A Security Audit Framework to Manage Information System Security

Teresa Pereira[1] and Henrique Santos[2]

[1] Polytechnic Institute of Viana do Castelo
Superior School of Business Studies, Valença, Portugal
[2] University of Minho, School of Engineering
Information System Department, Guimares, Portugal
tpereira@esce.ipvc.pt, hsantos@dsi.uminho.pt
http://www.esce.ipvc.pt, http://www.dsi.uminho.pt

Abstract. The widespread adoption of information and communication technology have promoted an increase dependency of organizations in the performance of their Information Systems. As a result, adequate security procedures to properly manage information security must be established by the organizations, in order to protect their valued or critical resources from accidental or intentional attacks, and ensure their normal activity. A conceptual security framework to manage and audit Information System Security is proposed and discussed. The proposed framework intends to assist organizations firstly to understand what they precisely need to protect assets and what are their weaknesses (vulnerabilities), enabling to perform an adequate security management. Secondly, enabling a security audit framework to support the organization to assess the efficiency of the controls and policy adopted to prevent or mitigate attacks, threats and vulnerabilities, promoted by the advances of new technologies and new Internet-enabled services, that the organizations are subject of. The presented framework is based on a conceptual model approach, which contains the semantic description of the concepts defined in information security domain, based on the ISO/IEC_JCT1 standards.

Keywords: Information security management, information system security, audit information system, ontology and conceptual model.

1 Introduction

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 conduct their activities. Consequently organizations become increasingly dependent on the availability, reliability and integrity of their information systems to be competitive and create new business opportunities [5]. However, the use of information technology brings significant risks to information systems and particularly to the critical resources, due to its own nature. An increased number of sophisticated attacks are expected to evolve as wireless and others technologies transcend. This fact enforces the

S. Tenreiro de Magalhães, H. Jahankhani, and A.G. Hessami (Eds.): ICGS3 2010, CCIS 92, pp. 9–18, 2010.

need to ensure the security of the organizations information systems. In this context, it is crucial to perform a proper management of security, through a continuous identification of the main assets and their vulnerabilities, as well as the threats and attacks that they be subject of. One strategy to approach this goal is to perform regular information system security audits, to evaluate the performance of the security information management and analyze if the existing security practices needed to be reviewed. A security audit of an information system is conducted to assess the effectiveness of an organizations ability to protect its valued or critical assets [10]. This paper intends to present an investigated approach to improve security management through a conceptual framework developed to assist organizations to classify attacks, identify assets and mitigate their vulnerabilities and threats. The proposed framework is based on a conceptual model with capability to represent the semantic concepts and their relationships in the information security domain, defined accordingly to the established security standard ISO/IEC_JTC1[1] [8]. The paper is structured as follows: in the section 2 it will be presented an overview of security management concepts; in section 3 we briefly introduces the related work in information system security domain; section 4 presents the proposed conceptual model, which contains the semantic concepts specified in the information security domain, and their relationships, hierarchical structured in an ontology; section 5 presents the proposed framework to manage and audit information systems security, based on the ontology structure; conclusions and future work are presented in section 6.

2 Security Management

Managing information system security is increasingly concerning organizations, due to the continuous growing dependence of organizations on technology to conduct theirs businesses and to create a competitive advantage. Organizations rely significantly on technology, such as Internet, for businesses operations and secure business transactions [11]. Its recognized that since the last decade, the organizations are more dependent on the use of computer networks for their operations. Society as well as governments, depends on the use of computing services for their administration. Institutions depend on the effective use of computers and theirs communications for administrators to perform their daily operations, while the military requires secure communications to disseminate classified information. These fact turns computer networks a critical asset. However, beside computer network, organizations have others critical resources, accordingly to their structure, objectives and activities. This fact enforces the complexity of managing information system security for organization, due to the diversity of their assets and respective value, which requires to be properly protected [11]. Additionally, sophisticated attacks have been developed in order to exploit new vulnerabilities in the critical assets, when new technologies and new Internet-enabled services transcend. As a result, organizations need to evolve security management strategies in response to the evolving information security requirements. Nowadays, a properly security strategy demands for a rigorous process, similar to any

