with related management standards. It is designed to enable an organization to align or integrate its ISMS with related management system requirements.

ISO/IEC 27002:2005 Information technology - Security techniques - Code of practice for information security management (ISO/IEC, 2005b) is the rename of the ISO/IEC 17799 standard. It establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. The control objectives and controls of this international standard provide general guidance on the commonly accepted goals of information security management. This standard may serve as a practical guideline for developing organizational security standards and effective security management practices and to help to build confidence in inter-organizational activities.

ISO/IEC 27002 contains 11 security control Clauses collectively containing a total of 39 security Categories and 133 Controls. Table 1 summarizes the structure of the standard.

Table 1: ISO/IEC 27002 Structure.

Clauses	Cate-gories	Con-trols
5 Security policy	1	2
6 Organization of information security	2	11
7 Asset management	2	5
8 Human resources security	3	9
9 Physical and environmental security	2	13
10 Communications and operations management	10	32
11 Access control	7	25
12 Information systems acquisition, development and maintenance	6	16
13 Information security incident management	2	5
14 Business continuity management	1	5
15 Compliance	3	10
Total	39	133

Each Category contains a control objective, stating what is to be achieved, and one or more controls that can be applied to achieve the control objective. Control descriptions are structured into three different fields: control, implementation guidance and other information. Table 2 shows this Category structure.

Table 2: ISO/IEC 27002 Category structure.

Category Name			
Control Objective			
Controls	(For each control of the Category)		
	Control name	Control description	
		Implementation guidance	
		Other information	

2.2 ISO/IEC 15504

ISO/IEC 15504 Information technology - Process assessment (ISO/IEC, 2004), also known as SPICE (Software Process Improvement and Capability dEtermination), is an International Standard for process assessment and improvement. It can be used by any organization to determine the current and potential capability of its own processes, and also to define areas and priorities for process improvement.

ISO/IEC 15504 is composed of seven parts that provide guidance to process assessment. In order to perform a process assessment conformant with ISO/IEC 15504-2:2003 (ISO/IEC, 2003) a Process Assessment Model (PAM), based upon a suitable Process Reference Model (PRM), needs to be properly defined.

ISO/IEC 15504-5:2006 (ISO/IEC, 2006) describes an exemplar PAM for the particular case of the software lifecycle processes defined in *ISO/IEC 12207:1995/Amd 1&2 Information technology - Software life cycle processes* (ISO/IEC, 1995). In this part the standard defines process performance indicators, also known as Base Practices (BP), for each one of the 48 software lifecycle processes which are structured in 9 Process Groups. Table 3 shows these nine Process Groups, the number of processes and the number of Base Practices per group.

Table 3: ISO/IEC 15504-5 summary of Process Groups.

Process Groups	Processes	BP
Acquisition (ACQ)	5	23
Supply (SPL)	3	25
Engineering (ENG)	12	66
Operation (OPE)	2	11
Management (MAN)	6	52
Process Improvement (PIM)	3	23
Resource & Infrastructure (RIN)	4	29
Reuse (REU)	3	26
Support (SUP)	10	73
Total	48	328

ISO/IEC 12207:1995/Amd 1&2 describes each process in terms of a Process Name, a Process Purpose and Process Outcomes. ISO/IEC 15504-5 extends this definition of a process by adding information in the form of a set of Base Practices, which provide a definition of the tasks and activities needed to accomplish the process purpose and fulfil the process outcomes, and a number of Input and Output Work Products related to the process outcomes. The complete structure of a process is shown in Table 4.

Table 4: ISO/IEC 15504-5 Process structure.

Process ID	
Process Name	
Process Purpose	
Process Outcomes	
Base Practices	
Work Products	
Inputs	Outputs

Finally, Table 5 summarises the structure of both ISO/IEC 27002 and ISO/IEC 15504-5 standards.

Table 5: Summary of the standards in quantitative terms.

ISO/IEC 27002	ISO/IEC 15504-5
Clause (11)	Process Group (9)
Category (39)	Process (48)
Control (133)	Base Practice (328)

3 MAPPING BETWEEN ISO/IEC 27002 AND ISO/IEC 15504-5

The mapping between the two standards was done by following an iterative and evolving strategy in which the ISO/IEC 27002 Controls and the ISO/IEC 15504-5 Base Practices have been compared. This version of the mapping is the result of a successive refinement process performed in three stages as shown in Figure 1.

