WOSIS 2006

Eduardo Fernández-Medina and
Mariemma I. Yagüe (Eds.)

Security in Information Systems

Proceedings of the
4th International Workshop on
Security in Information Systems - WOSIS 2006
In conjunction with ICEIS 2006
Cyprus, Paphos, May 2006

INSTICC Press

Eduardo Fernández-Medina and
Mariemma I. Yagüe (Eds.)

Security in Information Systems

**Proceedings of the
4th International Workshop on
Security in Information Systems,
WOSIS 2006**
In conjunction with ICEIS 2006
Paphos, Cyprus, May 2006

INSTICC PRESS
Portugal

Volume Editors

Eduardo Fernández-Medina
University of Castilla-La Mancha
Spain

and

Mariemma I. Yagüe
University of Málaga
Spain

4th International Workshop on
Security in Information Systems – (WOSIS 2006)
Paphos, Cyprus, May 2006
Eduardo Fernández-Medina and
Mariemma I. Yagüe (Eds.)

Printed in Portugal

ISBN: 972-8865-52-X
ISBN (13 digits): 978-972-8865-52-8
Depósito Legal: 241848/06

Foreword

Every year, WOSIS gather researchers and practitioners of Information Systems Security and gives them the opportunity to present the most recent advances in theory and practice in security for Information Systems, as well as the risks related to simplistic developments of security for information systems.

The Fourth International Workshop on Security in Information Systems received 54 submissions. All of them were reviewed by at least three program committee members or other experts at their organizations which acted as additional reviewers. Finally 25 papers were accepted; unfortunately, some excellent papers had to be rejected because they did not correspond to WOSIS'06 scope.

The Workshop is primarily interested in high quality, innovative and unpublished research. In this edition, a selection of the best works was done in order to include extended and revised versions of these papers in the prestigious Internet Research Journal. We especially want to thank to Dr. David Schwartz for his outstanding support throughout the whole process.

In this edition, Dr. Leonardo Chiariglione has honored us with his great experience offering the keynote speech of WOSIS 2006. We want to acknowledge his contribution and amiability. This fact has increased the quality of the technical program which we hope you find motivating.

It is also our pleasure to thank the members of the program committee and the additional reviewers for the work well-done. We also want to give our sincerest thanks to the members of the organisation committee for their hard work and support.

We gratefully acknowledge all the authors who submitted papers to WOSIS'06 for their efforts and we hope to receive new contributions for future editions of WOSIS.

To conclude, on behalf of the Organizing Committee we sincerely hope that you enjoy not only the workshop technical program, but also the beautiful and relaxing scenery of Paphos.

May 2006

Eduardo Fernández Medina
Mariemma I. Yagüe

Workshop Chairs

Eduardo Fernández-Medina
University of Castilla-La Mancha
Spain

and

Mariemma I. Yagüe
University of Málaga
Spain

Program Committee

Sabrina De Capitani di Vimercati, Università degli Studi di Milano, Italy
Ernesto Damiani, Università degli Studi di Milano, Italy
Csilla Farkas, University of South Carolina, USA
Eduardo B. Fernández, Florida Atlantic University, USA
Mariagrazia Fugini, Politecnico di Milano, Italy
Steven Furnell, University of Plymouth, UK
Christian Geuer-Pollmann, European Microsoft Innovation Center, Germany
Paolo Giorgini, University of Trento, Italy
Ehud Gudes, Ben-Gurion Univerity, Israel
Javier López, University of Málaga, Spain
Haralambos Mouratidis, University of East London, Dagenham, England
Sushil Jajodia, George Mason University, USA
Willem Jonker, University of Twente, The Netherlands
Jan Jürjens, TU Munich, Germany
Ravi Mukkamala, Old Dominion University, USA
Martin Olivier, University of Pretoria, South Africa
Sylvia Osborn, University of Western Ontario, Canada
Brajendra Panda, University of Arkansas, USA
Günther Pernul, University of Regensburg, Germany
Mario Piattini, University of Castilla-La Mancha, Spain
Indrajit Ray, Colorado State University, USA
Indrakshi Ray, Colorado State University, USA
Robert Tolksdorf, Freie Universität Berlin, Germany
Ambrosio Toval, University of Murcia, Spain
Duminda Wijesekera, University George Mason, USA

Auxiliary Reviewers

Carlos Gutiérrez, STL, Spain
Joaquín Lasheras, University of Murcia, Spain
Francisco Javier Lucas, University of Murcia, Spain
Vasilis Katos, Portsmouth University, UK
Miguel Ángel Martínez, University of Murcia, Spain
Fernando Molina, University of Murcia, Spain
Antonio Muñoz, University of Málaga, Spain
Damien Sauveron, University of Limoges, France
Daniel Serrano, University of Málaga, Spain
Rodolfo Villarroel, University "Católica del Maule", Chile

Table of Contents

Papers

An Audit Method of Personal Data Based on Requirements Engineering[1]

Miguel A. Martínez[1], Joaquín Lasheras[1], Ambrosio Toval[1], Mario Piattini[2]

