Computer Standards & Interfaces xxx (2010) xxx–xxx

Contents lists available at ScienceDirect

Computer Standards & Interfaces

journal homepage: www.elsevier.com/locate/csi

A Personal Data Audit Method through Requirements Engineering

Miguel A. Martínez [a,*], Joaquín Lasheras [a], Eduardo Fernández-Medina [b], Ambrosio Toval [a], Mario Piattini [b]

[a] Software Engineering Research Group, Computer and Systems Department, University of Murcia, Campus de Espinardo, 30071, Murcia, Spain
[b] 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

ARTICLE INFO

Article history:
Received 23 January 2008
Received in revised form 11 December 2009
Accepted 6 January 2010
Available online xxxx

Keywords:
Privacy
Data protection
Audit
Requirements Engineering
Health Information Systems

ABSTRACT

Organizations using personal data in areas such as in Health Information Systems have, in recent years, shown an increasing interest in the correct protection of these data. It is not only important to define security measures for these sensitive data, but also to define strategies to audit their fulfilment. Although standardisation organisations have defined recommendations and standards related to security and audit controls, no methodological frameworks proposing the audit of these sensitive data have been described. This paper presents a methodology with which to audit personal data protection, using Requirements Engineering and based on CobiT. This methodology has been validated in four real case studies.

Contents

1. Introduction

Information Systems (IS) audit is defined as the systematic process of gathering, grouping and evaluating evidence to determine whether an IS safeguards the assets, maintains the integrity of the data, effectively carries out the aims of the organization and uses resources efficiently [1]. A special type of audit within this discipline is the software audit, whose purpose is to verify that both functional and non-functional requirements are accomplished.

According to ISO 7498-2:1989 [2], a security audit is: "an independent review and examination of system records and operations in order to test for adequacy of 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 may include many aspects, such as the level to which facilities or people are protected. In this paper, we focus on the security related to data and information of a personal nature (privacy), which plays a decisive role in the security

* Corresponding author.
E-mail addresses: mmart@um.es (M.A. Martínez), jolave@um.es (J. Lasheras), Eduardo.FdezMedina@uclm.es (E. Fernández-Medina), atoval@um.es (A. Toval), Mario.Piattini@uclm.es (M. Piattini).

0920-5489/$ – see front matter © 2010 Elsevier B.V. All rights reserved.
doi:10.1016/j.csi.2010.01.001

of systems such as the Health Information System (HIS) [3] in which highly confidential information concerning medical patients is processed. Privacy is defined as the right to maintain our personal data and communications secret [4], and is of increasing importance. In ISO 27002 (formerly known as ISO 17799:2005) [5] the aim of Section 15.1 "Conformity with legal requirements" is explicitly "to avoid the breaches of any civil or penal law, statutory requirement, contractual regulation or obligation, and of all security requirements". The US National Science Foundation-dependent Computing Research Association (CRA, www.cra.org) has, furthermore, determined that the security of IS and the privacy of the end-users constitute one of the greatest global security-related challenges [6]. At present, and despite existing laws regulating this aspect [7–11], serious threats to privacy constantly take place. New techniques, methods and standards [12] are therefore needed to confront this problem. Moreover, it is not only important to define technical measures which guarantee security, but also to define strategies and mechanisms to audit its fulfilment.

Furthermore, Requirements Engineering (RE) is a growing area, which has demonstrated its capacity to improve the productivity and quality of the processes and software products [13]. RE offers techniques, methods and standards with which to tackle the initial tasks in the IS development cycle. RE [13–15] includes elicitation, analysis and negotiation, documentation and maintenance of the requirements established for IS. RE therefore contributes with concepts, techniques and tools which, if used appropriately (as we shall show later) can greatly facilitate and improve other tasks related to an organization, particularly audits.

Several studies [16–18] emphasize the benefits of considering *security* in the early phases of system development (in particular, the requirements specification phase), since the definition of security requirements together with the system requirements provides more economical and robust designs which assist in reducing conflicts between functional and security requirements [19]. With regard to personal data protection –*privacy*–, the inclusion of these requirements from the first stages of the system life cycle signifies that the systems are developed according to the requirements of the law from the outset, and not as a later addition [20]. Likewise, the reuse of these requirements helps to increase quality by detecting and correcting errors of inconsistency and ambiguity, and thus favours their subsequent use in new projects [21].

The audit method presented in this paper is based on SIREN (*SImple REuse of software requiremeNts*), a general Requirements Engineering method [21], which is described along with the proposed audit method in Section 2.

The IS audit method presented has a direct correspondence with the CobiT Framework (Control Objectives for Information Technologies) in its latest version (2005) [22]. CobiT is a de facto standard, developed by the *Information Systems Audit and Control Association* (ISACA), and is widely accepted by the international community of IS auditors and Chief Information Officers (CIOs). This proposal is expected to help fulfil those CobiT control objectives that deal with issues of privacy, since the use of the SIREN Personal Data Protection (PDP) requirements catalogue facilitates identification and verification of the fulfilment of the requirements related to these aspects.

Although numerous consortiums and international organizations have defined controls with which to audit IS security, there is no systematic approach that uses engineering techniques to tackle an audit process of information security which is as sensitive as data with guarantees. The development of formal audit methodologies has thus become a necessity [23], and their application domain will be a domain in which the protection of personal data is highly important to the audited organization, such as the HIS domain.

In this paper we propose a methodology which systematizes the audit of particularly sensitive data. We use the most important audit standards and recommendations, along with RE techniques. The use of RE techniques is extremely important because it allows us to identify, model and reuse security requirements, whose fulfilment can later be audited. This method has been validated in four real case studies using Action Research (A-R) methodology [24]. Three of these studies were related to the field of labour consultancy or to a software tool audit and are not, therefore, within the scope of this paper. We thus present only the most significant real case, which is related to an HIS in a private clinic.

The paper is structured as follows: in Section 2 the proposed audit method is described. Section 3 describes the practical applications of the method in a case study, along with the lessons learned and needs identified from the application of Action Research to this real case. Section 4 presents related work which is compared to our proposal. Finally, Section 5 shows our conclusions and future work.

2. Personal Data Audit Method based on Requirements Engineering (PDA-RE)

This section presents the method used to perform a personal data audit. We sought an agile, while comprehensive, systematic and repeatable method, which would fulfil the standards related to audits and Software Engineering, and the method used is an extension of a general audit process, based on CobiT, using a SIREN catalogue of PDP requirements and will be applicable in domains with personal data protection needs, whether as a legal requirement (according to Spanish PDP legislation an audit of the PDP system must be performed at least every two years), as a result of ethical issues, or simply because the organization being audited wishes to offer a good corporate identity.

SIREN requirements catalogues [21,25] contain reusability requirements which are organized within a hierarchy of requirements specification documents and are structured according to IEEE standards [26,27]. The requirements specification used for the audit of the software tool has been created in agreement with the IEEE 830-98 standard, which is responsible for defining the characteristics and contents of a good software requirements specification. We have used the same organization as this standard, along with the indications in the IEEE 1233-98. Requirements in the PDP are organized catalogue by means of types. For example, the SRSP and SYRSP types refer respectively to the PDP requirements contained in the Software Requirements Specification (SRS) and System Requirements Specification (SyRS) documents that correspond with the PDP catalogue. SyRS includes the functions and capabilities of the system, business requirements, organizational, user, security, privacy, etc., while the SRS requirements as regards the system functionality contain external interfaces, performance, design restrictions, non-functional requirements or quality (portability, maintenance, availability and reliability). The PDP catalogue contains two further requirements documents: the Software Test Specification (STS) document and the System Test Specification (SyTS) document, which will specify test cases to guarantee that the system or software fulfils the requirements specified in the SyRs and SRS, i.e. validation criteria needed to test the requirements. The sources used to write the current PDP catalogue requirements are shown in Fig. 1. The PDP catalogue used for the audit is currently composed of 169 requirements, and has 75 traceability relationships among the requirements defined. This PDP catalogue is available in both Spanish and English at http://paso.inf.um.es/pdp. Additional information about SIREN and the SIREN PDP Catalogue is shown in the appendices. The following subsection defines the explicit phases of the Personal Data Audit Method proposed in this paper, along with the role played by the SIREN PDP catalogue requirements documents.