[1] International Organization for Standardization (ISO)/ International Electro technical Commission (IEC), Joint Technical Committee (JTC 1).

other business process, where every agent interacting with critical resources need to be aware and participate in security management, both adopting secure behaviors and continuous evaluating security control's performance [3]. The performance evaluation of regular information system security audit is one approach to evaluate the organizations information systems practices and operations. An auditing process will enable to obtain evidences whether the organizations information systems security policies, maintains the assets integrity, confidentiality and availability, and operating effectively and efficiently to achieve the organizations security objectives.

3 Related Work

Information system security auditing is a process that evolves with the security needs of the business activity of any organization [12]. Hence different approaches exist for conducting and managing security audits, to help the auditors to support a security auditing process. However most of the available models or frameworks to support the security audit are generally based on more or less liberal interpretations of the security fundamental concepts [10]. Lo and Marc-hand present a case study of security audit of a medium-size organization [9]. Their study focused exclusively on specific audit components, such as infrastructure, remote access and wireless LAN audits. Moreover Baharin et al., propose a third party security audit procedure that solely concentrates its study on a single data analyzer for security auditing, such as firewall log audit [1]. The ISO/IEC 15408 -Common Criteria (CC) introduce some models that relates threats and vulnerabilities, presenting security concepts and their relationships, in terms of organizations, safeguards, risks and assets [2]. However this model has some limitations, since it doesn't include the representation of the vulnerabilities in asset neither establish a relationship between the vulnerabilities to other security concepts that are essential in protecting assets, accordingly to the increasingly grow of attacks that exploit the assets vulnerabilities [12]. Notwithstanding its importance, the CCs model is more focused and useful in the evaluation of engineering products [12]. Farahmand et al. [4], propose a model to classify threats and evaluate the effectiveness of the associated controls, in order to identify possible outcomes of an attack. However the relationships to other security resources, such as vulnerabilities in assets are not fully covered [12]. Besides these contributions there are also available some guidelines for information security management systems auditing, such as the one released in 2007 by ISO/IEC[7]. The Information Security Audit and Control Association (ISACA[2]) also provides security guidelines for security audit processes, and SANS[3] (System Administration, Networking and Security) developed the ISO 17799 Checklist [6]. 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. In this paper it is proposed a unified conceptual framework to support auditors to conduct a proper audit within and organization and hence to improve a better management of information systems security.

[2] http://www.isaca.org/

[3] http://www.sans.org

4 Proposed Conceptual Model Developed in the Context of Information System

The proposed framework is based on a conceptual model represented by an ontology. The adoption of an ontology structure was considered to be an appropriate strategy to organize and structure the fundamental terminology and concepts involved in the security information domain. The defined concepts are based on a wide recognized standard, produced by ISO/IEC_JCT1. The study of attacks, threats and the assets' vulnerabilities in an information system continues to grow because it is evolving and has significantly impacts on an organization. Managing those concepts requires both a detailed understanding of security concepts and their relationships. Such understanding can assist organizations in implementing the right combination of protection controls to mitigate security risks related with the assets' vulnerabilities. The implementation of a conceptual model, richly represent security concepts and their relationships in terms of threats, attacks, vulnerabilities, assets and countermeasures [12]. The advantages of this approach to organizations are that enables them to: (1) properly identify the valued or critical assets; (2) properly identify the vulnerabilities of assets; (3) identify and mitigate potential threats; (4) evaluate the risks; (5) evaluate the efficiency and effectiveness of the security policies and safeguards defined and therefore analyze and implement the necessary adjustments to security policy adopted. The proposed framework, based on conceptual ontology with capabilities to jointly model attacks, threats and vulnerabilities resources, and their relationships to other security concepts, stands an important advance in managing information systems security. The defined conceptual model comprises 8 concepts and 16 relationships, based on the security standards ISO/IEC_JCT1 and was represented on an ontology structure, as illustrated in the figure 1. These concepts are described as following:

Incident – A single or series of unwanted or unexpected events that might have significant probability to compromise the information system security.