[1] Grupo de Investigación de Ingeniería del Software. Dep. Informática y Sistemas.
University of Murcia. Campus de Espinardo. 30071. Murcia. Spain.
{mmart, jolave, atoval}@um.es
[2] ALARCOS Research Group. Information Systems and Technologies Department.
UCLM-Soluziona Research and Development Institute. University of Castilla-La Mancha.
Paseo de la Universidad, 4 - 13071. Ciudad Real. Spain.
{Mario.Piattini}@uclm.es

Abstract. Security analysis of computer systems studies the vulnerabilities that affect an organization from various points of view. In recent years, a growing interest in guaranteeing that the organization makes a suitable use of personal data has been identified. Furthermore, the privacy of personal data is regulated by the Law and is considered important in a number of Quality Standards. This paper presents a practical proposal to make a systematic audit of personal data protection - within the framework of CobiT audit - based on SIREN. SIREN is a method of Requirements Engineering based on standards of this discipline and requirements reuse. The requirements predefined in the SIREN catalog of Personal Data Protection (PDP), along with a method of data protection audit, based on the use of this catalog, can provide organizations with a guarantee of ensuring the privacy and the good use of personal data. The audit method proposed in this paper has been validated following the Action Research method, in a case study of a medical center, which has a high level of protection in the personal data that it handles.

1 Introduction

Information Systems (IS) audit has become increasingly more common in recent years, in order to analyze and to evaluate the planning, control, effectiveness, security, economy and adjustment of the computer infrastructure of the company.

A security audit according to ISO 7498-2:1989 (Information Processing Systems - Open Systems Interconnection - Basic Reference Model) is: "An independent review and examination of system records and operations in order to test for adequacy of

[1] Partially financed by the Spanish Ministry of Science and Technology, project PRESSURE (PREcise Software modelS and reqUirements ReusE), TIC2003-07804-C05-05 and by the Junta de Castilla-La Mancha (Spain), project DESERT (DEveloping Secure systEms through Requirements and Tools), PBC-05-012-3, and the the RETISTIC network (TIC2002-12487-E) financed by the "Dirección General de Investigación" of the Spanish Ministry of Science and Education.

system controls, to ensure compliance with established policy and operational procedures, to detect breaches in security, and to recommend any indicated changes in control, policy, and procedures".

A security audit can include many aspects, such as the level of protection of the facilities or the people. In this paper, however, we focus on the security related to data and information (privacy) of a personal nature, within the framework of the Spanish Personal Data Privacy Law [32, 33], which is an adaptation of the EU Legislation [8]. This law has been similarly adapted by other European countries, for example in Italy the law that regulates the personal data protection is the *Italian Law No. 196*, of 30th June 2003 [18], and in the UK, it is the *Data Protection Act* of 24th October 1998 [4]. In the US, the approach is "sectorial" and has as source a mixture of legislation, regulation and self-regulation. Privacy rights of information have been granted in a variety of sectorial laws, as for example, *The Privacy Act* of 1974, the *Fair Credit Reporting Act* of 1970, or the *Electronic Communications Privacy Act* of 1986. In the US, there is no national authority of data protection. The Department of Commerce of the USA (Federal Trade Commission [12]) is in charge of regulating personal data transfer from the European Union to the US.

Within the scope of the electronic communications, privacy is defined as the right to keep our personal data and communications secret [19]. At the moment, even in existing laws that regulate this aspect, we found a serious threat to privacy, which is why it is important to confront this problem.

Another aspect that emphasizes the importance of the treatment of the privacy of information, and therefore the legal requirements and the audit process implied, is that these requirements are considered important in Quality Standards like ISO 9001:2000 (Quality Management Systems - Requirements). Specifically, in ISO 9004:2000 (Quality Management Systems - Guidelines for performance improvements), section 5.2.3 "Statutory and Regulatory Requirements" appears: "*Management should ensure that the organization has knowledge of the statutory and regulatory requirements that apply to its products, processes and activities and should include such requirements as part of the quality management system*". In particular, and very recently, the US National Science Foundation-dependent Computing Research Association (CRA, www.cra.org) determined that the security of IS and the privacy of the end-users constitute one of the four biggest global security-related challenges [25].

The audit method presented in this paper is based on SIREN (SImple REuse of software requiremeNts), a general method of Requirements Engineering [29]. The requirements management process is obligatory for organizations which seek to reach levels 2 and 3 in CMMI [6]. SIREN is a practical approach to select and specify the requirements of a software system based on requirements reuse and software engineering standards [15, 16]. SIREN encompasses a spiral process model, requirements document templates and a reusable requirements repository, which is organized by catalogs. Currently, the only SIREN catalog related with privacy aspects is the personal data protection one (PDP) [30].

Several studies [5] emphasize the benefits of considering security in the early phases of the system development (in particular, phase of requirements specification of the system). In issues specifically related to personal data protection, the inclusion of these requirements from the first stages of the system life cycle means that the systems are developed according to the requirements of the law from the beginning, and not as a later addition. Thus security and productivity are improved. Likewise, the reuse of these requirements helps to increase quality by detecting and correcting errors of inconsistency and ambiguity and favoring later use in new projects [29].

