feature

Information Systems Security Audit

An Ontological Framework

The advancement of information systems and technology offers a vital benefit for businesses. However, it also brings ever-increasing challenges due to the existence of hackers, malware, viruses, cybercrimes, etc. Therefore, frequent and strong follow-up is required via regular information systems security audits. Nevertheless, the scarcity of professionals and the lack of well-suited frameworks in this domain are frequently cited as main barriers to success. The main objective of this article is to propose a simple and applicable information system security auditing framework to support practitioners in order to minimize the professionals' requirements and simplify managers' involvement in the follow-up.

An information systems security audit (ISSA) is an independent review and examination of system records, activities and related documents. These audits are intended to improve the level of information security, avoid improper information security designs, and optimize the efficiency of the security safeguards and security processes.[1] The term "security framework" has been used in a variety of ways in security literature over the years, but in 2006, it came to be used as an aggregate term for the various documents, some pieces of software, and the variety of sources that give advice on topics related to information systems security, in particular, with regard to the planning, managing or auditing of overall information security practices for a given institution.[2]

Although security is a never-ending process that requires continued follow-up, it is still in its infancy. Also, security audit is an unexplored area and requires a simple framework to guide the process. Hence, the need for a study followed by this proposed generic framework that outlines the main information for security audit tasks and responsibilities of auditors from the beginning of a project.

Survey Study

The main source of empirical data in this study came from interviews; its structure was designed based on the Zachman Framework.[3] It is a framework for enterprise architecture that provides a formal and highly structured way of viewing and defining an enterprise with six-by-six matrices.[4] The six layers in the framework are planner, owner, designer, builder, subcontractor and functioning enterprise/ the system. This article focuses on the first layer, the planners view or the scope level, and the six-column interrogative questions,[5] which are:

- **What?**—Addresses data or assets
- **Why?**—Addresses motivation
- **How?**—Addresses function or processes
- **Who?**—Addresses people or organizations
- **Where?**—Addresses networks
- **When?**—Addresses time lines

The aim of the questions is to gather respondents' thoughts on these topics and identify the respondents' understanding of the security audit.

The planner's view or scope level describes the framework's vision, mission, context, boundaries, architecture and constraints for the security audit.[6]

Shemlse Gebremedhin Kassa, CISA, MSCS
Is a systems and IT auditor for United Bank S.C. and a security consultant for MASSK Consulting in Ethiopia. He has a multidisciplinary academic and practicum background in business and IT with more than 10 years of experience in accounting, budgeting, auditing, controlling and security consultancy in the banking and financial industries. Kassa is highly motivated and engaged in IT security projects and research, and he strives to update current systems and IT audit developments to keep up with the dynamically changing world and ever-increasing challenge of cybercrimes and hacking.

The Zachman Framework for enterprise architecture was used as a guide for conducting interviews with security experts and auditors to identify existing frameworks, framework components and thoughts on the subject. In addition to basic security concepts such as confidentiality, integrity and availability (CIA), and asset efficiency, effectiveness, reliability, compliance, accountability and authentication (E^2RCA^2), threats, vulnerability, risk and controls are presented in an ontological structure, which is formalized through the use of the World Wide Web (W3C) standard web ontology language (OWL)[7] for modeling. The developed security concepts on the ontology have been properly defined and related in a hierarchical base. Further, the overall ISSA activity is proposed to be performed using eight audit steps which are defined in the framework.

Proposed Ontological Framework

Ontology is a collection of concepts that represent higher-level knowledge in the knowledge hierarchy in a given organization.[8] An ontological structure helps us understand specific domains because the class hierarchy of ontology is similar to the way human beings store knowledge. Nowadays, ontology is widely used to describe a specific domain's knowledge and to achieve reusability and sharing of knowledge that can be communicated between humans and applications.[9] To make ontology available to information systems, various ontological languages have been developed and proposed for standardization. The most popular is OWL, which has been standardized by the W3C consortium[10] and has been adopted in this ontological structure. Concepts learned from the review of literature and the survey study led to the proposed ontology outlined in this article. The security ontology framework developed consists of three major levels (**figure 1**):