(Security) Event – An identified occurrence of a particular set of circum stances that changed the status of the information system security.

Asset – Any resource that has value and importance to the owner of the organization, which includes information, programs, network and communications infrastructures, software, operating systems, data and people.

CIA – The information properties to be ensured, namely: confidentiality, integrity and availability; besides these main security properties, and depending on the context, other security properties may need to the addressed, such as: authenticity, accountability and reliability.

Threat – Represents the types of dangers against a given set of properties (security properties). The attributes defined in this concept follow the Pfleeger approach (Pfleeger 2007), which include an attacker actions or position to perform an interception, fabrication, modification and interruption, over a resource.

Attack – A sequence of actions executed by some agent (automatic or manual) that explore any vulnerability and produce one or more se curity events.

Control – A mechanisms used to detect an incident or an event, to protect an asset and their security properties, to reduce a threat and to detect or prevent the effects of an attack.

Vulnerability – Represents any weakness of the system.

In short, the rational behind the ontology is structured as following: an incident is made from – *madeFromEven*t – events; the occurrence of an event can leadtoa lostof – *lostO*f – a set of security properties (CIA); an asset has security properties – *hasSecurityPropertie*s – and each one can be *affecte*d by a threat; on the other hand, a threat can *affec*t one or more security properties; and finally, an asset *ha*s vulnerabilities. A threat is *materialize*d by an attack, while the attacks *exploi*t one or more vulnerabilities; an attack is also triggered *towar*d an asset. Further, the implementation of control