We present an approach for making an audit of data protection based on the use of a reusable requirements catalog of data protection [30] developed according to SIREN. This research arises from the experience acquired after applying this audit method of personal data protection at a medical center using the Action Research methodology [2].

Our IS audit proposal, has a direct correspondence with the CobiT Framework (Control Objectives for Information Technologies), in its latest version (2005) [7], which is widely accepted by the international community of IS auditors and CIOs.

This proposal is expected to help fulfil those CobiT control objectives that deal with issues of privacy, since the use of the SIREN PDP requirements catalog facilitates identification and verification of the fulfilment of the requirements related to these aspects.

The paper is structured as follows: in Section 2 the CobiT Framework is explained briefly. In Section 3, the audit method proposed is described, including a section where the SIREN method is described briefly, together with the improvements made to the personal data protection requirements catalog. In Section 4, the phase of practical application of our study case is described. In Section 5, some related works are presented and compared to our proposal. Finally Section 6 shows the conclusions, indicating the lessons learned after this application, and some further work.

2 CobiT Framework

The principal objective of the CobiT project [7] is the development of clear policies and good practices for the security and the control of Information Technologies (IT), with the purpose of obtaining worldwide approval and support of commercial, governmental and professional organizations. CobiT has been developed by the ISACA [17], the most important professional association for the regulation of the practice of the computer audit in the world. CobiT is designed to be used by three types of different users: Management, Users and Auditors. CobiT can be seen as a "bucket" of 3 dimensions: Business Requirements, IT Resources and IT Processes. Fig.1 shows this bucket where the parts related to our work are shaded.

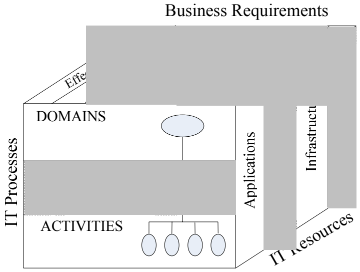

Fig. 1. The CobiT Cube (CobiT 4.0).

The proposed methodology in this audit work follows the same structure and processes proposed in CobiT, since we offer requirements documents with direct correspondence with CobiT Control Objectives that will help the accomplishment of the audit and also a procedure to follow, which is compatible with the CobiT process. Our main contribution is the use of a PDP requirements catalog, elaborated according to the method of Requirements Engineering SIREN. It helps to specify the requirements corresponding to the control objectives related to legal aspects of Personal Data Protection and also helps in the later verification of its fulfilment.

Corresponding to each of the 34 high level control objectives defined in CobiT, there exists an audit guide that allows the checking of the IT processes against the 214 detailed control objectives recommended by CobiT and thus provides the Management with confirmation of its fulfilment and/or suggestions for its improvement.

Some correspondences between the CobiT Control Objectives and the requirements of our SIREN PDP catalog are the following (examples of requirements can be seen in section 4.2):

- The Control Objective DS 5.3. *Identity Management*, is audited by verifying the fulfilment of requirements SyRSL13, SyRSL14, SyRSL15, SyRSL16, SyRSL17, SyRSL18, SyRSL19, SyRSL20, SRSL4, SRSL6 and SRSL9.
- The Control Objective PO 2.3. *Data Classification Scheme*, is audited by verifying the fulfilment of requirements SyRSL8, SyRSL21, SyRSL36, SyRSL49, SyRSL55, SyRSL80, SyRSL81 and SyRSL82.
- The Control Objective DS 11.5. *Backup and restoration*, is audited by verifying the fulfilment of requirements SyRSL25, SyRSL26, SyRSL27, SyRSL28, SyRSL29, SyRSL30, SyRSL31, SyRSL32, SyRSL33, SyRSL34, and SyRSL35.
- The Control Objectives related to the *data encoding* (DS 5.3, DS 5.8, DS 5.11), are audited verifying the fulfilment of requirements SRSL3, SRSL8 and SRSL11.

3 Audit Method of Personal Data Based on Requirements Engineering

In this section we present a practical method to perform an audit of personal data on an IS. This method is an extension of a general audit process, based on CobiT, with the use of a requirements SIREN catalog of Personal Data Protection. In the following two sections we show how a method of Requirements Engineering based on reusability, as SIREN, contributes to improving the audit process (section 3.1) and to defining the explicit phases to carry out this personal data audit (section 3.2).

3.1 SIREN: a Method of Requirements Engineering

Starting from a set of requirements which have been specified for other projects or domains, we can improve the precision and efficiency of the requirements specification for the current project and we can also reduce the time to elaborate this specification. In order to explore the benefits of requirements reuse, our group has proposed SIREN (SImple REuse of software requiremeNts) [30] as a practical way to deal with requirements reuse. Specifically, we distinguish in SIREN a double process model:

- SIRENc, which considers pre-existing catalogs of reusable requirements in a repository and obtains the requirements specification of the current project from them.
- SIRENp, which is the necessary process model for the creation of these requirements catalogs, i.e. the reusable products.