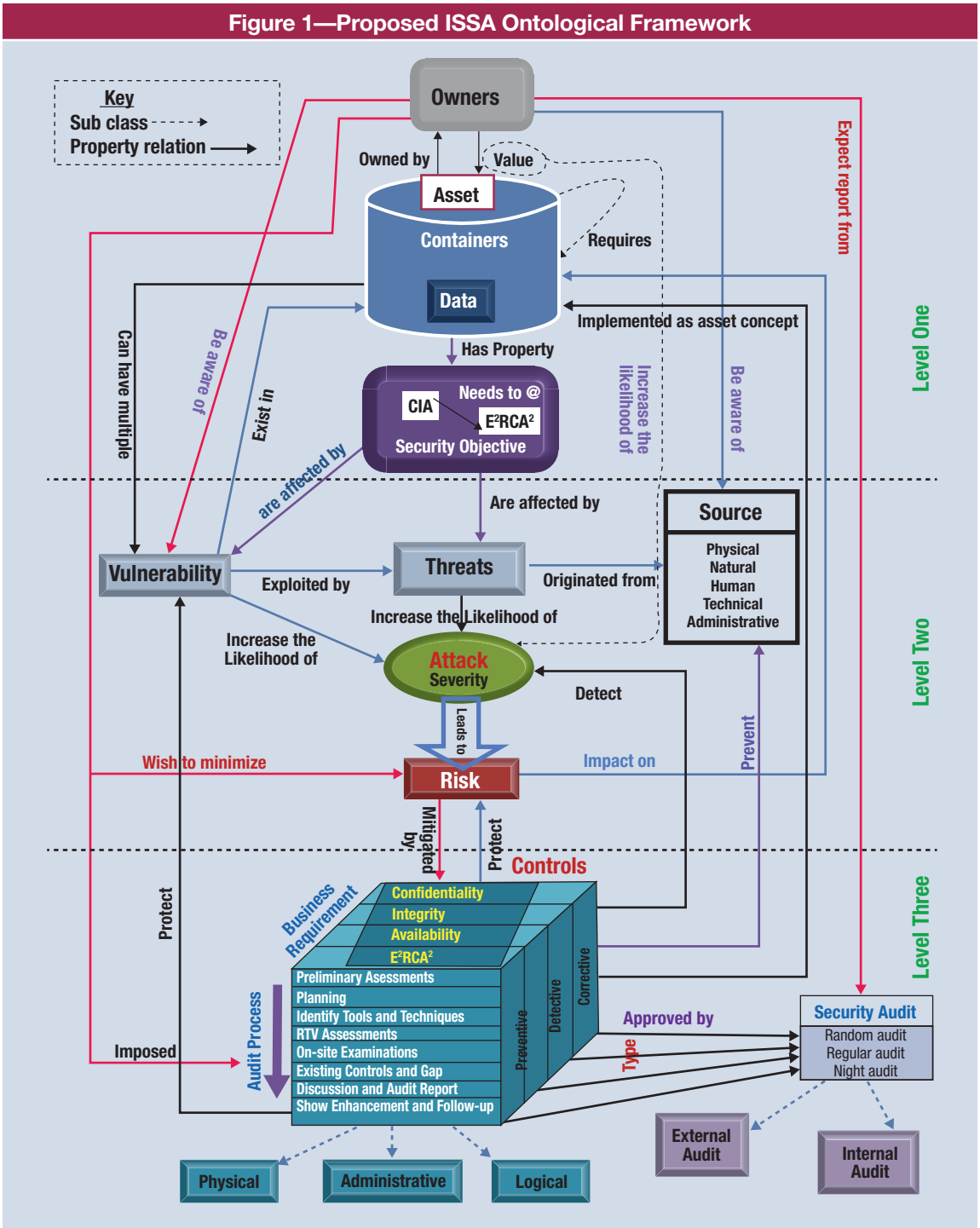
- **The first level illustrates the organization's assets and its security objective.** In this level, the auditor or the responsible organizational bodies is able to identify asset owned by the organization and their categorization, based on security objectives or assets properties of CIA and E^2RCA^2. This framework level does not require the involvement of experts to identify assets and the organization's security objective.
- **The second level of the framework depicts the measurements of severity of attack with the stated value of threats.** Vulnerabilities and the underlying risk analysis for the required assets are explicitly described. Therefore, this level requires some trained personnel and/or an auditor's involvement to perform the tasks effectively.
- **The third level of the ontology presents the required controls, which are shown as physical, administrative and logical controls for the business requirements (CIA and E^2RCA^2).** In addition, eight step-by-step security audit processes and audit types are presented. This level of the framework requires some expertise for better achievement of the security audit objective.