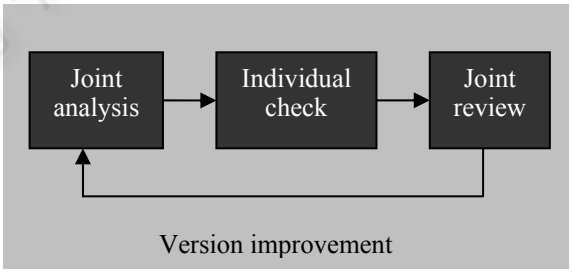

Figure 1: The mapping process flow.

With the objective of sharing the knowledge and the different points of view among the authors, during the joint analysis stage both standards were analysed in group. Since it was not possible to perform a complete mapping in only one session, different meetings were necessary in order to obtain a first preliminary version of the mapping. During each meeting two or three ISO/IEC 27002 Clauses were analysed. More specifically, taking into account that each Clause is composed of different Categories and that these Categories are composed of Controls, for each Control the Description, the

Table 6: Mapping between the ISO/IEC 27002 Clauses and the ISO/IEC 15504-5 Process Groups.

	ISO/IEC 15504-5 Process Groups								
ISO/IEC 27002 Clauses	ACQ	SPL	ENG	OPE	MAN	PIM	RIN	REU	SUP
5 Security policy					✓		✓		
6 Organization of information security	✓	✓			✓		✓		✓
7 Asset management							✓		
8 Human resources security					✓		✓		
9 Physical and environmental security							✓		
10 Communications and operations management	✓	✓	✓				✓		✓
11 Access control							✓		
12 Inf. systems acquisition, development and maintenance	✓		✓		✓		✓		✓
13 Information security incident management					✓		✓		✓
14 Business continuity management					✓		✓		
15 Compliance	✓	✓	✓			✓	✓		✓

Implementation guidance and the Other information fields were analysed in depth. It should be noted that the authors' knowledge of the ISO/IEC 15504 standard facilitated the initial selection of the set of processes related to the Control under consideration. After a detailed analysis of the Base Practices of the ISO/IEC 15504-5 selected processes, it was possible to determine the existence or not of a connection between the ISO/IEC 27002 Control and a particular ISO/IEC 15504-5 process.

With the intention of consolidating the results obtained after the meetings, these results were individually re-examined by each author to confirm the decisions reached or, on the contrary, to make some modifications to the initial version of the mapping.

Finally, during the joint review stage the individual proposals of each author were carefully discussed in order to reach a general consensus to accept or reject each proposal.

In this section due to a limitation of space the whole mapping is not included. Otherwise, a summary of the results of the mapping from different perspectives is offered to facilitate the understanding of the connections between the two standards.

Firstly, Table 6 shows a high level view of the relations between the ISO/IEC 27002 Clauses and the ISO/IEC 15504-5 Process Groups.

Secondly, at a more detailed level, Table 7 shows an extract of the mapping between the ISO/IEC 27002 Controls and the ISO/IEC 15504-5 Base Practices. More concretely, the relations between the Controls in clause 10 Communications and operations management and the Base Practices of the initially selected processes for each Control are shown. In case a Control is related to all the Base Practices of a process, the table only shows the Process Name.

Table 7: Example of mapping between the ISO/IEC 27002 security Controls and the ISO/IEC 15504-5 Base Practices.

Clause:	10 Communications and operations management
Categories:	10
Controls:	32
10.1 Operational procedures and responsibilities	
10.1.1 Documented operating procedures	SUP.7.BP1,BP7-BP8
10.1.2 Change management	SUP.10
10.1.3 Segregation of duties	RIN.4.BP2
10.1.4 Separation of development, test and operational facilities	ENG.7
10.2 Third party service delivery management	
10.2.1 Service delivery	ACQ.3.BP1,BP3
10.2.2 Monitoring and review of third party services	ACQ.4.BP3,BP4
10.2.3 Managing changes to third party services	ACQ.4.BP5 SUP.10.BP1-BP9
10.3 System planning and acceptance	
10.3.1 Capacity management	---
10.3.2 System acceptance	ACQ.5.BP3
10.4 Protection against malicious and mobile code	
10.4.1 Controls against malicious code	RIN.4.BP2
10.4.2 Controls against mobile code	RIN.4.BP2
10.5 Back-up	
10.5.1 Information back-up	SUP.8.BP10 RIN.4.BP2
10.6 Network security management	
10.6.1 Network controls	RIN.4.BP4,BP6
10.6.2 Security of network services	ACQ.3.BP1
10.7 Media handling	
10.7.1 Management of removable media	RIN.4.BP1-BP2
10.7.2 Disposal of media	---
10.7.3 Information handling procedures	RIN.4.BP2 SUP.8.BP10
10.7.4 Security of system documentation	SUP.7.BP1,BP3,BP6-BP8 RIN.4.BP2
10.8 Exchange of information	