SIREN requirements catalogs contain reusability requirements organized within a hierarchy of requirements specification documents which is structured according to IEEE standards [15, 16]. One of the catalogs related to this proposal is the PDP catalog [30].

In SIREN, each requirement has a minimal and common set of attributes (i.e. source, state, etc.). Additional attributes can be defined depending on the type of the requirement. Requirements are organized in the catalogs by means of types. For example, the types SRSP and SYRSP refer -respectively- to the PDP requirements contained in the SRS (Software Requirements Specification) and SyRS (System Requirements Specification) documents that correspond to the PDP catalog.

Additionally, other two requirements documents exist in the PDP catalog: the Software Test Specification (STS) document and the System Test Specification (SyTS) document.

In order to be able to validate the requirements, these must be quantified in the SyRS and the SRS. In test specification documents (SyTS or STS) testing criteria will be specified to ensure that the system or software fulfils the requirements specified.

This way, for each one of the requirements identified in the SyRS is necessary also to specify how that requirement can be checked, by means of a textual description of the process to follow. We think that the SyTS could be very useful in the PDP catalog because the privacy policy of the organization can be defined directly from the SyTS. This policy will include a list of questions related to the data protection, which could be easily checked. The role of the STS document is to define when a requirement included in the SRS is fulfilled. This document helps to study if the requirements are fulfilled with the purpose of taking the measures to correct them and/or to verify its degree of fulfilment.

One of the common attributes is the exclusive traceability relationship, which means that the requirements involved in the relationships are mutually alternative. In SIREN we also have parameterized requirements, which contain some parts that have to be adapted to each application or system and have to be instantiated when it is reused.

The Personal Data Protection Requirements Catalog

The PDP catalog is compatible with PDP Spanish legislation, namely the Constitutional Law 15/1999, (LOPD) [27], the Security Measures Regulations of Automated Files which contain personal data (RMS) [28], Directive 1995/46/CE [8], Regulation 45/2001/CE [22] and Directive 2002/58/CE [9].

The LOPD seeks to gather the requirements for an IS to guarantee protection in issues relating to the handling of personal data, civil rights and the fundamental rights of the individual, and especially those relating to individuals' honor and personal privacy. On the other hand, the RMS seeks to determine the measures of a technical and organizational kind that guarantee the confidentiality and integrity of information in order to preserve honor, personal and familial privacy and the full exercising of personal rights against any alteration, loss, handling or non authorized access.

Any IS that incorporates the requirements defined in this catalog will be able to successfully meet the demands of the Spanish Legislation [32, 33] as regards the processing of personal data, and in accordance with the level of protection demanded. In the same way, this is applicable to any member state of the EU, since a shared base [8, 9 and 26] for the development of its own laws is established.

Therefore, the application of the PDP catalog for a personal data audit on a certain organization is simple, because it is sufficient to verify that the audited organization fulfils one by one the requirements established in the PDP catalog.

The PDP catalog proposed in this work, is more powerful than traditional checklists used to perform audits, since the information associated in form of attribute to each requirement, provides to the auditor a more complete guide to carry out the audit. In addition, thanks to the reusability, the catalog can be updated and revised in a continuous way. Furthermore, by means of, traceability, requirements with a dependency relationship can be easily tracked.

Additionally to the presented advantages of the use of PDP catalog for an auditor, a requirements engineer who has to develop a software system that must fulfil privacy legal requirements, will also take advantage of it, because of having gathered, in an understandable language for him, those requirements imposed in the different laws which regulate this matter, normally in more legal terms.

The sources used to write the present requirements of the PDP catalog, in addition to the directives mentioned, LOPD and RMS, were the directives and regulations of communitarian right related to electronic communication and data processing [9, 22], and CobiT [7].

Another aspect that improves the catalog is the handling of exceptional cases, which occur with some frequency in texts of a legislative nature. These exceptions are reflected in the attribute exception, associated to each of the requirements of the catalog, to ensure that the catalog is complete and self-sufficient.

The PDP catalog used for the audit presented in this work is currently composed of 150 requirements, and has 75 traceability relationships between the requirements defined. The requirements of the catalog, in addition to the text itself, have associated self-information (attributes with information on each requirement) which enriches the requirement. At the moment there are 18 attributes defined, among which stand out: *source*, *exceptions*, *security level*, *motivation* and *fulfilment*.

3.2 Phases of the Audit Method

The personal data audit method proposed in this paper consists of the phases described in Fig 2. The phases are detailed as follows:

Phase 1.- *Previous analysis of the company's situation.*

This consists of an initial interview in which it will be necessary to specify the reach of the audit in order to draw up an initial budget. The aim is to obtain all types of information on the handling of the data that the company uses.

