Computer Standards & Interfaces 32 (2010) 166–178

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 18 January 2010

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,