> **"Ontology is a collection of concepts that represent higher-level knowledge in the knowledge hierarchy in a given organization."**

Important Elements of the Proposed Framework

The underlying principle behind this ontology briefly describes the fundamental security concepts and their relationships. Therefore, the conceptual model defines 10 main concepts, 21 subconcepts and more than 20 relationships (**figure 1**). The main concepts are owner, asset, security objectives, vulnerability, threat, sources, attack, risk, control and security audit, but

Figure 1—Proposed ISSA Ontological Framework



Source: S. G. Kassa. Reprinted with permission.

the relationships among components are described based on these fundamental concepts:

- An asset is something of value owned by organizations or individuals. Some assets require another asset to be identifiable and useful. An asset has a set of security properties (CIA) and needs to address the additional properties of E^2RCA^2, the security objective affected by both vulnerabilities and threat sources, and threats originated from threat sources and exploited by vulnerabilities.
- Vulnerabilities and threats increase the likelihood of attack, and the higher the value of an asset, the more likely it is to be targeted by an attack. More severe threats and vulnerabilities make incidents of attack more severe, and more severe attacks lead to more substantial risk.
- This risk is mitigated by controls, which are administrative, logical and/or physical. Controls help mitigate risk, but to make the control of risk practical, proper security audit processes should be used (i.e., the eight audit steps).
- The existence of proper security should be checked and assured by internal and external security audits and controls and should have preventive, detective and corrective properties. Hence, security auditing is not a one-time task; it is a continuous process (regular or random).
- The implementation of control mechanisms helps to reduce threats, block the source of threats, protect security properties, protect vulnerabilities and keep assets safe by implementing different concepts to assess risk and detect attacks. Owners of an asset wish to minimize risk; therefore, they must be aware of the sources of threats and vulnerabilities. They then need to impose different control mechanisms to prevent threats from the source and/or detect breaches and mitigate damage after an attack has occurred.

Framework Components Defined

It is important to describe some of the terms and concepts used in the ontological structure presented.

- **Owner**—The person or entity that has been given formal responsibility for the security of an asset or asset category. This does not mean that the asset belongs to the owner in a legal sense. Asset owners are formally responsible for making sure that assets are secure while they are being developed, produced, maintained and used.[11]
- **Asset**—Any tangible or intangible resource that has value to the owner of the organization or entity,[12] such as information, data, software/applications, operating systems, hardware and people.
- **Data**—A collection of all financial and nonfinancial facts, records and information that is highly important to the operation of the organization. Data may be stored in any format and include customer transactions and financial, shareholder, employee and client information.

- **Containers**—The place where an information asset or data "lives" or any type of information asset (data) is stored, transported or processed.[13] Containers are categorized in four types:
  1. Systems and applications
  2. Hardware
  3. People
  4. Other containers
- **Security objective**—A statement of intent to counter specified threats and/or satisfy specified organizational security policies or assumptions.[14] It is also called asset properties or business requirements, which include CIA and E²RCA².
- **Vulnerability**—A flaw or weakness of an asset or group of assets that can be exploited by one or more threats. It is a weakness in the system that makes an attack more likely to succeed or a defect in a process, system, application or other asset that creates the potential for loss or harm.[15]
- **Threat**—An unwanted incident that may result in harm to a system or organization.
- **Sources**—Either intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability.[16] The sources or origins of threats/hazards include physical, natural, human, technical and administrative, among others.
- **Attack**—Any attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset. An attack should lead to a security incident, i.e., a security event that involves a security violation.[17]
- **Severity**—The level of harm that may occur as a result of exposure to or contact with a hazard. This may be referred to as the reasonably foreseeable worst-case injury.
- **Risk**—The likelihood of harm occurring, combined with the potential severity of an event, to produce a level of risk or risk rating.[18]
- **Control**—Any administrative, management, technical or legal method that is used to manage risk. Controls are safeguards or countermeasures. Controls include things such as practices, policies, procedures, programs, techniques, technologies, guidelines and organizational structures.[19]
- **Audit process**—A step-by-step procedure to achieve the security objective of an asset.