Phase 2.- *Activities of the audit.*

- **Activity 2.1.-** *Requirements verification with initial questionnaires (checklists).* After various interviews with personnel of the organization, the auditor fills out initial questionnaires (checklists) with questions related to security, with emphasis on aspects of personal data protection. The auditor weighs up the value of the answers, and draws his own conclusions.
- **Activity 2.2.-** *Requirements verification with SIREN PDP catalog*. The auditor will make verifications in the system of the audited organization to verify the fulfilment or non fulfilment of the requirements contained in the catalog. These verifications will be made with the support of the personnel responsible for the organization, who, as far as possible, facilitate the task of the auditor. This verification is simple, because it is sufficient to choose those requirements of catalog that are of application in the audited organization and to verify one by one if they are fulfilled or not in the IS of this organization. For example, if a high level of protection is demanded of an organization in its data, the auditor will extract from the catalog those requirements necessary to reach this level of protection and will verify if these requirements are present in the organization. This extraction or filtrate of requirements of the catalog is possible thanks to the use of the self-information that a requirement has associated, in this case through the attribute *security level.*

Phase 3.- *Fulfilment tests.*

In this phase it has to be proved if the system is working as expected. The risk that exists to the organization if some of the evaluated measures are not fulfilled also has to be checked. To carry out the tests, the SyTS and STS documents of the SIREN PDP catalog will be used, which offers the advantage that any person (just incorporated or inexperience), could make the tests in a simple and systematic way. For example, for a requirement of the SyRS which specifies the system performance when it is performing a concrete operation, the test requirement, included in the SyTS document, that check it, has the following textual description: "the person in charge of security of the organization will execute [Number of applications simultaneously] in [Number of computers], and will observe the behaviour of the system, measuring the used time to execute all these applications".

Phase 4.- *Preparation and writing of the final report.*

The function of the audit will be exclusively in writing. Therefore, the writing of the report must be the final item, as a result of the evaluation made.

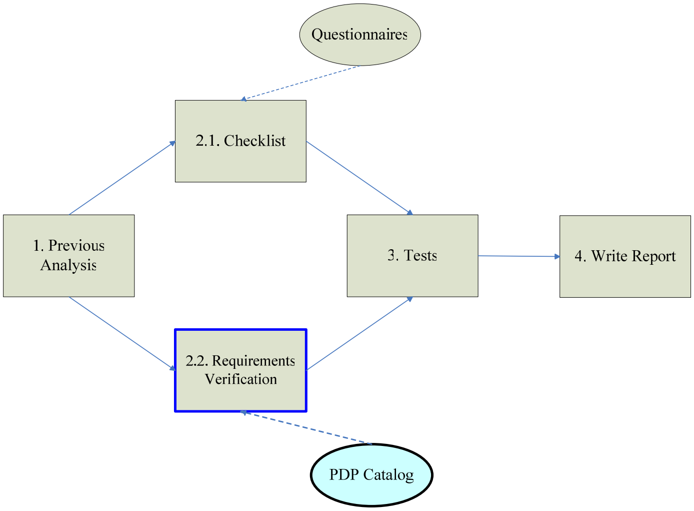

Fig. 2. Phases of the Audit Method of Personal Data.

The main contribution of this paper to a common audit method is centred in Activity 2.2, where a verification of the systems of the audited organization is made, based on reusability requirements SIREN PDP catalog [30]. Our correspondence with the CobiT Framework is determined by the following:

- Catalog SIREN (document of requirements) is compatible with CobiT documents.
- Process SIREN is compatible with the process defined in CobiT.
- Catalog SIREN includes requirements extracted from the LOPD (related to CobiT control objectives) and others directly take out from CobiT, among other sources.

4 Practical Application of the Audit Method of Personal Data Based on Requirements Engineering

The results shown in this work have been validated in a real practical case used to define a generic personal data audit method. The use of our catalog in the personal data audit method has been put into practice in an organization with 60 employers approximately, within the health sector (a clinic), which is subject to a high level of protection, according to the RMS. For the sake of confidentiality, the name of the organization is not included. For the design of this study case we have decided to use a qualitative investigation method in software engineering, called Action Research (AR) [2], which is explained below.

4.1 Design of the Study Case

The application of AR implies a cyclical process where the different parts implied participate in the investigation, which examines the existing situation (considered problematic) with the aim of changing and improving it. AR is one of the few valid approaches for studying the effects of specific alterations in development and maintenance methodologies of systems in human organizations [3].

Using the terminology of AR the following roles and participants have been considered in this study case:

- The ‘researcher’ is the Software Engineering Research Group of the University of Murcia.
- The ‘object under research’ is the application of the PDP catalog in an audit process in a health sector organization with a high level of protection in the files of personal data it handles.
- The ‘critical reference group’ (CRG), in other words, the one for which the research is made because it has a problem that needs to be solved. This group is formed by the members of the audited organization, which in this case is the medical center. According to AR, the CRG also has to participate in the research process, although in a less active way than the researcher.
- The ‘stakeholders’ are organizations who can obtain benefits from the results of the research, in particular, the members themselves of the CRG and, in general, other organizations whose activity is similar to that of the audited organization.

In this research, a participative application of AR has been made, in which the CRG puts into practice the recommendations made by the researcher, and shares its effects and results.