2.1. Phases of the Audit Method PDA-RE

The phases of the PDA-RE method are shown in Fig. 2. The method has been described by following the SPEM notation [28], which is a metamodel for defining processes and their constituting components,

Please cite this article as: M.A. Martínez, et al., A Personal Data Audit Method through Requirements Engineering, Comput. Stand. Interfaces (2010), doi:10.1016/j.csi.2010.01.001

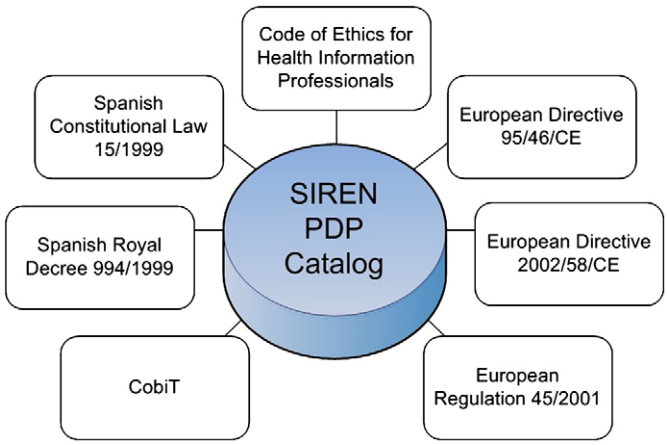

Fig. 1. Sources of SIREN PDP Catalogue contents.

oriented towards the engineering process based on UML. This general method can be used to audit IS or a software tool, signifying that the differences between both are specified in each of the phases.

The actors (roles) implied in the different PDA-RE phases are the following:

- Audit client: the organization which requests an audit of its personal data protection systems or the software tool used to manage its personal data.
- Security audit team: person or set of people in charge of carrying out the audit process.
- Security manager: the person to whom the manager of the organization has formally assigned the task of coordinating and controlling the security measures, including measures concerning the execution of backups, management of storage devices, access control, etc. Under ideal working conditions, this role should be played by the person in charge of implementing and monitoring the safety regulations in the organization's IS, but experience tells us that in many cases this role does not exist, particularly in small and medium enterprises (SMEs), or that the person concerned is overburdened with work. This role could, therefore, be played by a member of the audited organization with sufficient training and experience who is able to provide the aforementioned information, such as, for example, the manager of the human resources or administration departments, etc. This person must have received the proper authorization from the manager of the organization.

For the sake of simplicity, the *security audit team* role is not drawn in Fig. 2 since it appears in all phases of the method. The activities in Phases 1, 3 and 4 are similarly not drawn in Fig. 2 because they will be shown in greater detail in Figs. 3–5. The phases of the PDA-RE method are described as follows:

2.1.1. Phase 1 — previous analysis of the situation

This first phase, in which the three previous actors are involved, is divided into the following three activities (details of the activities of Phase 1 are shown in Fig. 3):

Activity 1.1 *Initial interview*. The scope of the audit is specified through a preliminary *interview* with the *audit client* (organizations or software development teams) in order to draw up an initial budget and planning of the calendar audit.

Activity 1.2 *Initial questionnaire*. A reusable audit questionnaire is sent to the *security manager* (an example of this questionnaire is shown in Appendix B). When auditing an IS, our aim is to obtain all types of information concerning the handling of the data that the company uses. In this initial study of the IS audit, the auditor receives the following information:

- Organization structure (organization chart, information flow, number of work places, etc.).
- Operational environment in which the audit is developed, defining the geographical situation of the systems, the type of internal and external communication of the systems, hardware and software stocktaking, and their architecture and configuration.

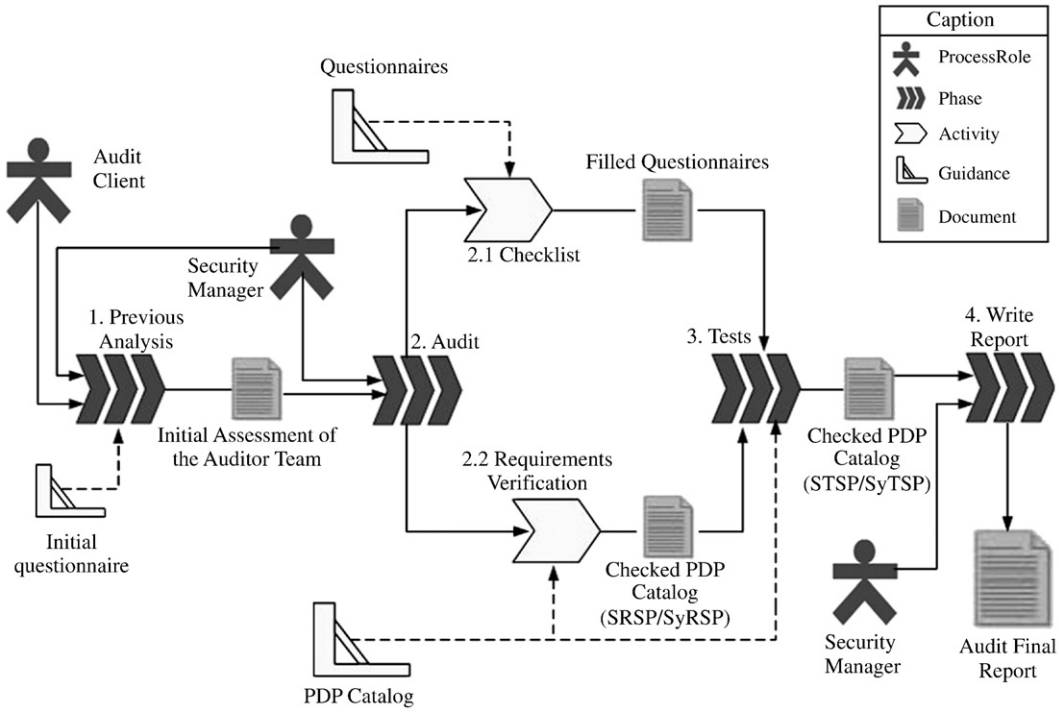

Fig. 2. Phases of the Personal Data Audit Method.

Please cite this article as: M.A. Martínez, et al., A Personal Data Audit Method through Requirements Engineering, Comput. Stand. Interfaces (2010), doi:10.1016/j.csi.2010.01.001

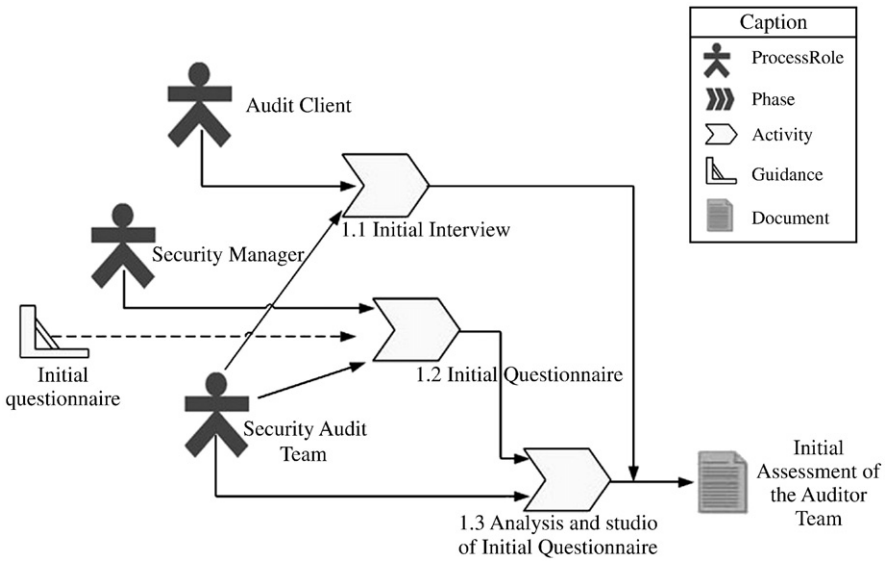

Fig. 3. Details of activities in Phase 1 of the PDA-RE method.

- Identification and classification of the different *existing files*, and the structure of the *database* used, to decide the applicable security level (do they manage medical or health data?; does previous authorization to manage personal data from clients exist?; are the data registered with the Spanish Data Protection Agency?, etc.)
- Information regarding previous security audits (in our case PDP audits).
- Logic security controls in the IS (user identification and password systems, information encryption systems, etc.).

However, if we are auditing a *software tool* the aim is only to gather all types of items/details about the implementation itself and the database used. The auditor receives the following items:

- Methodology used in the design of the software tool.
- Software documentation, such as use manual, UML diagrams, etc.
- Size and features of the database that the software tool logs into.