Achieving Security Objectives

Based on the results of the interviews with professionals conducted in preparation for this article, it can be concluded that, in order to achieve the required security objectives of an asset, the following eight steps are recommended.

Step 1: Preliminary Audit Assessment

In the first stage of the audit process, the auditor is responsible for assessing the current technological maturity level of a company. This stage is used to assess the current status of the company and helps identify the required time, cost and scope of an audit. To assess the company's maturity level, it is necessary to identify the status of the 12 minimum security requirements:[20]

1. Security policy and standards
2. Organizational security
3. Personnel security
4. Communication and operation management
5. Asset management
6. Physical and environmental security
7. Access control
8. IT systems development and maintenance
9. IT security incident management

10. Disaster recovery and business continuity management
11. Compliance
12. Risk management of that specific organization

Step 2: Planning

After proper assessment of the maturity level of a company, the auditor should plan to audit the company based on the information found in the first step. There are three main benefits of planning audits:

- It helps the auditor obtain sufficient and appropriate evidence for the circumstances.
- It helps predict audit costs at a reasonable level.
- It helps assign the proper manpower and time line.
- It helps avoid misunderstandings with clients.

Step 3: Identify Efficient Security Audit Tools and Techniques

Audit processes are supported by several computer-aided audit tools and techniques (CAATTs). The purpose of the overall audit tool identification is to develop an effective response to the risk. CAATTs can be defined as any use of technology to assist in the completion of an audit.[21] This broad definition includes using basic office productivity software such as spreadsheets, text editing programs, traditional word processing applications, automated working papers, and more advanced software packages that can be used by the auditor to perform audits and achieve the goals of auditing.[22]

Step 4: Threat, Vulnerability and Risk Assessments

At this stage of the audit, the auditor is responsible for extensively assessing the threat, vulnerability and risk (TVR) of each asset of the company and reaching some specific measure that shows the position of the company with regard to risk exposure. Risk management is an essential requirement of modern IT systems; it can be defined as a process of identifying risk, assessing risk and taking steps to reduce risk to an acceptable level, where risk is the net negative impact of the exercise of vulnerability, considering both the probability and the impact of occurrence. It is, therefore, necessary in an audit to understand that there is a payoff between the costs and the risk that is acceptable to management.[23]

Step 5: Identify Technical and Nontechnical Audit Tasks and On-site Examinations

Identifying technical and nontechnical audit tasks helps with assigning proper expertise to the specific case. On-site examination is the assessment of the company's business operations and the state of its property by examining securable IT assets and infrastructure based on its executed contracts. "The technical audit on-site investigations should include performing scans with various static audit tools. These tools gather a vast amount of information based on their pre-programmed functionality."[24] Physical audit evidence is generally more reliable than the representations of an individual.

> **"Auditing is a systematic independent examination of information systems, in a continuous search for compliance."**

Step 6: Identify Existing Controls and Gaps From the Required Controls

At this stage, the auditor assesses the existing controls for each asset and checks the gap from current status to the maximum possible security implementation stage. This reveals the remaining possible actions to minimize the identified risk of the company.

Step 7: Discussions With Responsible Bodies and Preparing Audit Reports

After the audit examination is completed, the audit findings and suggestions for corrective actions can be communicated to responsible stakeholders in a formal meeting. This ensures better understanding and support of the audit recommendations. It also gives the audited organization an opportunity to express its views on the issues raised. Writing a report after such a meeting and describing where agreements have been reached on all audit issues can greatly enhance audit effectiveness. Exit conferences also help finalize recommendations that are practical and feasible.[25]

Step 8: Show the Enhancements and Follow-up

This is the last and most critical phase of an audit. It recommends the possible enhancements or upgrades to the organization's control activity and the follow-up needed to check whether or not the enhancements are properly implemented.