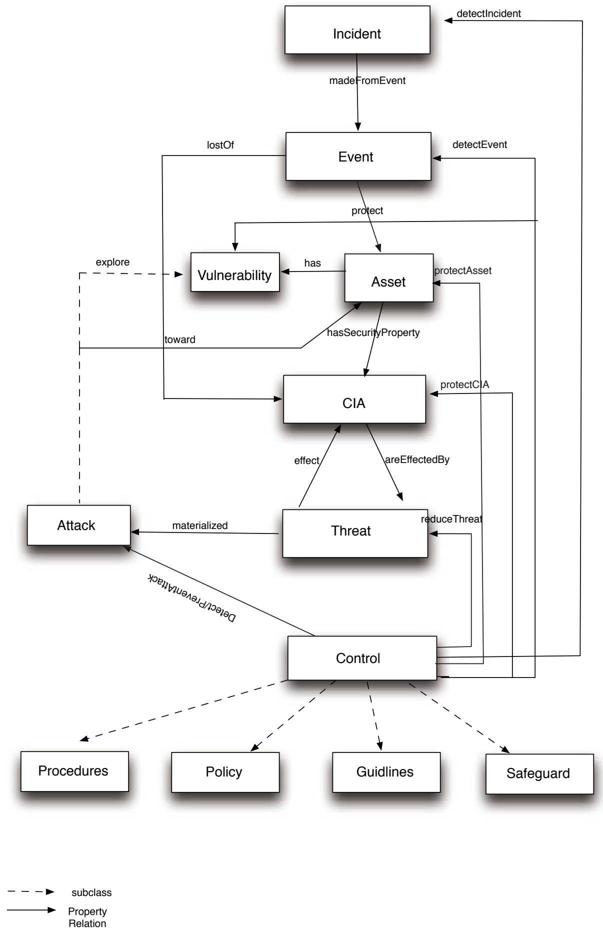


Fig. 1. Concepts and relationships defined in the conceptual framework

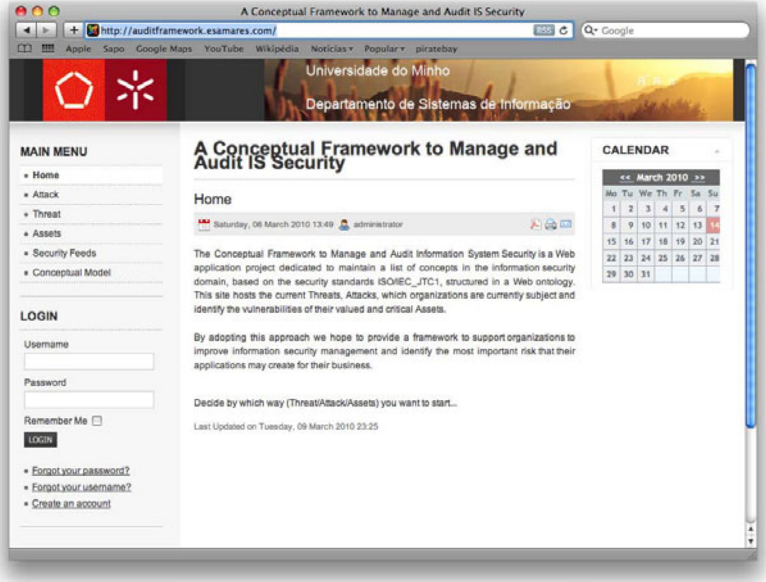
mechanisms, help to *reduc*e threats, to *detec*t and *preven*t an attack, to *protec*t security properties; to *protec*t assets and vulnerabilities, as well to *detec*t events, in order to *protec*t assets [13] . The description of those concepts and their relationships, presented in the ontology, was formalized through the use of the W3C standard language for modeling ontologies Web Ontology Language (OWL). This web language has been developed by the Web Ontology Working Group as a part of the W3C Semantic Web Activity [16]. In spite of OWL has not been designed to specifically express security issues, it was selected because it is a W3C recommendation since February of 2004 and due to its expressiveness with superior machine interpretability. The OWL is build upon Resource Description Framework (RDF) and Resource Description Framework Schema (RDFS). In fact the OWL vocabulary is an extension of RDF and uses RDF/XML syntax. The formalization of this ontology in OWL will be a step forward to promote its interoperability among different information security systems. In the next section, it will be presented the framework under proposal, which follows the hierarchical structure of the semantic concepts represented in the defined ontology, and try to provide an easy way to understand user interface so all users in an organization can participate in security auditing like tasks.

5 Proposed Framework to Manage and Audit Information System Security, Based on Ontology

The establishment of ISO/IEC_JTC1 standards promoted the standardization of the semantic concepts defined in the information security domain. The correct understanding and identification of those concepts are the primarily requirement to be considered in the performance of a proper examination of the information system security effectiveness, and further to identify and characterize an occurred security incident, as well as to estimate its impacts. The proposed conceptual framework intends to assists the organization, firstly to precisely determine what should be protected (the assets) and their weaknesses (vulnerabilities) involved in their daily activity. Secondly assess what vulnerabilities can be exploited by an attack, as well the threats that might be materialized in an attack. Finally, evaluate the efficiency and the effectiveness of the policy and controls implemented, in order to evaluate if they are being correctly implemented or if they need any adjustment [13]. Figure 2 illustrates the conceptual framework proposed, presenting these three nuclear concepts: attack, threat and assets. The auditor can select the concept from which he/she intends to start the auditing process, and proceed to the directed related concepts. Each concept contains a list of elements that are linked to the other concepts, conforming to the hierarchical structure of the semantic concepts, defined in the ontology. These three concepts were included in the front-end of the framework, rather the others, due to the nature of the audit operation, which the auditor intends to perform. Traditionally, a security audit is conducted once an incident has occurred (reactive followed by a corrective audit), that is when an asset has been compromised. In this case, an audit is requested in order to determine the source of the attack and how the incident happened, proceeding with the adequate corrective mechanisms. However a security audit is not only about investigating security break-ins, but rather to mitigate recognized threats, in order to ensure: (1) the security compliance; (2) the security of critical assets; (3) the right controls are in the right place. In this last view a security audit is performed in the context of the security risk management process, and aims to produce or evaluate a security policy. Being conducted by the main concepts and their relationships defined by an ontology, the proposed framework intends to assist organizations to understand, prepare and perform security audits, by themselves. This framework does not focus exclusively on technical controls involved with information security, but enforces procedures and practices to assist organizations to maintain consistently high levels of useful and good quality information concerning their information security systems.