Activity 1.3 *Analysis and study of the initial questionnaire*. The security audit team analyzes the initial questionnaire filled in by the security manager. In this activity, the security audit team will give an idea of the applicable security level according to the type of data used. Once the questionnaire has been analyzed and the applicable security level (high, medium or low) for the software tool or organization audited has been decided, the audit team can perform other necessary tasks to comply with different legal procedures, such as registering data files with the relevant organization (e.g., the Spanish Data Protection Agency), registering the software tool copyright, registering the organization Website in the trade register, etc.). Table 1 shows the parameters involved in Phase 1.

2.1.2. Phase 2 — system verification audit

This second phase, which involves the security manager and the security audit team roles, is divided into the following two activities:

Activity 2.1 *Filling in the questionnaires (checklists) related to management security of the organization*. This is based on the objective control defined in ISO 27002 (Sections 5 to 15) and CobiT. After Phase 1, the auditor sends the organization's security manager a questionnaire (checklist) related to the organization's management security. This questionnaire has a dual purpose, and is different to the

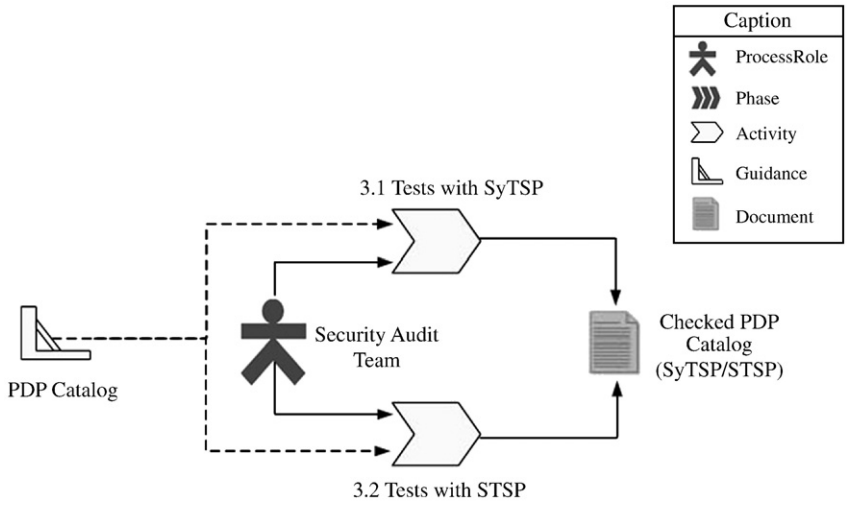

Fig. 4. Details of activities in Phase 3 of the PDA-RE method.

Please cite this article as: M.A. Martínez, et al., A Personal Data Audit Method through Requirements Engineering, Comput. Stand. Interfaces (2010), doi:10.1016/j.csi.2010.01.001

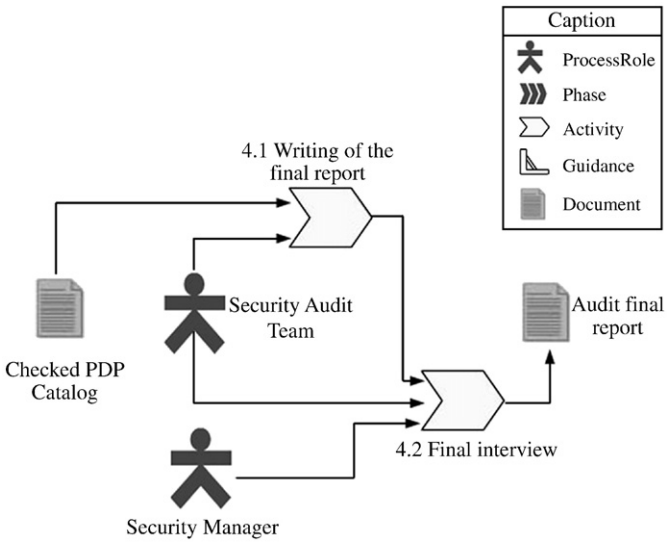

Fig. 5. Details of activities in Phase 4 of the PDA-RE method.

PDP catalogue in activity 2.2, since it is more general and does not only focus upon PDP: on the one hand it permits the auditor to obtain a more concise idea of the organization's state in security issues and on the other, any possible weaknesses in security issues are discovered by the organization's security manager. The questionnaire used by the auditor is based on a standard questionnaire which is valid for all security audits, and on the information obtained in Phase 1. It has a question list concerning the basic issues of the internal control system. This questionnaire is divided into sections or operative areas (output controls, material security, etc.). Once the questionnaire has been filled in, and after an interview, the auditor weighs up the value of the answers, and draws his/her own conclusions. This activity is not necessary in the case of auditing a software tool because these questionnaires only contain questions relating to the physical security of the organization's IS.

Activity 2.2 *Requirements verification with the SIREN PDP catalogue*. The auditor checks the system of the audited organization or the software tool to verify the fulfilment or non-fulfilment of the requirements contained in the catalogue (SRSP and SyRSP in the case of auditing an IS, and only SRSP in the case of auditing a software tool). In this activity we must to take into account whether a report of a previous PDP audit exists, since more attention should be paid to the verification of those controls which were not fulfilled in the previous PDP audit. These verifications will be made with the support of the organization's *security manager* who should, as far as possible, facilitate the auditor's task in deciding whether or not each requirement is fulfilled. This verification is lightweight, because it is sufficient to choose those requirements from the catalogue that are relevant in the audited organization and to individually verify whether or not they are fulfilled in the organization's IS (or software tool). Both the requirements of the catalogue and the text itself, have associated meta-information (attributes containing information about each requirement) which enriches the requirement. At present 20 attributes are defined, which include: *source, exceptions, security level, motivation, fulfilment* and *infringement*. The use of these attributes is more powerful than the use of traditional checklists in that, for example, they permit the rapid discovery of what the fine for the non-fulfilment of a requirement is (thanks to the *infringement* attribute), or whether the organization requires a high level of data protection. The auditor will extract the requirements which are necessary to attain this level of protection from the catalogue and will verify whether said requirements are present in the organization. This extraction or filtrate of requirements from the catalogue is possible thanks to the use of the *meta-information* associated with each requirement, in this case through the *security level* attribute. An additional advantage of the use of SIREN in this activity is the traceability management that it performs (inclusive, exclusive and parent–child [21]). This is useful when applied to the audit if, for example, a parent requirement is not fulfilled since it is not necessary to verify its child requirements, because they will not be fulfilled by the organization or software tool, and this reduces the number of verifications to be carried out by the audit team. Moreover, the traceability requirements are grouped logically, so if a requirement which includes traceability is not fulfilled then the audit team will be put on alert to detect any other possible non-fulfilment requirements associated with it. Table 2 shows the parameters involved in Phase 2.

2.1.3. Phase 3 — system testing

In this phase it is necessary to ascertain whether the IS software is working as expected. If we are only auditing a software tool, this phase must confirm the results obtained in the previous phase, whereas if we are auditing an IS, the risk to the organization if some of the checked measures are not fulfilled must also be verified. The SIREN PDP catalogue SyTS and STS documents will be used to carry out the tests. The SyTS and STS documents are useful since, for each of the requirements identified in the SyRS or SRS it is also necessary to

Table 1
Parameters of Phase 1.

Inputs	■ Initial questionnaire
Outputs	■ Organization structure ■ Operational environment of the organization. ■ Existing files and previous audits ■ Documentation of the software tool. ■ Initial assessment of the auditor (scope and audit target, study of the audit environment).
Roles	■ Audit client. ■ Security audit team. ■ Security Manager.
Techniques and practices	■ Information collection techniques [14]: – Closed interviews. – Observation and social analysis. – Facilitated Application Specification Techniques (FAST). ■ Documentation study.

Table 2
Parameters of Phase 2.

Inputs	■ Previous analysis. ■ Questionnaires. ■ PDP Catalogue (SRSP/SyRSP).
Outputs	■ Checked SRSP/SyRSP. ■ Questionnaires filled in by the security audit team.
Roles	■ Security manager. ■ Security audit team.
Techniques and Practices	■ Use of software tools: – Software tools specific to audit, such as BSA tools (www.bsa.org) – Computer-Aided Requirements Engineering (CARE), such as Rational IBM RequisitePro (www-306.ibm.com/software/awdtools/reqpro/).

Please cite this article as: M.A. Martínez, et al., A Personal Data Audit Method through Requirements Engineering, Comput. Stand. Interfaces (2010), doi:10.1016/j.csi.2010.01.001

specify how those requirements can be checked by means of a textual description of the process that follows. This signifies that any person (recently incorporated or inexperienced) can perform the tests in a simple and systematic manner. This third phase is divided into the following two activities (details of the activities of Phase 3 are shown in Fig. 4):

Activity 3.1 *Tests with the SyTS*. The organization's privacy policy can be directly defined from the SyTS. This policy will include a list of questions related to data protection, which can easily be checked.

