Semana de Engenharia 2010
Guimarães, 11 a 15 de Outubro

A Conceptual Framework to Manage and Audit Information Systems Security

Teresa Susana Mendes Pereira and Henrique Santos
Department of Information Systems
E-mail: tpereira@esce.ipvc.pt
hsantos@dsi.uminho.pt

KEYWORDS
Information security management , information system security, information system security auditing and ontology.

ABSTRACT

Auditing information systems security is difficult and is becomming crucial to ensure the daily operational activities of organizations as well as to promote competition and to create new business opportunities. A conceptual security framework to manage and audit information system security is the proposed research project, presented and discussed. The proposed framework is supported by a conceptual model approach, based on the ISO/IEC_JCT1 – *International Organization for Standardization/International Electrotechnical Commission, Joint Technical Committee* (ISO/IEC_JTC1 2005) security standards, and will produce a technological tool to assist organizations to better manage and audit their information systems security. This research work started by the analysis of the security stantards ISO/IEC_JTC1, followed by the identification and selection of the security concepts to be included in the conceptual model. Afterward those elements were hierarchically represented in an ontology and formalized through the use of the W3C standard language for modeling ontologies *Web Ontology Language* (OWL) (Smith et al. 2004). The developed of conceptual framework outlines the hierarchical structure of the security concepts, defined in the ontology. As a result of the research project is expected to demonstrate the effectiveness of a conceptual framework to improve organizations performance concerning the management and auditing of information system security.

INFORMATION SYSTEM SECURITY AUDIT

The rapid advances of the information and communication technologies, in particularly the Internet, and its increase use, have promoted the speed and accessibility of operations, resulting in significant changes in the way organizations and governments conduct their activities. Consequently organizations and governments become increasingly dependent on the availability, reliability and integrity of their information systems. However, the use of information technology brings significant risks to information systems and particularly to the critical resources, due to its own nature. Infrastructure elements such as telecommunications, power distributions, national defence, law enforcement, emergency service, as well the necessary resources to maintain the normal activity of an organization, are subject of these risks (Walker 2001). In addition natural disasters and inadvertent errors by authorized computer users can also compromise the organization activity, if the information resources are poorly protected. Organizations and governments, reinforce the need for a proper information security management model. Users must periodical evaluate the effectiveness of the implemented security controls or procedures, and assess or reassess the information security systems, in order to make the appropriate updates to the security policies. The inputs to this security management reviews are provided by the monitored events and audit trails, mostly provided by the information system itself (ISO/IEC_JTC1 2005).

In this context and in a more formal way, auditing the security of an information system involves the assessment of the security controls previously implemented by an organization, to ensure the confidentiality, integrity and availability of critical resources, involved in the daily activities of an organization. According to the guidelines presented on the ISO/IEC_JTC1 standards an organization should undertake regular audits to the information system security, to determine the effectiveness of controls and verify if the security requirements established have been accomplished. The audits results will enable to detect the existence of nonconformities on the information security system requirements, allowing to proceed with the necessary corrective and preventive actions.

Security audit operations can be performed in very different approaches, and the skills and "feelings" of the auditor plays a very important role concerning the time taken and the results achieved. Furthermore, most of the time an external expert team is required, which can be very intrusive and a source of delays. Under this assumptions it is demanded an agile and almost automatic process in such a way that a minimal security ware person can conduct. There are a few models or frameworks to support the security audit, most of the time based on more or less liberal interpretations of the security fundamental concepts (Onwubiko, 2009). Alternatively there are the Guidelines for information security management systems auditing, released in 2007 by ISO/IEC, the Information Security Audit and Control Association (ISACA) also provides security guidelines for security audit processes, and the ISO 17799 Checklist (AS/NZS 7799.2:2003 BS 7799.2:2002 2003) developed by SANS (System Administration, Networking and Security). These standards precisely define the main procedures, but are limited concerning

the strict relations or process flows necessary to undertake a security task, such as an audit. To address this lack, it is presented a framework to support the security audit of information systems security, based on a conceptual model.

CONCEPTUAL FRAMEWORK

The use of a conceptual model approach in the context of information systems security is a new perpective to model information. It allows the description of the data semantics and enables to firm up and unify the concepts and terminology defined in the information security domain, based on the ISO/IEC_JTC1 standards.

Research Question guiding the study

The goal of the research and the final thesis is to answer the key question of ***"A conceptual model based on hierarchical concepts structured in an ontology can improve Information System Security managementen and auditing?"*** The research question can be further clarified by the following sub-questions and the corresponding hypothesis presented in the Table 1.