4.2 Practical Application of the Audit Method

The organization object of the study has offered, since 1988, all health care services, including therapeutic and diagnosis surgery related to different medical specialties, in response to demands of the more than 5000 patients who visit its facilities monthly (according to data collected from the personnel of the organization). This organization has held the certificate of quality according to standard UNE-EN-ISO 9001:2000, for all the clinic's activities (consultancy and medical clinic) and for all the areas (commercial, marketing, management, etc.), since May of 2004.

Once the information obtained from the personnel of the audited organization, through the different interviews made in Phase 1 of the audit has been analysed, Phase 2 can be completed, using two work tools:

- Questionnaires. After the interview to fill out these, and a weighting of the answers, we conclude that the organization has, at first sight, an acceptable level of security. We can not be more precise at the moment because this is a subjective point of view. With the next activity we will be able to be more objective.
- SIREN Personal Data Protection Catalog. In order to carry out this activity, a meeting with the personnel was held, where fulfilment, or non fulfilment, of the requirements of the SIREN PDP catalog was reviewed individually.

The results obtained after this verification were satisfactory for both parts (audited Organization/Research Group), with a 61% fulfilment of the requirements contained in the catalog relative to organizations of high level of security LOPD/RMS.

Some examples of the fulfilment or non fulfilment of the requirements of the catalog in the system of the audited organization are the following:

Requirement 61. *High level of security*: The backup copies and procedures of data recovery will be conserved in a different place from that of the computer equipment that handles them.

Not fulfilled. The backups are conserved in a hard non-flammable box that is in the same location as the computer systems.

Requirement 62. *High level of security*: The transmission of data of a personal nature through telecommunications networks will be made by encoding these data or using any other mechanism that guarantees that the information is neither intelligible to nor manipulated by third parties.

Fulfilled. This is done by means of connections encoded through Lotus Notes clients or Remote control software (Remote Administrator).

Once the two first stages of the audit method have been completed, the appropriate tests to verify the operation of the system were made. Finally, the Final Report was written as result of the evaluation made.

Lastly, and after the audit, the organization will implant the solutions and proposed security measures in our audit. It is important to emphasize that the implantation of such measures is not part of the audit method, since a basic principle of the audits, is that these finish with conclusions and possible solutions, but never implement solutions themselves.

To complete the implantation of the proposed security measures after a personal data protection audit, the following activities have to be performed:

- Declaration of files to the Data Protection Agency [26], which is the Spanish institution that oversees the fulfilment of the legislation about data protection and controls its application.
- Elaboration of the security document, which is a document that must be implanted by the person in charge of the file in which the security norm is reflected.

In this case, the audited organization is equipped with the measures required by law, as regards security and personal data protection, except for small deficiencies found, and these are the only ones that the system administrators of the organization will try to correct. In the same way, the obligatory security document for an organization which has a high level of protection is already written up suitably, so the measures to implant in the Medical Center are minimum.

Requirements not fulfilled in the audited system, as well as several problems that put the security of the system at risk, have been detected:

- After classifying the different files and reviewing the current declaration of the files with personal data, a deficiency in the procedure has been detected, since there exist data (profession, situation...) gathered through the computer application of the medical center, which have not been reflected in the files registered in the Data Protection Agency.
- After analyzing all the contracts by which the company can transfer personal data or communicate them for management by third parties, we have found a

deficiency, because it is not reflected in the security document that the data can be transferred or be communicated to third parties. This information would have to be reflected in a visible form.

- After obtaining and reviewing the file with the list of users with access to personal data and their level of access, some incidences of security have been detected, since some users have authorization to access all the files of the company, when according to their position in the organization they should not.

Another aspect to consider in this study case is the biennial audit that has to be made to fulfil the Security Measures Regulation. This audit was made in June of 2004 in the audited organization, with the next one in 2006. In this audit, 6 smaller deficiencies were detected. After applying our method of audit we verified that all the deficiencies except one had been corrected.

Finally, as a consequence of the information obtained, an improvement in the requirements PDP catalog has been obtained [30], which as we already commented, corresponds with one of the phases of method SIREN.

5 Related Work

Some studies related to our proposal, like for example the paper by Shandu and Samarati [24], provide an introduction to the personal data audit, emphasizing its importance in the organizations which deal with personal character data, and in the paper by Hughes [14], which in addition, describes the importance of the audits in the health sector. Nevertheless, in these papers, no application to a study case appears, nor are the specific phases of an audit process distinguished.

In the paper by Baldwin and Shiu [1] the data audit is tackled but focuses on how the data are stored and processed in the system, and on how these data are accessed to make the audit. Dowie and Kennedy [10] analyse the audit processes used in several clinics of British Health Service and come to the conclusion that there is a need for strong staff involvement during the running of the audit, as well as highlighting the importance of following audit standards. This practice, despite its importance, is not widely extended according to the paper. These studies underline that improvement in quality obtained in the systems of these organizations is due to accomplishment of the audits. A further contribution of our work is the proposal of a concrete audit method, compatible, among others, with the CobiT Framework, which is the international standard most widely, accepted for the accomplishment of audits.