Activity 3.2 *Tests with STS*. The role of the STS document is to define when a requirement included in the SRS is fulfilled. This document serves as an aid to ascertain whether the software tool's requirements are fulfilled (verifying its degree of fulfilment) and to indicate what measures should be taken if this is not the case.

For example, one of the SyRS requirements, which specifies the system's performance when it is performing a concrete operation (the test requirement) included in the SyTS document that checks it has the following descriptor: "the person in charge of the organization's security will execute [number of simultaneous applications] on [number of computers], and will observe the system's behaviour, measuring the time taken to execute all these applications". Table 3 shows the parameters involved in Phase 3.

2.1.4. Phase 4 — final interview and writing of the final report

This fourth phase, which involves the security manager and the security audit team roles, is divided into the following two activities (details of the activities in Phase 4 are shown in Fig. 5):

Activity 4.1 *Writing of the final report*. The writing of the report represents the final stage, and is the result of the evaluation made. The contents of the report will depend on the aims of the audit, but as a minimum the report will contain the following information:

- Situation: which briefly describes the resultant weaknesses after the analysis of the IS or the software tool has been carried out.
- Threats: the possible risks to which the organization or the software tool is exposed are enumerated. The degree to which the problem is critical is shown with a qualification of 1 to 3 (1: Low; 2: Medium; 3: High).
- Recommendations and action plans are proposed to the organization or development team.

Activity 4.2 *Final interview*. Once the report has been completed, a final interview is held with the *security manager*, in which the report is analysed. The purpose of this interview is to describe the deviations detected in the system. These deviations must be accepted and understood by the *security manager* of the audited organization or software tool. The *security manager* will take the appropriate corrective measures proposed by the audit team. In the case of auditing an organization's IS, s/he will keep the report, which will remain at the disposition of the Data Protection Agency [29], the Spanish institution that oversees compliance with legislation on data protection and controls its application. Moreover, if a report of a previous PDP audit exists it is also possible to provide information about the evolution of the security in the organization or software tool. Table 4 shows the parameters involved in Phase 4. After the audit, the organization will implant the solutions and security measures proposed.

Table 3
Parameters of Phase 3.

Inputs	■ PDP Catalogue.
Outputs	■ Checked STSP/SyTSP.
Roles	■ Security audit team.
Techniques and Practices	■ STS and SYTS SIREN documents.

Table 4
Parameters of Phase 4.

Inputs	■ Checked PDP Catalogue.
Outputs	■ Final audit report.
Roles	■ Security audit team. ■ Security manager.
Techniques and Practices	■ IS Standards, Guidelines and Procedures for Auditing and Control Professionals, by the ISACA [30].

In Table 5, we summarize the phases and activities of the PDA-RE method. We show the differences between the application of PDA-RE to an IS (such as an HIS) or a software tool, showing the activities which are applicable or otherwise in both types of audit.

This paper's main contribution towards a common audit method is centred on Activity 2.2, in which a verification of the systems of the audited organization, based on the SIREN PDP catalogue [25], is carried out. Furthermore, a correspondence exists between these requirements and the CobiT Control Objectives. This correspondence is not shown in the paper owing to space constraints. Concrete examples can be found in the "Conformance with the CobiT Framework" section at http://paso.inf.um.es/pdp.

As an improvement to the PDA-RE method, and following the successive applications of the method and analogy to the requirements repository improvement phase described in SIREN, the audit method now contains a new final and additional phase which improves the guidelines used in the different phases. This specifically improves: the initial questionnaire in Activity 1.2; the questionnaires related to the management of physical security in the organisation in Activity 2.1; and the SIREN PDP catalogue in Activity 2.2.

3. Practical applications of the audit method PDA-RE

PDA-RE has been validated in four real practical cases, of which only one is presented here owing to space constraints. The case study took place in the IS of an organization of approximately 60 employees, within the health sector (a private clinic). This organization is subject to a high level of protection, in accordance with the *SMR*. The organization's name is not included for reasons of confidentiality. This private clinic, which is located in Murcia (Spain), has an agreement with the public sector and therefore also cares for National Health patients. The qualitative research method denominated as Action Research (A-R) [24] has been used in the design of this case study.

Table 5
Summary of the phases and activities of the PDA-RE method.

Phases	Activities	IS audit	SW tool audit
Phase 1	Activity 1.1	Yes	Yes
	Activity 1.2	Yes	Yes
	Activity 1.3	Yes	Yes
Phase 2	Activity 2.1	Yes	No
	Activity 2.2	Yes (SyRS and SRS requirements document)	Yes (SRS requirements document)
Phase 3	–	Yes	Yes
Phase 4	–	Yes (Report at the disposition of the Spanish Data Protection Agency)	Yes

Please cite this article as: M.A. Martínez, et al., A Personal Data Audit Method through Requirements Engineering, Comput. Stand. Interfaces (2010), doi:10.1016/j.csi.2010.01.001

3.1. Audit of a Health Information System

The organization which is the object of this study has, since 1998, offered a wide variety of health care services, including therapeutic and diagnostic surgery, related to different medical specialties, and treats more than 5000 patients per month. This organization has held the ISO 9001:2000 certificate of quality for all the clinic's activities (consultancy and medical clinic) and in all its areas (commercial, marketing, management, etc.), since May 2004. The audit phases are described as follows:

Phase 1 the information regarding the organization audited was obtained from its personnel through two meetings (two closed interviews of two hours each). Three hours were also spent on the study of the documentation gathered in those initial meetings and on the initial questionnaire.

Phase 2 This phase has two activities:

2.1 Questionnaires. Once we had received the questionnaire filled in by the organization's *security manager*, the answers were checked and we concluded that, at first sight, the organization had an acceptable level of security (62.5%). The questionnaire used to carry out this audit will serve as a standard questionnaire in future audits. It is made up of 30 questions, which directly correspond with some of the requirements of the SIREN PDP Catalogue. 24 questions (of the 30) correspond to a binary checklist (i.e. the answer can only be "yes" or "no"). 15 of these questions received a positive response (controls that exist in the organization) and 9 received a negative response. A summary of the questionnaire used to perform this audit is shown in Table 6. This table was filled in by the organization's security manager, who responded to the questions (by putting a mark against the multiple choice questions or by answering yes/no to the single-choice questions), and who wrote additional comments in the observation column.

2.2 SIREN PDP catalogue. In order to carry out this activity, a meeting was held with the personnel in which the fulfilment, or non-fulfilment, of the requirements of the SIREN PDP catalogue were reviewed individually. The PDP catalogue used for this audit is currently composed of 169 requirements, and has 75 traceability relationships among the requirements defined which help to manage the corresponding aspects related to the HIS. The results obtained after this verification provided specific data for both parties (the audited Organization and the Research Group). 61.5% of the requirements contained in the catalogue which were relative to organizations of a high level of security *LOPD/SMR* were thus fulfilled. If the requirements that could not be applied to this organization (those marked *undetermined*) are not taken into consideration, then 83.8% of the SIREN PDP catalogue requirements were fulfilled.

Table 7 shows the results obtained after these requirements had been checked in greater detail.

Table 6
Questionnaire regarding the check of massive storage.

Protection data audit — questionnaire checklist					
Reference		Question	Results		
ID	Requirement		Yes	No	Observation
1	SYRSP30	Do the places in which the massive storage devices are kept have:	Air-conditioning ☑ Protection against the fire ☑ Special lock ☑ Other protection ☐		
2	SYRSP30	Do these places have any automatic protection against the fire?	X		
3	SYRSP30	What minimal information does the magnetic files inventory contain?	Serial number ☑ Password ☐ File number ☑ System which generates it ☐ File expiration ☐ Volume number ☑ Other information ☐		
4	SYRSP31	Is the validity of the magnetic files inventory often verified?		X	It is done in manually
5	SYRSP31	Are files with confidential information identified and stored with passwords?	X		All files store confidential information
6	SYRSP31	Is there a strict control of backups of these files?	X		
7	SYRSP32	What storage device is used?	Piece of furniture with lock ☐ Strongbox ☑ Other storage devices ☐		
8	SYRSP32	Where is this storage device situated?	Department of the building ☐ Server room ☑ Other place ☐		
9	SYRSP32	Are the files of the storage devices deleted when they are discarded?	X		
10	SYRSP33	Are the new storage devices received in this place registered as part of the inventory?	X		
11	SYRSP33	Are periodic audits of the storage devices often performed?	X		
12	SYRSP33	Is access to the places in which the storage devices are kept restricted to authorized employees?	X		
13	SYRSP33	Is there a list of the authorized employees who can sign out confidential files?		X	Files cannot be signed out
14	SYRSP33	Is there a procedure to register the lending of files and the date when they must be returned?		X	Files cannot be lent

Some examples of the fulfilment (or otherwise) of the catalogue requirements in the audited organization's system are the following:

Requirement SRSP 6. Basic level of security: "The [identification procedure] and [authentication procedure] will limit the possibility of repeatedly attempting a non-authorized access to the application".