Within the ontology, each concept is mapped to real subjects. For example a malicious code attack, as illustrated in the figure 3, includes a brief description of its main features, followed by the available connection/link to the affected assets, the vulnerability it explores, and the security properties that have been compromised, as illustrated in the figure 4. Despite the large amount of information available to complete a basic ontology, we accept that each organization will develop its one view of security awareness. The framework is modular concerning this aspect, allowing evolving the ontology by adding the relevant subjects. This way, the auditor may proceed through the examination of the relevant vulnerabilities in the assets that can compromise the security of the information system, within the organization; or the auditor may go along with the analyses of new threats that might be materialized in an attack.

Additionally, the proposed framework includes the typical functions of similar tools, enabling a set of functionalities, like the possibility of the auditor to generate a report with all steps performed, as well as the registration date of the audit. According to the results of the auditor examinations, he can also schedule the next audit. Moreover, if the auditor during his examination detects a new incident, i.e. an attack that is



A Conceptual Framework to Manage and Audit IS Security

Home

Saturday, 06 March 2010 13:49 administrator

The Conceptual Framework to Manage and Audit Information System Security is a Web application project dedicated to maintain a list of concepts in the information security domain, based on the security standards ISO/IEC_JTC1, structured in a Web ontology. This site hosts the current Threats, Attacks, which organizations are currently subject and identify the vulnerabilities of their valued and critical Assets.

By adopting this approach we hope to provide a framework to support organizations to improve information security management and identify the most important risk that their applications may create for their business.

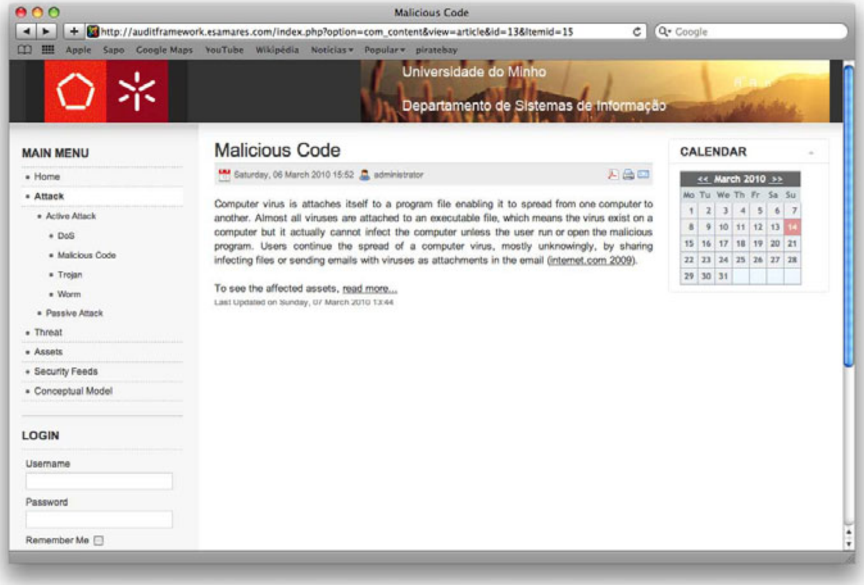
Decide by which way (Threat/Attack/Assets) you want to start...