Lusignan et al. [20] makes a revision of the state of the art about the role of the sanitary computers systems in the protection of the clinical data. This paper includes a table with the chronological order of the different treaties of the EU, where the fundamental principles of the personal data protection have been developed. Furthermore, another table with a comparison of these principles, adding to this comparison, the general principles of the ethics in health computer systems. In this work, therefore, the general bases of the data protection in the EU are established, and the main international work groups of informatics applied to the medicine, focused on the security of the treated data, are identified.

In the papers by van der Haak et al. [31] and of Massacci et al. [21], practical applications of personal data protection in different European countries, as they are Germany and Italy, respectively, are described. First of them is centred in the identification of specific legal requirements related to the data security and data protection of medical patients, included in electronic clinical files. It is based on the set of laws about data protection existing in Germany. The second paper presents a practical case of the application of a requirements engineering methodology for the fulfilment of the Italian legislation in privacy and data protection, developed by the University of Trento. A contribution of our work with respect to these two is the use of a requirement PDP catalog that gathers, in an understandable language for the requirements engineer, all the requirements related to the privacy and the personal data protection. This PDP catalog developed has validity, carrying out light modifications, in any country of the EU, since it is based among others on the Directive 1995/46/CE [8] and on the Directive 2002/58/CE [9], which are the base of the privacy laws of any European country.

Duri et al. [11] published a data privacy paper in the domain of the automotive where privacy is understood as the people capacity to decide, when, how and what information about themselves, is accessible to others. This paper proposes different models from policies models of personal data privacy and offers a framework that provides confidentiality and integrity of the data in the telematics services of automotive industry, but does not offer a systematic method to make the audit.

In the paper by Rindfleisch [23] methods and techniques are described to protect the personal data of the medical patients. This work is focused on making the patients aware of the necessity of the protection of their medical data, and of how the technology threatens the privacy of their information. This work provides advice about protecting oneself before these threats occur, but again without following any specific methodology. Finally, in the line of Requirements Engineering, we emphasize the work by Firesmith [13], which provides examples and directives for requirements engineers to specify suitably security requirement. The different types of security requirements are identified and defined, among which privacy, security audit and physical protection requirements are highlighted. In this work, nevertheless, no concrete methodology is followed to specify these requirements.

In contrast with the previously described works, our paper offers, an integrated systematic method to make an audit of personal data based on international standards of audit (CobiT) and good practices of Software Engineering (SIREN and international standards of Requirements Engineering) and, it is validated in a real study case. Our work completes other current proposals in the audit area.

6 Conclusions and Further Work

The immediate benefit for an IS that includes the requirements of the PDP catalog is that it will fulfil the LOPD and the RMS “by definition”, thus passing the biennial audit demanded by the RMS in organizations which deal with sensitive data (health, beliefs, economy, etc.).

The requirements catalog presented in this paper fulfils the Spanish Constitutional Law 15/1999, on Personal Data Protection (LOPD). The strategy presented can be extended to the legislation of other countries, particularly to the member states of the EU, because these share a common source, the Directive 95/46/CE [8].

The most important conclusions of this research are the following:

1. The method defined is easy and permits an audit of data protection in organizations which deal specially with protected data, in a systematic way.
2. With the application of the proposed method the security measures are adapted to the standards and regulations demanded by the law in the audited organization.
3. The use of "good practices" in Software Engineering considerably facilitates the subsequent audit work.
4. The possibility of giving precise answers (in %) on the degree of fulfilment of the organization with respect to the requirements document is settled as a result of the audit. Therefore, the organization can ascertain its exact situation regarding this issue, in a quantitative and precise way.
5. In addition to the described advantages directed to the audit and independently of the legal aspects that it helps to fulfil, the application of the catalog in the development of IS supposes, from its outset, an effective and systematic improvement in the security of these.

One future work is the development of a more specific requirements catalog of Medical Records, which will not only cover the legal aspects in the LOPD but would also bring together the obligations imposed in the General Health Law (Law 14/1986), the regulating basic Law on the autonomy of the patient and rights and obligations as regards clinical information and documentation (Law 41/2002), the Law of the Insurance (Law 50/1980), and the Law of Arrangement and Supervision of Private Insurances (Law 30/1995). These Medical Records are very important documents in those organizations dealing with issues of health, and must be maintained with integrity over many years.

Our method also would be applicable in other standards related to the security of IS like ISO/IEC 17799:2005 (Information Technology - Security Techniques - Code of practice for information security management). In this case it would be useful to carry out the control objectives for “conformity” (described in section 12 of the standard), in particular the objective of “conformity with the legal requirements” and the subobjective of “personal character data protection and of the privacy of the people”.