Fulfilled. This is limited to three failed access attempts.

Requirement SRSP 7. Medium level of security: "Tests to the software performed prior to the implantation or modification of IS dealing with files containing

Table 7
Results of Activity 2.2 of the audit of Health IS.

	System Requirements (SyRSP)	Software Requirements (SRSP)
Fulfilled	80	24
Not fulfilled	16	4
Undetermined	25	20

Please cite this article as: M.A. Martínez, et al., A Personal Data Audit Method through Requirements Engineering, Comput. Stand. Interfaces (2010), doi:10.1016/j.csi.2010.01.001

personal data will not be made with real data unless the corresponding security level is assured".

Not fulfilled. The previous software tests add a possible improvement to the software tool and are composed of real data from clinical patients.

Requirement SYRSP 61. *High level of security*: "The backup copies and data recovery procedures will be kept in a different place to those of the computer equipment which handles them".

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

Requirement SYRSP 62. *High level of security*: "The transmission of data of a personal nature via telecommunications networks will be carried out by encoding these data or by using any other mechanism that guarantees that the information is neither intelligible nor capable of being manipulated by third parties".

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

Phase 3 Once the first two stages of the audit method had been completed, the SyTS and STS documents from the SIREN PDP catalogue were used to verify the correct operation of the system. Of the 80 requirements fulfilled by the organization, it was possible to check 34 by means of a specific procedure, and these therefore had a correspondence with the SyTSP document. In the case of the SRSP requirements, 18 of the 24 fulfilled requirements had a direct correspondence with the STSP document. After checking these SyTSP and STSP requirements, we were able to ensure that the IS of the organization was working as expected, thus confirming the results of Phase 2.

Phase 4 The final report was written as a result of the evaluations made. The final report gathers together those requirements which were not fulfilled in the audit system, thus ensuring the identification of the weak points and threats which put the system's security at risk.

In this case, the audited organization was equipped with the measures required by law (as regards security and personal data protection), with the exception of the discovery of slight deficiencies, which were all that the organization's system administrators had to correct. Similarly, the obligatory security document for an organization with a high level of protection had already been written up in a suitable manner, signifying that the measures that the Medical Centre had to implant were minimal.

Some of the slight deficiencies detected were the following:

- Data (profession, situation...) gathered through the medical centre's computer application existed and had not been reflected in the files registered with the Data Protection Agency [29], which is required by Spanish Legislation (Spanish Royal Decree 994, Section 17).
- The company had stipulated (by contract) the transference of personal data for management by third parties, but this information was not reflected in a visible form.
- Some users, whose position within the organization did not allow them this privilege, had authorization to access all the company's files.

A summary of the final audit report delivered to the audited organization is shown in Tables 8 and 9. The confidentiality of the data handled in the audited organization, and the commitment to confidentiality that the audit team must maintain obviously signifies that personal data cannot be revealed to third parties not involved in the audit process.

All the roles involved in the method participated in this case study, including the security manager, since that role exists in the audited organization. The roles of the administration department and the

Table 8
A summary of the final audit report delivered to the audited organization (part 1).

Customer data
- Applicant organization: Not shown for reasons of confidentiality.
- Social address: Not shown for reasons of confidentiality.
- Manager of the organization: Not shown for reasons of confidentiality.

Participating roles
- Auditor/s: Miguel Angel Martinez and Joaquin Lasheras.
- Security manager: Not shown for reasons of confidentiality.
- Authorized employees:
  - Manager of the administration department: Not shown for reasons of confidentiality.
  - Manager of the computer department: Not shown for reasons of confidentiality.

Audit Summary
- Carried out on 1st and 2nd June, 2006.
- The aim of this audit is to verify the adequacy of and compliance with the requirements of the SIREN PDP catalogue, according to current legislation on personal data protection.
- The audit's objective is the IS of (organization's name not shown for reasons of confidentiality), focused on the following topics:
  - The processing of the organization's personal data.
  - The physical and logical security of the IS.

We have checked the security document and its associated procedures. We have simultaneously verified the implementation of the technical measures required in the identification and authentication systems, physical and logical access control, media management and backup.

In the process of applying the method, exceptions or limitations have not been defined.

In general, the personal data protection system is updated, with a well structured and comprehensive security document, in which both the document itself and its associated procedures precisely reflect the current state of the system. There are no significant shortcomings.

To carry out the audit we have used the PDA-RE method, proposed by the Software Engineering Research Group (University of Murcia, Spain) and by the ALARCOS Research Group (University of Castilla–La Mancha, Spain). We should like to express our gratitude to the clinic's staff for their cooperation during our work, particularly those of the Computer Department. We remain at your disposal for any necessary clarification of this report.

Table 9
A summary of the final audit report delivered to the audited organization (part 2).

Situation (deficiencies)

Security in the physical and logical area:
- D1. There is no special vigilance of the organization's data server.
- D2. The data transmitted over the network for internal communication does not contain any encryption mechanism.
- D3. Some users of the IS access more data than the functions of their jobs authorize them to do.
- D4. There are no copies of confidential files outside the organization itself.
- D5. The validity of the inventory data files is not automatically checked.
- D6. There is no record of the destruction of magnetic devices.
- D7. The tool collects personal data from more patients who are registered with the Spanish Data Protection Agency.

Threats
- D1, D2 and D3. Probable distribution of confidential data (2).
- D4. Loss of vital information (2).
- D5 and D6. Poor document management of the organization processes (1).
- D7. Economic sanctions by the Spanish Data Protection Agency (1)

Recommendations and action plans

In order to minimize the risks described above, we suggest the following actions:
- D1, D2 and D3. Establish a more sophisticated security mechanism in the server room during working hours (camcorder).
- D4. Establish a safe place outside the organization to store backup copies of high level personal data.
- D5 and D6. Establish a procedure for updating the inventory data file and a record for the destruction of magnetic devices.
- D7. Change the registration of the patients' file in the Spanish Data Protection Agency, adding the fields that are not declared.

Please cite this article as: M.A. Martínez, et al., A Personal Data Audit Method through Requirements Engineering, Comput. Stand. Interfaces (2010), doi:10.1016/j.csi.2010.01.001

computer department managers also participated as collaborators (during Phase 2.2), since these roles are perfectly capable of taking on the security manager's role owing to the ease of the application of the process. The security manager's increased workload during the development of the audit made it necessary for these roles to participate in the process implementation. The relationship between the audit team and the other participants was excellent. Their participation was positive and they provided the information required by the audit team at all times. According to conversations with (more experienced) staff during the process implementation, we verified that the audit with our PDA-RE method is more agile and rapid than previous audits of their IS, since the audit of the entire IS is achieved in very few steps.

Since the audits are repeated (at least every two years in accordance with Spanish PDP Legislation), it is necessary to take the previous audits performed in the organization into consideration. The organization's evolution in security issues can thus be included in the final audit report. This was taken into account in the second audit which was performed in the private clinic in December 2008. In this last audit we again applied the PDA-RE method, and we verified that the private clinic had undergone an improvement in its IS security measures and that 65% of the requirements contained in the SIREN catalogue had thus now been fulfilled. If the requirements that could not be applied to this organization (those marked *undetermined*) are not taken into consideration, then 88.7% of the SIREN PDP catalogue requirements were fulfilled.

Two of the deficiencies that were rectified in the clinic between the first and second audit are the following:

- A security camera has been installed in the clinic hall which captures the access to the IS server room.
- A backup of the high level personal data is stored in a bank near the clinic once every two weeks.