Last Updated on Tuesday, 09 March 2010 23:25

<< March 2010 >>

Mo	Tu	We	Th	Fr	Sa	Su
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

Fig. 2. Print screen of the developed framework



Mo	Tu	We	Th	Fr	Sa	Su
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

Malicious Code

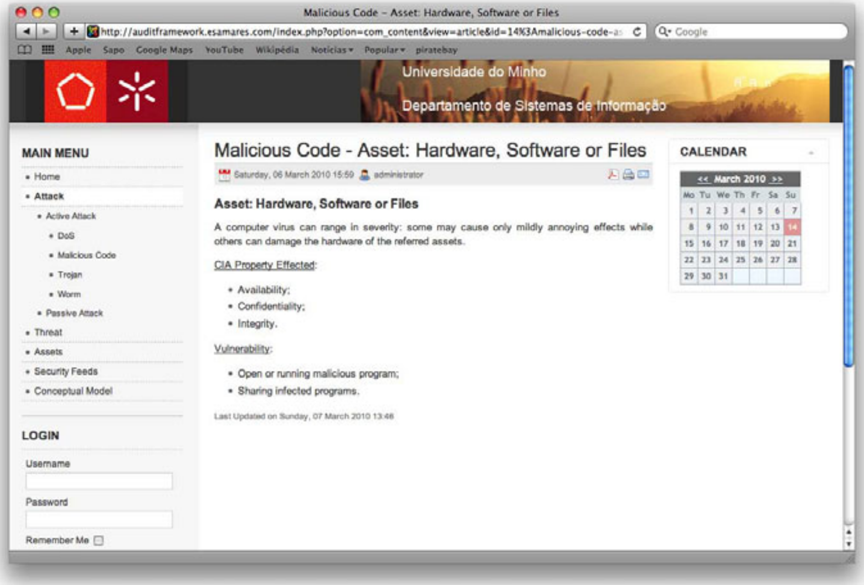
Saturday, 06 March 2010 15:52 administrator

Computer virus is attaches itself to a program file enabling it to spread from one computer to another. Almost all viruses are attached to an executable file, which means the virus exist on a computer but it actually cannot infect the computer unless the user run or open the malicious program. Users continue the spread of a computer virus, mostly unknowingly, by sharing infecting files or sending emails with viruses as attachments in the email (internet.com 2009).

To see the affected assets, read more...

Last Updated on Sunday, 07 March 2010 13:44

Fig. 3. Print screen of the developed framework


Malicious Code – Asset: Hardware, Software or Files
http://auditframework.esamares.com/index.php?option=com_content&view=article&id=14%3Amalicious-code-a
Google
Apple Sapo Google Maps YouTube Wikipédia Notícias ▾ Popular ▾ piratebay
Universidade do Minho
Departamento de Sistemas de Informação
MAIN MENU
Home
Attack
Active Attack
DoS
Malicious Code
Trojan
Worm
Passive Attack
Threat
Assets
Security Feeds
Conceptual Model
LOGIN
Username
Password
Remember Me □
CALENDAR
<< March 2010 >>

Mo	Tu	We	Th	Fr	Sa	Su
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

Malicious Code - Asset: Hardware, Software or Files

Saturday, 06 March 2010 15:59 administrator

Asset: Hardware, Software or Files

A computer virus can range in severity: some may cause only mildly annoying effects while others can damage the hardware of the referred assets.

CIA Property Effected:

- Availability;
- Confidentiality;
- Integrity.

Vulnerability:

- Open or running malicious program;
- Sharing infected programs.

Last Updated on Sunday, 07 March 2010 13:46

Fig. 4. Print screen of the assets affected by a Malicious Code attack with de security properties compromised and the vulnerabilities exploited by this attack

not presented on the list of attacks, the auditor should report this new attack with its features, which will be validated by the administrator of the framework and, after that, the administrator will index the attack to the list of attacks. This procedure is the same if the auditor decides to conduct the audit through the examination of the assets or threats and during the process identifies a new vulnerability in an asset or a new threat. The development of this framework is in a preliminary stage and it needs further improvements. However the concept of this framework is to assist the auditing process and promote improvements to the current methodologies available for information security management.