References

1. Baldwin, A., Shiu, S. Enabling shared audit data. International Journal of Information Security. Springer-Verlag. Volume 4, Number 4. pp. 263 – 276. October 2005.
2. Baskerville, R. L. (1999) Investigating Information Systems with Action Research, Communications of the Association for Information Systems, 2.
3. Baskerville, R. L. and Wood-Harper, A. T. (1996) A Critical Perspective on Action Research. Communications of the Association for Information Systems, 2(19).
4. British Authority of Data Protection. http://www.informationcommissioner.gov.uk

5. Chung L. Dealing with Security Requirements during the development of Information Systems. In: Rolland C, Bodat F. and Cauvert C. (eds). Advanced Information Systems Eng., Proc., 5th Int. Conf. CAiSE '93. Berlin: Springer Verlag. Paris. pp. 234-251.
6. CMMI. CAPABILITY MATURITY MODEL INTEGRATION, VERSION 1.1. Technical Report. CMU/SEI-2002-TR-028. Carnegie Mellon. Software Engineering Institute. August.
7. CobiT. Control Objectives for Information and related Technology. Version 4.0. 2005. http://www.isaca.org/cobit.htm
8. Directive 95/46/CE of the European Parliament and Council, dated October 24th: about People protection regarding the personal data management and the free circulation of these data. DOCE no. L281, 23/11/1995, P.0031-0050.
9. Directive 2002/58/CE, of the European Parliament and Council, of July 12, 2002, relative to the processing of personal data and the protection of privacy in the electronic communications industry (Official Gazette of the European Union L 201 of 31.7.2002).
10. Dowie, R., Kennedy, A. Clinical audit in NHS acute and community trusts: a comparative analysis. British Journal of Clinical Governance, Volume 6, Number 2 (2001), pp. 94-101.
11. Duri, S., Elliott, J., Gruteser, M., Liu, X., Moskowitz, P., Perez, R., Singh, M., Tang, J. Data Protection and Data Sharing in Telematics. Mobile Networks and Applications. Volume 9, Issue 6. Pages: 693-701. December, 2004.
12. Federal Trade Commission. Protecting America's Consumers. http://www.ftc.gov
13. Firesmith, D. Engineering Security Requirements. Journal of Object Technology (JOT), 2(1), Swiss Federal Institute of Technology (ETH), Zurich, Switzerland, pp. 53-68, January/February 2003.
14. Hughes, R. Is audit research? The relationships between clinical audit and social research. International Journal of Health Care Quality Assurance, Volume 18, Number 4 (April 2005), pp. 289-299.
15. IEEE (1999). Std 830-1998 Guide to Software Requirements Specifications (ANSI). In Volume 4: Resource and Technique Standards The Institute of Electrical and Electronics Engineers, Inc. IEEE Software Engineering Standards Collection.
16. IEEE (1999). Std 1233-1998 Guide for Developing System Requirements Specifications. In Volume 1: Customer and Terminology Standards The Institute of Electrical and Electronics Engineers, Inc. IEEE Software Engineering Standards Collection.
17. ISACA. Information Systems Audit and Control Association. http://www.isaca.org/
18. Italy Authority of Data Protection. http://www.garanteprivacy.it/garante/navig/jsp/index.jsp
19. Kenny, S. Assuring Data Privacy Compliance. Information Systems Control Journal, Volume 4, 2004.
20. Lusignan, S., Chan, T., Theadom, A., Dhoul, N. (2006) The roles of policy and professionalism in the protection of processed clinical data: A literature review. International Journal of Medical Informatics.
21. Massacci, F., Prest, M., Zannone, N. Using a security requirements engineering methodology in practice: The compliance with the Italian data protection legislation. Computer Standards & Interfaces 27 (2005) 445-455.
22. Regulation (EC) Nº 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.
23. Rindfleisch, T. Privacy, Information Technology, and Health Care. Communications of the ACM. Volume 40, Issue 8. Pages: 92-100. August, 1997.
24. Sandhu, R., Samarati, P. Authentication. Access Control and Audit. ACM Computing Surveys (CSUR). Volume 28, Issue 1. Pages: 241-243. March, 1996. ISBN: 0360-0300.
25. Smith, S. W. and Spafford, E. H. (2004) Grand Challenges in Information Security: Process and Output, IEEE Security & Privacy, 2, 69-71.
26. Spanish Agency of Data Protection. http://www.agpd.es
27. Spanish Constitutional Law 15/1999, December 13th, on Personal Data Protection. BOE no. 298, 14/12/1999 (In Spanish).

28. Spanish Royal Decree 994/1999, June 11th, by means of which the Security Measures Regulations of Automated Files which contain personal data is approved. BOE no. 151, 25/06/1999, page 24241 (In Spanish).
29. Toval, A., Nicolás, J., Moros, B., Baidez, F. Requirements Reuse for Improving Information Systems Security: A Practitioner's Approach. Requirements Engineering Journal (2002) 6:205-219.
30. Toval, A., Olmos, A., Piattini, M. Legal Requirements Reuse: A Critical Success Factor for Requirements Quality and Personal Data Protection. Proceedings of the IEEE Joint International Conference on Requirements Engineering (ICRE'02 and RE'02), pp: 9-13, September 2002.
31. Van der Haak, M., Wolff, A., Brandner, R., Drings, P., Wannenmacher, M., Wetter, Th. Data security and protection in cross-institutional electronic patient records. International Journal of Medical Informatics (2003) 70, 117-130.