3.2. Lessons learned

The lessons learned in our experience as health IS and software tool auditors are principally the following:

- A-R has been shown to be a useful research method for combining theory and practice by means of a cyclic, collaborative process. A-R is oriented towards the production of new, practical knowledge for the current situation of a group of practitioners. A-R promotes a reflective learning process and a search for solutions which involve both researchers and practitioners.
- It is possible to inform the audited organization about the degree of law-fulfilment in security issues related to the protection of personal data. It is also possible to show the non-fulfilment of the privacy law. Similarly, in the case of a software tool, audit supposes an important aid to new version improvement.
- Thanks to the existence of a previous requirements catalogue, we have been able to reduce the time dedicated to meetings and other auditing activities. The interviews with the development team and the organization's board of directors (who usually have very little time available) can be directly focused on and guided towards the crucial points concerning the audit. The audited organization has, moreover, confirmed that, in comparison to previous audits, our method has required less effort: fewer stakeholders are involved and less time is needed to assimilate the concepts described by the Law, because the requirements are gathered in a more understandable language than that which appears in legal documents.
- We have detected weak points in the requirements catalogue used in the audit. These inconsistencies were caused by the existence of ambiguous and badly-written requirements, which impeded the audit team from making firm decisions about the fulfilment of or breach in the software tool or health IS. As a consequence of the information obtained, an improvement has been made to the PDP requirements catalogue [25], which corresponds with one of the phases in the SIREN method.
- The traceability in SIREN catalogues was also revealed to be useful in detecting linked threats in the systems audited. For example, in our case study of the private clinic, we detected that a primary threat to the client was knowledge regarding who managed their personal data, and thanks to traceability we detected a deficiency in contracts with third parties.

As regards the use of standards:

- There is no universal standard for audit. As is mentioned below, the importance of audit Standards has been detected by other authors [31].
- We suggest a “de iure” standardization of CobiT as the audit standard, with the advantage that every auditor will be able to follow the same criteria.
- The ISO 27000 standards family concerning Information Security Management Systems will contribute towards promoting a culture of security in organizations. Audits must play a central role in establishing this security “culture”.
- The use of “good practices” in Software Engineering, such as IEEE Standards or CMMI (and SCMM, its extension to secure systems), on the part of the department or company which provides computer science support to health organizations, considerably facilitates the subsequent auditing work. On the other hand, we have identified certain deficiencies in the use of some IEEE standards. We thus propose to identify privacy requirements as a section in the IEEE 830 requirements document.

4. Related work

To the best of our knowledge, little work has been carried out on audit privacy techniques during the last few years. There now follows a summary of certain proposals related to personal data audit [31,32], HIS [33,34], legal requirements [35–37], the audit process in software tools [38] and security requirements [23,39–41].

Hughes [32] provides an introduction to personal data audit, emphasizing its importance in those organizations that deal with personal data. This paper additionally studies the relationships between audits and research methods, such as A-R, when applied to the health sector of the United Kingdom. Hughes concludes that audit is insufficiently defined, both philosophically and conceptually, for it to be researched, and that much current audit practice is not sufficiently rigorous to constitute research. However, in our paper we show how A-R has been applied in a case study and we describe the specific phases of an audit process.

Dowie and Kennedy [31] analyse the audit processes used in several British Health Service clinics and conclude that there is a need for strong staff involvement during the running of the audit, along with highlighting the importance of following audit standards. According to their paper this practice is not widely extended, despite its importance. This study underlines that any improvement in quality obtained in these organizations' systems is owing to audit fulfilment.

Lusignan et al. [33] review the state of the art in the role of health computer systems in the protection of clinical data. Their paper includes a table with the chronological order of the various EU treaties, in which the fundamental principles of personal data protection have been developed. Another table shows a comparison of these principles, and includes the general principles of the ethics in health computer systems. The general bases of data protection in the European Union are therefore established in this work, and the main international work groups in computer science applied to medicine, which focus on the security of that data, are identified. The European directives and regulations cited by Lusignan et al. are the same as those used to create the PDP requirements catalogue.

Please cite this article as: M.A. Martínez, et al., A Personal Data Audit Method through Requirements Engineering, Comput. Stand. Interfaces (2010), doi:10.1016/j.csi.2010.01.001

The paper by Rindfleisch [34] describes certain methods and techniques with which to protect medical patients' personal data. This work focuses on making patients aware of the necessity to protect their medical data, and of how technology threatens the privacy of this information. This work provides advice regarding protecting oneself before these threats occur, but again fails to follow any specific methodology or provide concrete lists of PDP requirements.

The papers by van der Haak et al. [35] and Massacci et al. [37] describe the practical applications of personal data protection in two different European countries (Germany and Italy). The first paper focuses on 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 on 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. Nevertheless, neither of these approaches uses any source of specific requirements, such as our PDP catalogue, as a basis.

Some of the most important European computer science standards for health appear in the paper by Kokolakis and Lambrinoudakis [36], with emphasis upon their contribution towards an interoperability of HIS, and the fulfilment of legal requirements and security.

With regard to the auditing process in software tools, we should like to draw attention to the work by N. Greif [38] which reviews the various software quality assurance approaches. As in our proposal, the authors use requirements catalogues or audit checklists (which are continuously updated) to carry out preventive software audits, thus reducing the time spent by the auditor. These catalogues are available on the World-Wide Web, although they are difficult to read for those people who are not relatively fluent in German. Furthermore, none of these predefined catalogues deal with aspects of personal data protection or follow Software Engineering Standards, such as IEEE 830-1998 and IEEE 1233–1998.

Finally, with regard to RE, several methods that attempt to integrate security into the development of information systems are currently being developed. These approaches pursue the integration between security engineering and requirements engineering with the aim of developing more secure software systems from the early development stages [39]. Of these approaches we should like to draw attention to the work by Mead et al. [23] which defines a model (SQUARE, Security Quality Requirements Engineering Methodology) in which a means for eliciting, categorizing and prioritizing security requirements for information technology systems and applications is provided, and that of Zuccato et al. [40] which defines a security engineering method called SKYDD that covers information, infrastructure, and business requirements based on information classification and uses a combination of reference tables and checklists. These methods do not, however, meet security standards and do not support the reuse of security requirements. We should also emphasize the work by Firesmith [41], that provides examples and directives with which requirements engineers can specify suitable security requirements. The various types of security requirements are identified and defined, among which privacy, security audit and physical protection requirements are highlighted. Nevertheless, no concrete methodology is followed to specify these requirements.

In contrast with the aforementioned work, our paper offers an integrated and repeatable systematic method with which to audit personal data, based on de facto auditing standards (CobiT) and good Software Engineering practices (SIREN and the IEEE Requirements Engineering international standards [26,27]). The approach presented could be used in conjunction with those works that integrate security into requirements engineering since our approach meets with some of the most characteristic issues of both disciplines, such as the use of security standards to define the requirements and their reuse, which keeps the requirements catalogue constantly updated. It has been validated in a real case study. A further contribution of our paper with regard to the above is that it provides a product (a requirements catalogue) that fulfils the main laws of protection of personal data, extended to the scope of health. Thus, our work complements other current proposals within the area of auditing.

5. Conclusions and further work

The application of this method and our experience with its users permits us to first conclude that the method defined is easy to use and permits a systematic audit of data protection in organizations which deal specifically with protected data.

The application of the proposed method allows security measures to be adapted to the standards and regulations demanded by law, both in the organization audited and in those which use the software tool.

The application of the method permits precise answers (in %) about the organization's degree of fulfilment with regard to the requirements document established as a result of the audit. The organization can therefore ascertain its exact situation with regard to this issue in a quantitative and precise manner.

Furthermore, an improvement to the PDP requirements catalogue has been made, which corresponds to one of the SIREN method phases. The quality of the existing requirements has therefore been improved and some requirements, which were identified as necessary or advisable, have now been included in the PDP SIREN catalogue.

In addition to the advantages described for the audit, and independently of the legal aspects that it helps to fulfil, the application of the catalogue in the development of IS, such as HIS, supposes an effective and systematic improvement in security from the outset.

In relation to this last point, the immediate benefit for an IS that includes the PDP catalogue requirements described with the SIREN methodology is that it will fulfil the *LOPD* and the *SMR* "by definition", thus passing the biennial audit demanded by the *SMR* in organizations which deal with sensitive data (health, beliefs, economy, etc.). If the IS has not been constructed in this way, the method proposed in this paper will identify those parts of IS that do not fulfil this norm.

Our method could also be applicable in other standards related to the security of IS such as ISO/IEC 27002 (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 sub-objective of "personal character data protection and the privacy of the people".

However, although our method can be generalized to other functional and non-functional software concerns, it is necessary to have a requirements catalogue which is similar to that used in this paper. We have recently developed the following reusable requirements catalogue:

- Personal Data Protection (PDP) [25].
- Security in Information Systems [21].
- Tele-operated Systems [42].