Table 1 - Diagram of the deduction associated with the research methodology

Theme	Main/Central Question	Questions		Hypothesis
A Conceptual Framework to Manage and Audit Information Systems Security	A conceptual model based on hierarchical concepts structured in an ontology can improve Information System Security managementen and auditing	What is the impact of the rapid advances in technology and the new and competitive Internet-enabled services associated to speed and accessibility operations?	→	ITC advances introduce new competitive factors as well several risks. In response to these technological evolvement organizations change the way they conduct their activities, verifying an increasingly dependence on the availability, reliability and integrity of there IS.
		How can organizations response to the evolving information security requirements?	→	A proper information security management is fundamental to deal with more demanding information security requirements.
A Conceptual Framework to Manage and Audit Information Systems Security	A conceptual model based on hierarchical concepts structured in an ontology can improve Information System Security managementen and auditing	What are the impacts of using ontologies within information security domain?	→	Ontologies have been pointed as a strategic solution to deal with the continued growth of information. They are commonly used to formally represent knowledge in other areas.
		How can organizations perform a proper management of Information Systems Security?	→	The concepts and terminology in the information security domain are completely defined in the ISO/IEC_JTC1 security standards. A better utilization of those concepts passes through the definition of a conceptual structure of those semantic concepts.
		Are organizations able to identify their crucial assets/resources and their vulnerabilities and then be able to define a security strategy in order to be prepared to attacks, which may compromise the organization activity?	→	The definition of a framework based on ontologies is the most effective strategy for organizations to specify their assets and vulnerabilities, as well the threats and attacks (security policy!).
		How can organizations conduct an internal auditing to their Information Systems Security?	→	A conceptual framework assist the auditor to easily identify the assets, their vulnerabilities as well the threats and attacks the organizations are subject of.

This study is focused on producing a framework based on a conceptual model to assist the organizations to manage and audit their information systems security. Using this framework, organizations will be able to identify their valueable and critical assets, their vulnerabilities, as well the threats and attacks that exploit those vulnerabilities, and finally assess and/or reassess security procedures adopted. This framework empowers security managers to preventing and/or mitigating the materializations of attacks, threats and vulnerabilities, and improve security management.

The methodology followed in the development of the framework comprised several phases. The central phrase was the development of the conceptual model, with identification and definition of each concept and their relationships, and further their hierarchical representation in the ontology. As mentioned before, the conceptual approach concerning informations systems security was based on ISO standards. This is a new strategy and there aren't constructive research studies addressing this approach. This fact is specially related to the lack of a standard model to manage and audit information system security and by the fact that each

organization perform the information system security management accordingly to their own objectives, activities, structure and its particular view of risks. We will accomplish the proof of concept, through the instantiation of the conceptual framework within an organization.

Results of this study have both scientific and professional implications. The scientific contribution of this research is a new conceptual model with security concepts hierarchical structured in a ontology, in the context of information system security, a better understanding of the terminology and the semantic concepts in the security domain. The professional contribution of the research is the development of a technological framework to assist and support organizations to improve security management and audit as well as to promote its interoperability among different information security systems.

REFERENCES

Information Security Management, Part2: Specification for Information security management systems AS/NZS 7799.2:2003 BS 7799.2:2002 (2003), [on-line], SANS, http://www.sans.org/score/checklists/ISO_17799_checklist.pdf.

ISO/IEC FDIS 27000 Information technology – Security techniques – Information security management systems Overview and vocabulary, ISO copyright office. Geneva, Switzerland (2009).

ISO/IEC FDIS 27001 Information technology – Security techniques – Information security management systems – Requirements, ISO copyright office. Geneva, Switzerland (2005).

Onwubiko, C. (2009). A Security Audit Framework for security Management in the Enterprise. In *Global Security, Safety, and Sustainability: 5th International Conference, ICGS3 2009, London, UK, September 1-2, 2009*.

Walker, David M., Jones, Ronald L. (2001). Management Planning Guide for Information Systems Security Auditing, special publication of the National State Auditors Association and the U.S. General Accounting Office, December 10, 2001, [on-line]. Available from: http://www.gao.gov/special.pubs/mgmtpln.pdf.

Smith, Michael K., Welty, Chris, McGuinness, Deborah L.: OWL Web Ontology Language Guide, W3C Recommendation 10 February 2004. Technical report, W3C (2004), [on-line]. Available from: http://www.w3.org/TR/owl- guide/.