Table 7: Example of mapping between the ISO/IEC 27002 security Controls and the ISO/IEC 15504-5 Base Practices.(Cont.)

10.8.1 Information exchange policies and procedures	RIN.4.BP1-BP2,BP4
10.8.2 Exchange agreements	ACQ.3.BP1,BP2 SPL.1.BP9-BP10 RIN.4.BP1-BP2
10.8.3 Physical media in transit	SPL.2.BP8
10.8.4 Electronic messaging	RIN.4.BP2
10.8.5 Business information systems	RIN.4.BP1-BP2,BP4
10.9 Electronic commerce services	
10.9.1 Electronic commerce	ENG.1.BP1-BP6 ENG.2.BP1-BP6 RIN.4.BP2
10.9.2 On-line transactions	ENG.1.BP1-BP6 ENG.2.BP1-BP6 RIN.4.BP2
10.9.3 Publicly available information	ENG.1.BP1-BP6 ENG.2.BP1-BP6 RIN.4.BP2
10.10 Monitoring	
10.10.1 Audit logging	RIN.4.BP2,BP4
10.10.2 Monitoring system use	RIN.4.BP2,BP4,BP6
10.10.3 Protection of log information	---
10.10.4 Administrator and operator logs	---
10.10.5 Fault logging	---
10.10.6 Clock synchronization	---

Finally, starting from the ISO/IEC 15504 another point of view of the mapping can be obtained. As an example, Table 8 shows all the ISO/IEC 27002 Categories related to the processes of the ISO/IEC 15504-5 Management Process Group (MAN).

Table 8: Example of the mapping between the ISO/IEC 15504-5 Processes and the ISO/IEC 27002 Categories.

ISO/IEC 15504 Process	ISO/IEC 27002 Category
MAN.1 Organizational alignment	5.1 Information security policy
	8.1 Prior to employment
	8.2 During employment
MAN.2 Organizational management	6.1 Internal organization
	14.1 Information security aspects of business continuity management
MAN.3 Project management	---
MAN.4 Quality management	---
MAN.5 Risk management	6.2 External parties
	12.6 Technical Vulnerability Management
	13.1 Reporting information security events and weaknesses
	13.2 Management of information security incidents and improvements
MAN.6 Measurement	---

4 RESULTS AND DISCUSSION

In this section the results of the mapping between ISO/IEC 15504 and ISO/IEC 27002 are analysed and the different types of relations between the Base Practices and Controls are exposed.

4.1 Analysis of the Relations

Table 6, presented in the previous section, can be analysed from two different points of view. On the one hand, an analysis by columns gives information about the relations from the perspective of ISO/IEC 15504 Process Groups. On the other hand, an analysis by rows determines the relations from the perspective of ISO/IEC 27002 Controls.

Beginning with an analysis of Table 6 by columns, it can be seen that the Resource and Infrastructure Process Group (RIN) is the only Process Group that is related to all ISO/IEC 27002 Clauses. This Process Group consists of processes performed in order to provide adequate human resources and the necessary infrastructure as required by any other process. Not surprisingly, the relations established between this Process Group and the ISO/IEC 270002 Clauses are quite evident.

On the contrary, the Operation Process Group (OPE), the Process Improvement Group (PIM) and the Reuse Process Group (REU) have a weak or non-existent connection with any clause in ISO/IEC 27002.

The OPE Process Group contains Base Practices for the correct operation and use of the software product and/or service. Consequently, it is hardly surprising that no relation with the ISO/IEC 27002 standard has been found.