If a predefined specific requirements catalogue dealing with the concern or concerns that we wish to audit is not available, then other widely accepted alternative sources may be used. For example, standard ISO/IEC 9126 [43] could be used as a guide for a software quality audit.

Further work, which is already underway, is the development of a more specific Electronic Medical Records (EMR) requirements

Please cite this article as: M.A. Martínez, et al., A Personal Data Audit Method through Requirements Engineering, Comput. Stand. Interfaces (2010), doi:10.1016/j.csi.2010.01.001

catalogue, in accordance with the legislation in force (national and international) and the HL7 standard (Health Level Seven, www.hl7.org). This catalogue will be used for the exchange, management and integration of electronic healthcare information, and the European standard EN13606 will be used for the structuring and representation of health data.

Acknowledgments

This work has been partially financed by the Spanish Ministry of Science and Technology, project PEGASO, TIN2009-13718-C02-01, PANGEA, TIN2009-13718-C02-02 and BUSINESS, PET2008-0136, and by the FEDER and the Castilla-La Mancha Regional Government, project MELISA:GREIS, PAC08-0142-335.

Appendix A. SIREN and the PDP requirements catalogue

SIREN [21,25] has, until now, been used in four ways with regard to security and privacy issues: 1) from the beginning of the development to guarantee direct compliance with the applicable norm (e.g. in security and the PDP) through the use of adapted catalogues, similar to an RE method; 2) as a guide and support to create an audit which permits us to determine the existing controls and the degree of the security fulfilment in an organization; 3) as a method for auditing software (either developed by the organization or acquired) in operation; and 4) similarly, as a consultation method in the acquisition of new software, so that this software can be guaranteed to satisfy the expected level of security. The use of SIREN in the first manner was published and presented in [21,25]. In this work, we focus on the second to fourth issues.

It is recognized that, by using a set of requirements which have been previously specified and used for other projects or domains as a starting point, we can improve the precision and efficiency of the requirements specification for the current project [13] and also reduce the time needed to elaborate this specification.

The PDP requirements catalogue used in this paper conforms to the Spanish Personal Data Privacy Law, which is an adaptation of European Union Legislation. The proposal can be generalized to other European countries, since they have a shared basis [7,44,45] for the development of their own privacy laws.

With regard to Spanish PDP legislation, on the one hand we deal with the Constitutional Law 15/1999, (*LOPD*) [10]. The *LOPD* seeks to gather, to guarantee and to protect issues relating to the handling of personal data, civil rights and the fundamental rights of the individual, and especially those relating to an individual's honour, and personal and familial privacy. On the other hand we deal with the Security Measure Regulations of Automated Files which contain personal data (*SMR*) [11]. The *SMR* seeks to determine measures of a technical and organizational nature which will guarantee the confidentiality and integrity of information in order to preserve honour, personal and familial privacy and the full exercising of personal rights against any alteration, loss, handling or non-authorized access. The *SMR* classifies the indispensable security measures in 3 levels: *basic*, *medium* and *high*. These levels are established on the basis of the nature of the information dealt with, and according to the greater or lesser extent to which it is necessary to guarantee the confidentiality and integrity of the information.

As regards the European directives and regulations, we consider as a basis the European Directive 1995/46/CE [7] on the protection of physical people with regard to the treatment of personal data and the free circulation of data. This directive, which is made up of a total of 34 articles distributed throughout seven chapters, was the reference for the adaptation of European member countries' laws with regard to privacy; Regulation 45/2001/CE [45] of the European Parliament and Council, relative to the protection of physical people with regard to personal data processing by the communitarian institutions and organisms and to the free circulation of these data; and Directive 2002/58/CE [44] of the European Parliament and Council, which is relative to the treatment of personal data and to the protection of privacy in the sector of electronic communications.

The PDP catalogue proposed in this work is more powerful than the traditional checklists used to perform audits since the information associated with each requirement (by means of attributes) provides the auditor with a more complete guide to carry out the audit. The catalogue can also be continuously updated and revised thanks to its reusability. Furthermore requirements with dependencies or exclusive mutual relationships can be easily tracked by means of traceability.

Another important aspect of the catalogue is the handling of exceptional cases, which occurs relatively frequently in texts of a legislative nature. These exceptions are reflected in the attribute exception (associated with each of the requirements of the catalogue), thus ensuring that the catalogue is complete and self-sufficient.

Finally, PDP catalogue requirements directly correspond with the code of ethics for professionals in medical computer science developed by the International Medical Informatics Association (IMIA) [46]. An example of this correspondence, can be seen in Principle 4 of Access, "*the subject of an electronic record has the right of access to that record and the right to correct the record with regard to its accurateness, completeness and relevance*", and requirements from the SYRSP105 to the SYRSP111 of the PDP catalogue in which, for example, the requirement SYRSP106 has the following textual description: "*The interested party will have the right to obtain an immediate rectification of the inexact or incomplete personal data from the person in charge of the handling*".

Appendix B. Initial questionnaire

Questions related to general data of the organization.

Question	Yes/No/Number
Number of employees	
Number of dependent offices	
Are there servers in the dependent offices?	
Are computer facilities similar in the dependent offices?	
Does the organization have a customer advertising campaign?	
Are the responsibilities and functions of the workers well documented?	
Has anything been reported to the Spanish Data Protection Agency by affected persons?	

Questions related to Information Systems

Question	Yes/No/Number
Number of servers	
Number of net devices (switches, hubs, routers, proxies, etc.)	
Are there outside connections?	
Number of work positions in Information Systems	
Number of software tools	

Questions related to data level

Question	Yes/No/Number
Does the organization have the workers' economic data?	
Does the organization have the workers' health data?	
Are any data files registered with the Spanish Data Protection Agency?	
Are workers' or customers' data sent to other organizations?	
Are personal data received from other organizations?	
Do people provide their express authorization for their personal data to be dealt with?	
Are people informed about the rights related to their personal data?	

Please cite this article as: M.A. Martínez, et al., A Personal Data Audit Method through Requirements Engineering, Comput. Stand. Interfaces (2010), doi:10.1016/j.csi.2010.01.001

Questions related to logic/physical security controls in the Information Systems

Question	Yes/No/Number
Do user and password identification systems exist?	
Are the passwords sometimes changed?	
Are the passwords kept secret?	
Are there any information encryption systems?	
Are there any restricted physical access systems to the computers and/or servers?	