6 Conclusions and Future Work

Managing attacks and threats which the information system of the organizations are subject of, is increasingly difficult, due to the natural evolve of the attacks, threats and vulnerabilities, promoted by the advances of technology [5]. Auditing security information management is essential, and should not be performed only when an incident occurred, but also to assess if security controls and procedures are adequate and compliant with local or global regulations. The main contributions of this paper is a proposed framework based on a conceptual model approach, to support the auditor to primarily understand the business requirements in managing security of an organization, through the (1) exactly identification of the assets that needs to be protected; (2) identify and assess the vulnerabilities in the assets; (3) identify the potential threats that could be materialized in attacks; (4) evaluate the risks; (5) finally, assessment or reassessment of the policy and controls adopted. This solution introduces a new perspective to model information, in the security domain. Actually, a framework based on a conceptual model with capabilities to richly describe multiple security resources within an organization is an important advance, compared to the current models that typically address general purpose security issues. Besides the aforementioned advantage, its pertinent to highlight that it also promotes firming up and unifying the concepts and terminology defined in the scope of information security, based on the relevant ISO/IEC_JTC1 standards. Furthermore, it enables an organization evolving its own instantiation of the security ontology, obeying to standard concepts, but embedding its one view and assumed risk of exposition. As future work we intend to complete the implemented framework, introducing more elements to the concepts defined, as well as to implement the necessary adjustments to integrate further functionalities of the framework, e.g., direct link to attack and vulnerabilities description databases, alert mechanism for ontology outdate and continuous monitoring of security controls to promote early detection of security policies breaks.

References

1. Baharin, K.N., Md Din, N., Jamaludin, M., Md Tahir, N.: Third Party Security Audit Procedure for Network Environment. In: 4th National Conference on Telecommunication Technology, Shah Alam, Malaysia (2003)
2. Common Criteria for Information Technology Security Evaluation, Part I: Introduction and General Model, Version 3.1, Revision 1, CCMB-2006-09-001 (September 2006)

3. Da Veiga, A., Eloff, J.H.P.: An information security governance framework. Information Systems Management 24, 361–372 (2007)
4. Farahmand, F., Navathe, S.B., Sharp, G.P., Enslow, P.H.: Managing Vulnerabilities of Information System to Security Incidents. In: Proceedings of ICEC 2003, Pittsburg, PA. ACM, New York (2003) 1 58113-788-5/03/09.
5. Hayes, B.: Conducting a Security Audit: An Introductory Overview. Security Focus, `http://www.securityfocus.com/infocus/1697` (accessed January 2010)
6. Information Security Management, Part2: Specification for Information security management systems AS/NZS 7799.2:2003 BS 7799.2:2002. (2003) SANS, `http://www.sans.org/score/checklists/ISO_17799_checklist.pdf`
7. ISO/IEC FDIS 27000 Information technology – Security techniques – Information security management systems Overview and vocabulary. ISO copyright office, Geneva, Switzerland (2009)
8. ISO/IEC FDIS 27001 Information technology – Security techniques – Information security management systems – Requirements. ISO copyright office, Geneva, Switzerland (2005)
9. Lo, E.C., Marchand, M.: Security Audit: A Case Study. In: Proceedings of the CCECE, Niagara Falls, 0-7803-8253-6/04. IEEE, Los Alamitos (May 2004)
10. Onwubiko, C.: 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)
11. Onwubiko, C., Lenaghan, A.P.: Challenges and complexities of managing information security. Int. J. Electronic Security and Digital Forensic 2(3), 306–321 (2009)
12. Onwubiko, C., Lenaghan, A.P.: Managing Security Threats and Vulnerabilities for Small and Medium Enterprises. In: Proceeding of the 5th IEEE International Conference on Intelligence and Security Informatics, IEEE ISI 2007, New Brunswick, New Jersey, May 23-24 (2007)
13. Pereira, T., Santos, H.: An Ontology Based Approach To Information Security. In: Sartori, F., Sicilia, M.-A., Manouselis, N. (eds.) Communication in computer and Information Science, vol. XIII, 330 p. (2009) (Soft-cover); 3rd International Conference, Metadata and Semantics Research (MTSR 2009), Milan, Italy, September 30th -October, pp. 183–193. Springer, Heidelberg (2009) ISBN: 978-3642-04589-9
14. Pfleeger, C.P., Pfleeger, S.L.: Security in Computing, 4th edn. Prentice Hall PTR, Englewood Cliffs (2007)
15. Walker, D.M., Jones, R.L.: 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), `http://www.gao.gov/special.pubs/mgmtpln.pdf`
16. Smith, M.K., Welty, C., McGuinness, D.L.: OWL Web Ontology Language Guide, W3C Recommendation. Technical report, W3C (February 10, 2004), `http://www.w3.org/TR/owl-guide/`