The PIM Process Group consists of processes performed in order to define, deploy, assess and improve the processes performed in the organizational unit. These kinds of aspects are not considered specifically in the ISO/IEC 27002 standard. They are related to the ISO/IEC 27001 standard, more concretely to the proposed PDCA process model which is applied to structure all ISMS processes.

The purpose of the REU processes is to manage the life of reusable assets and to plan, establish, manage, control, and monitor an organization's reuse program to systematically exploit reuse opportunities. These activities are better related to the ISO/IEC 27001 standard than to ISO/IEC 27002. That is the reason why no evidences of REU Base Practices in ISO/IEC 27002 Controls have been identified.

Finally, analysing Table 6 from the perspective of the ISO/IEC 27002 Clauses, it can be observed that the "Asset management", "Physical and environmental security" and "Access control" Clauses have only weak connections with the RIN Process Group. Moreover, "Security policy", "Human resources security" and "Business continuity management" are only related to the MAN and RIN Process Groups.

4.2 Types of Correspondence

From the analysis of the relations between ISO/IEC 27002 Controls and ISO/IEC 15504-5 Base practices, five different types of correspondence between both standards have been established:

1. **Correspondence between a Control and the Whole Set of the Base Practices of a Process.**

The connection between the "10.1.2 Change Management" Control and the Base Practices of the "SUP.10 Change request management" process can be considered an example of this particular case. Although this set of Base Practices is performed in order to ensure that changes to products in development are managed and controlled, the same set of Base Practices could be performed in order to manage changes to information processing facilities in the manner indicated by the Control.

Another example of this case can be observed in the connection between the "10.1.1 Documented operating procedures" Control and the "SUP.7 Documentation" process.

2. **Correspondence between the Control and Part of the Set of the Base Practices of a Process.**

This is the case of the "10.5.1 Information back-up" Control which is clearly related to SUP.8.BP10 and RIN.4.BP2.

The description of this Control states that back-up copies of information and software should be taken and tested regularly in accordance with the agreed backup policy.

This description fits with SUP.8.BP10 description: Manage the backup, storage, archiving, handling and delivery of configured items. Ensure the integrity and consistency of configured items through appropriate scheduling and resourcing of backup, storage and archiving. Control the handling and delivery of configured items.

Likewise, the Control description also fits with RIN.4.BP2 description: Define the infrastructure requirements to support the performance of appropriate processes. Infrastructure process requirements may include: security, throughput and data sharing requirements, backup and recovery, remote access facility, physical workspace and equipment, user support requirements and maintenance requirements.

3. **Correspondence between a Control and a Process.**

In this case there is a correspondence between a Control and a process without an explicit connection with a particular Base Practice of the process. The relation has been identified by comparing the control description with the process purpose.

This is the case of the "10.7.4 Security of system documentation" Control with the "SUP.7 Documentation" process. The description of this Control states that system documentation should be protected against unauthorized access and the purpose of SUP.7 is to develop and maintain the recorded information produced by a process.

In this case, in order to include the security aspects considered by the Control in the related process two possible solutions could be undertaken. On the one hand, a new Base Practice could be added to the process in order to satisfy the Control objective. The description of this new Base Practice could be adapted from the Control implementation guidance. On the other hand, the description of the existent Base Practices and the process purpose could be modified or expanded.

For the particular of case of SUP.7, SUP.7.BP1, SUP.7.BP3, SUP.7.BP6, SUP.7.BP7 and SUP.7.BP8 should be expanded in order to meet the Control objective. Moreover, the process purpose could also be changed to "to develop, maintain and protect against unauthorized access the recorded information produced by a process".

4. **Nonexistence of a Correspondence between a Control and a Process.**

This is the case of controls "10.10.4 Administrator and operator logs", "10.10.5 Fault logging" and "10.10.6 Clock synchronization".

Because of its particular nature, these controls are related to system administration activities which are not covered by ISO/IEC 15504-5.

5. **Correspondence between a Control and RIN.4 Infrastructure Process.**

In this case, a Control is only related to the RIN.4 Infrastructure process which purpose is to maintain a stable and reliable infrastructure that is needed to support the performance of any other process. The RIN.4 Base Practices most frequently connected are RIN.4.BP2 and RIN.4.BP4.

An example of this case can be observed in the first Control of the Category 10.10 Monitoring, "10.10.1 Audit logging", which objective is to

produce and keep audit logs recording user activities, exceptions and information security events. If this objective is understood as a security infrastructure requirement, the Control should be related to RIN.4.BP2 and RIN.4.BP4. A similar case could be found in the "10.10.2 Monitoring system use" Control.