References

[1] R. Weber, EDP auditing: conceptual foundations and practice, in: M.G. Hill (Ed.), 2nd edition, 1988.
[2] ISO/IEC-7498-2, Information processing systems — Open Systems Interconnection — basic reference model — Part 2: security architecture, 1989.
[3] B. Thuraisingham, Privacy constraint processing in a privacy enhanced database management system, Data and Knowledge Engineering Journal 55 (2) (2005) 159–188.
[4] S. Kenny, Assuring data privacy compliance, Information Systems Control Journal 4 (2004).
[5] ISO/IEC-17799-27002, Information technologies — security techniques — code of practice for information security management, 2005.
[6] S.W. Smith, E.H. Spafford, Grand challenges in information security: process and output, IEEE Security & Privacy 2 (1) (2004) 69–71.
[7] Directive-95/46/CE, about People protection regarding the personal data management and the free circulation of these data, DOCE no. L281, 23/11/1995, 1995, pp. 0031–0050.
[8] IADP. Italy Authority of Data Protection 2009. http://www.garanteprivacy.it/garante/navig/jsp/index.jsp.
[9] ICO. British Authority of Data Protection 2009. http://www.informationcommissioner.gov.uk.
[10] Spanish-Constitutional-Law-15/1999, on Personal Data Protection, BOE no. 298, 14/12/1999, 1999, In Spanish.
[11] Spanish-Royal-Decree-994/1999, by means of which the security measures regulations of automated files which contain personal data is approved, BOE no. 151, 25/06/1999, 1999, p. 24241, In Spanish.
[12] D. Harris, L. Khan, R. Paul, B. Thuraisingham, Standards for secure data sharing across organizations, Computer Standards & Interfaces 29 (2007) 86–96.
[13] S. Robertson and J. Robertson, Mastering the Requirements Process, ed. Addison-Wesley. 1999.
[14] G. Kotonya, I. Sommerville, Requirements engineering. Processes and techniques, John Wiley & Sons, 1998.
[15] K.E. Wiegers, Software requirements, Microsoft Press, 1999.
[16] R. Crook, D. Ince, B. Nuseibeh, On modelling access policies: relating roles to their organisational context, Proc. 13th IEEE International Requirements Engineering Conference (RE'05), 2005, pp. 157–166.
[17] D. Mellado, E. Fernández-Medina, M. Piattini, A common criteria based security requirements engineering process for the development of secure information systems, Computer Standards and Interfaces 29 (2) (2007) 244–253.
[18] H. Mouratidis, P. Giorgini, G. Manson, When security meets software engineering: a case of modelling secure information systems, Information Systems 30 (8) (2005) 609–629.
[19] H. Mouratidis, P. Giorgini, Integrating security and software engineering: advances and future visions, Idea Group Publishing, 2007.
[20] C. Kalloniatis, E. Kavakli, S. Gritzalis, Addressing privacy requirements in system design: the PriS method, Requirements Engineering 13 (3) (2008) 241–255.
[21] A. Toval, J. Nicolás, B. Moros, F. García, Requirements reuse for improving information systems security: a practicioner's approach, Requirements Engineering Journal, vol. 6 (4), Springer, 2002, pp. 205–219.
[22] CobiT, IT Governance Institute, Control Objectives for Information and related Technology (v. 4.0), , 2005 http://www.isaca.org/cobit.htm.
[23] N.R. Mead, Identifying Security Requirements Using the Security Quality Requirements Engineering (SQUARE) method, integrating security and software engineering: advances and future visions, Idea Group Publishing, 2007.
[24] R.L. Baskerville, Investigating Information Systems with Action Research, Communications of the Association for Information Systems 2 (19) (1999).
[25] A. Toval, A. Olmos, M. Piattini, Legal requirements reuse: a critical success factor for requirements quality and personal data protection, IEEE Joint International Conference on Requirements Engineering (ICRE'02 and RE'02), (Essen, Germany), 2002, pp. 9–13.
[26] IEEE, Std 830-1998 Guide to Software Requirements Specifications (ANSI), Volume 4: Resource and Technique Standards, The Institute of Electrical and Electronics Engineers, Inc. IEEE Software Engineering Standards Collection, 1999.
[27] IEEE, Std 1233-1998 Guide for Developing System Requirements Specifications, Volume 1: Customer and Terminology Standards, The Institute of Electrical and Electronics Engineers, Inc. IEEE Software Engineering Standards Collection, 1999.
[28] OMG, Software Process Engineering Metamodel Specification (SPEM), Version 1.1, 2005 http://www.omg.org/cgi-bin/doc?formal/2005-01-06.
[29] AEPD. Spanish Agency of Data Protection 2009. http://www.agpd.es.
[30] ISACA. Information Systems Audit and Control Association 2009. http://www.isaca.org/.
[31] R. Dowie, A. Kennedy, Clinical audit in NHS acute and community trusts: a comparative analysis, British Journal of Clinical Governance 6 (2) (2001) 94–101.
[32] R. Hughes, Is audit research? The relationships between clinical audit and social research, International Journal of Health Care Quality Assurance 18 (4) (2005) 289–299.
[33] S. Lusignan, T. Chan, A. Theadom, N. Dhoul, The roles of policy and professionalism in the protection of processed clinical data: a literature review, International Journal of Medical Informatics 76 (4) (2006) 261–268.
[34] T. Rindfleisch, Privacy, information technology and health care, Communications of the ACM 40 (8) (1997) 92–100.
[35] M.V.d. Haak, A. Wolff, R. Brandner, P. Drings, M. Wannenmacher, Data security and protection in cross-institutional electronic patient records, International Journal of Medical Informatics 70 (2–3) (2003) 117–130.
[36] S. Kokolakis, C. Lambrinoudakis, ICT security standards for healthcare applications, The European Journal for the Informatics Professional 6 (4) (2005).
[37] F. Massacci, M. Prest, N. Zannone, Using a security requirements engineering methodology in practice: the compliance with the Italian data protection legislation, Computer Standards & Interfaces 27 (2005) 445–455.
[38] N. Greif, Software testing and preventive quality assurance for metrology, Computer Standards & Interfaces 28 (2006) 286–296.
[39] C.B. Haley, R. Laney, J.D. Moffet, B. Nuseibeh, Security requirements engineering: a framework for representation and analysis, IEEE Transactions Software Engineering 34 (1) (2008) 133–153.
[40] A. Zuccato, V. Endersz, N. Daniels, Security engineering at a telecom provider, Proc. 3rd International Conference on Availability, Reliability and Security (ARES'08), 2008, pp. 1139–1147.
[41] D.G. Firesmith, Engineering security requirements, Journal of Object Technology (JOT) 2 (1) (2003) 53–68.
[42] J. Nicolás, J. Lasheras, A. Toval, F.J. Ortiz, B. Alvarez, A collaborative learning experience in modelling the requirements of teleoperated systems for ship hull maintenance, Workshop on Learning Software Organizations and Requirements Engineering (LSO + RE 2006), (Hannover, Germany), 2006.
[43] ISO/IEC-9126-1, Software Engineering - Product Quality — Part1: Quality Model, 2001.
[44] Directive-2002/58/CE, relative to the processing of personal data and the protection of privacy in the electronic communications industry. (2002). Official Gazette of the European Union, L 201 of 31/7/2002.
[45] Regulation-45/2001/CE, 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, 2001.
[46] IMIA, Code of Ethics for Health Information Professionals, 2002 http://www.imia.org/code_of_ethics.html.

Miguel Angel Martinez Aguilar is a PhD student at the University of Murcia, in Spain. He received his degree in computer science from the University of Murcia. He is a member of the Software Engineering research group of the Department of Informatics and System (www.um.es/giisw) whose research manager is Professor Ambrosio Toval. His current research interests include requirements engineering, reuse, component-based software engineering and security. He is a member of the International Program Committee of ICEIS (International Conference on Enterprise Information Systems) since 2006. Currently, he also performs audits and implementations of the personal data protection system in different Spanish companies, as a collaborator member of the company ISOTADER Group.

Joaquín Lasheras Velasco is a PhD student at the University of Murcia, in Spain. He received his degree in computer science from the University of Murcia. He is a member of the Software Engineering research group of the Department of Informatics and System (www.um.es/giisw) whose research manager is Professor José Ambrosio Toval Álvarez. His current research interests include requirements engineering, reuse, ontologies and security. He is involved in a variety of applied research and development projects with industry and networks related to security and quality.

Eduardo Fernández-Medina holds a PhD and an MSc in Computer Science from the University of Sevilla. He is an Associate Professor at the Escuela Superior de Informática of the University of Castilla-La Mancha at Ciudad Real (Spain), his research activity being in the field of security in information systems, and particularly in security in business processes, databases, datawarehouses, and web services. Fernández-Medina is co-editor of several books and chapter books on these subjects, and has several dozens of papers in national and international conferences (BPM, UML, ER, ESORICS, TRUSTBUS, etc.). He is author of several manuscripts in national and international journals (Decision Support Systems, Information Systems, ACM Sigmod Record, Information Software Technology, Computers and Security, Computer Standards and Interfaces, etc.). He is a member of the Alarcos Research Group of the Department of Computer Science at the University of Castilla-La Mancha, in Ciudad Real, Spain, and he leads the subgroup of security in the Alarcos Research Group.

Please cite this article as: M.A. Martínez, et al., A Personal Data Audit Method through Requirements Engineering, Comput. Stand. Interfaces (2010), doi:10.1016/j.csi.2010.01.001

Ambrosio Toval Álvarez is a full professor at the University of Murcia, in Spain. He holds a BS in Mathematics from the University Complutense of Madrid, and received a PhD in Computer Science (cum laude) from the Technical University of Valencia (both in Spain). He is involved in a variety of applied research and development projects with industry and conducts research in the design and implementation of conceptual UML model verification, requirements engineering processes, computer-aided requirements engineering tools, and security requirements. Dr. Toval is currently the Head of the Software Engineering Research Group, at the University of Murcia.

Mario Piattini has an MSc and PhD in Computer Science from the Technical University of Madrid and is a CISA, CISM and CGEIT by ISACA (Information System Audit and Control Association) and CSQE by ASQ. He is a professor in the Department of Computer Science at the University of Castilla-La Mancha, in Ciudad Real, Spain. Author of several books and papers on software engineering, databases and information systems, he leads the ALARCOS Research Group of the Department of Information Systems and Technologies at the University of Castilla-La Mancha.

Please cite this article as: M.A. Martínez, et al., A Personal Data Audit Method through Requirements Engineering, Comput. Stand. Interfaces (2010), doi:10.1016/j.csi.2010.01.001