5 CONCLUSIONS

In this article, a mapping between the ISO/IEC 27002 security Controls and the ISO/IEC 15504-5 Base Practices for software lifecycle processes has been presented.

As it has been proved, ISO/IEC 15504 considers an important number of the security aspects and controls which are necessary for the implementation of an Information Security Management System. Consequently, software companies involved in a process improvement program according to this standard have already performed some steps in order to implement the ISO/IEC 27000 Standard.

After demonstrating the relations between these two different standards, further work is expected to be performed in order to meet the following goals:

- Development of a method with the necessary guidelines for the implementation of both standards reducing the amount of effort.
- Improvement of this method by considering the lessons learned from its application in software companies.
- Analysis of the relations between the ISO/IEC 27002 Security controls and the Generic Practices of Capability levels 2-5 provided by ISO/IEC 15504-5 to determine if the implementation of security controls could help process improvement in a company.
- Development of a software tool to support the implementation of both standards.

ACKNOWLEDGEMENTS

This research has been supported by CICYT TIN2007-67843 - TIN2007-67843-C06-04 "Modelos de simulación basados en ontologías y mejora de procesos para arquitecturas orientadas a servicios", SOAQSim.

REFERENCES

Amengual, E. and Mas, A. (2003). A New Method of ISO/IEC TR 15504 and ISO 9001:2000 Simultaneous Application on Software SMEs. In *SPICE 2003, Joint ESA - 3rd International SPICE Conference on Process Assessment and Improvement*. (pp. 87-92). Noordwijk, the Netherlands.

Amengual, E. and Mas, A. (2007). Software Process Improvement in Small Companies: An Experience. In *Proceedings of the EuroSPI 2007*. Potsdam, Germany, September 2007.

Barafort, B., Humbet, J-P., Poggi, S., 2006. Information Security Management and ISO/IEC 15504: the link opportunity between Security and Quality. In *SPICE 2006, International SPICE Conference on Process Assessment and Improvement*. Luxembourg.

ISO/IEC. (1995). ISO/IEC 12207:1995 Information technology - Software life cycle processes. Amd 1:2002. Amd 2:2004.

ISO/IEC. (2003). ISO/IEC 15504-2:2004 Software Engineering - Process Assessment - Part 2: Performing an assessment.

ISO/IEC. (2004). ISO/IEC 15504-1:2004 Information Technology - Process Assessment - Part 1: Concepts and Vocabulary.

ISO/IEC. (2005a). ISO/IEC 27001: Information technology - Security techniques - Information security management systems - Requirements.

ISO/IEC. (2005b). ISO/IEC 27002: Information technology - Security techniques - Code of practice for information security management.

ISO/IEC. (2006). ISO/IEC 15504-5: Information technology - Software Process Assessment - Part 5: An exemplar process assessment model.

Mas, A. and Amengual, E. (2004). A Method for the Implementation of a Quality Management System in Software SMEs. In *Proceedings of the Twelfth International Conference on Software Quality Management*. British Computer Society, pp. 61-74, March 2004.

Mas, A. and Amengual, E. (2005). La mejora de los procesos de software en las pequeñas y medianas empresas (pyme). Un nuevo modelo y su aplicación en un caso real. In *Revista Española de Innovación, Calidad e Ingeniería del Software (REICIS)*. Vol. 1, no. 2, pp. 7-29, December 2005.

Mas, A., Fluxà, B. and Amengual, E. (2009). Lessons learned from an ISO/IEC 15504 SPI Programme in a Company. In *Proceedings of the EuroSPI 2009*. Alcalá de Henares, Spain, September 2009.

Mesquida, A. L., Mas, A. and Amengual, E. (2009). La madurez de los servicios TI. In *Revista Española de Innovación, Calidad e Ingeniería del Software (REICIS)*. Vol. 5, nº 2, pp. 77-87, September 2009.

Valdevi, T., Mayer, N., Barafort, B., 2009. Tailoring 27001 for SMEs: A Guide to Implement an Information Security Management System in Small Settings. In *Proceedings of the EuroSPI 2009*, *CCIS* 42, pp. 201-212. Springer-Verlag Berlin Heidelberg.