Guidance for Implementation

The framework and its approach to quantitative implementation is illustrated, explained and measured based on concepts from ISO 27001 presented at the Implementers Forum in 2009[26] and empirical analysis results taken from interviews with professionals. Accordingly, the proposed framework is able to measure the following key elements of security audit implementation:

- Determining and evaluating the business information assets, containers and their categorization
- Identifying and evaluating vulnerability and threat levels of the information assets
- Determining the value of risk based on the severity of vulnerability and threats
- Measuring the impacts of risk based on the probability of occurrence
- Implementing risk mitigation techniques using various control strategies.

Conclusion

Auditing is a systematic independent examination of information systems, in a continuous search for compliance. Therefore, it requires a simple and applicable framework for use by professionals. Based on research conducted for this article, the author proposes an applicable framework for organizations' information systems security audits to help managers, auditors and stakeholders manage the security auditing process from beginning to end.

In an era in which professionals with appropriate expertise are scarce, it is important to find approaches that minimize their efforts while maximizing results. The proposed single, unified framework helps ensure effective management of the complete security audit process through a three-tiered method that supports the efficient allocation of labor.

Endnotes

1 Slade, R. M.; "Security Frameworks," University of British Columbia, Vancouver, Canada, *http://courses.ece.ubc.ca/412/previous_years/2008/sessions/guest_lectures/robert_slade_frameworks.pdf*
2 *Ibid*.
3 Zachman, J.; "John Zachman's Concise Definition of The Zachman Framework," Zachman International, 2008, *https://www.zachman.com/about-the-zachman-framework*
4 Ertaul, L.; R. Sudarsanam; "Security Planning Using Zachman Framework for Enterprises," *http://mgov.cn/lab/Archives/EuromGov2005/PDF/16_S039EL-S13.pdf*
5 *Ibid.*
6 *Op cit,* Slade
7 W3C Semantic Web, Web Ontology Language (OWL), *www.w3.org/2001/sw/wiki/OWL*

8 Gomes, H.; A. Zúquete; G. Paiva Dias; "An Overview of Security Ontology," Department of Electronics, Telecommunications and Informatics, University of Aveiro, Portugal, July 2010, *https://www.researchgate.net/publication/228692638_An_Overview_of_Security_Ontologies*

9 Studer, R.; V. R. Benjamins; D. Fensel; "Knowledge Engineering: Principles and Methods," *Data and Knowledge Engineering*, vol. 25, issue 1-2, March 1998, p. 161-197

10 Smith, M. K.; C. Welty; D. L. McGuinness; *OWL Web Ontology Language Guide*, *W3C Recommendation*, W3C, technical report, 10 February 2004, *www.w3.org/TR/owl-guide*

11 International Organization for Standardization, ISO 27001 *Information Security Management*, 2013, *www.iso.org/iso/home/standards/management-standards/iso27001.htm*, ISO 27002 *Information Technology—Security Techniques—Code of Practice for Information Security Controls*, 2013, *www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54533*

12 Praxiom Research Group Limited, "Archive of Plain English ISO 27001 2005 Definitions," 12 June 2006, *www.praxiom.com/iso-27001-definitions.htm*

13 Caralli, R., *et al*.; "Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process," Carnegie Mellon University, Pittsburgh, Pennsylvania, USA, May 2007, *www.sei.cmu.edu/reports/07tr012.pdf*

14 Citrix Systems, *Common Criteria Security Target for Citrix Xen Desktop 5.6 Platinum Edition*, Version 1-1, November 2012, *www.commoncriteriaportal.org/files/epfiles/ST271%20v1-1%20for%20Citrix%20XenDesktop%205.6.pdf*

15 *Op cit,* Praxiom Research Group Limited

16 National Institute of Standards and Technology, "Risk Management Guide for Information Technology Systems," USA, July 2002, *http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf*

17 International Organization for Standardization and the International Electrotechnical Commission, ISO/IEC 27000, *Information Technology—Security Techniques— Information Security Management Systems—Overview and Vocabulary*, 2009, *http://standards.iso.org/itff/Publicly Available Standards/CO41933_ISO_IEC_27000—2009.zip*

18 *Op cit,* Praxiom Research Group Limited

19 *Ibid*.

20 National Institute of Standards and Technology, "Minimum Security Requirements for Federal Information and Information Systems," FIPS PUB 200, USA, March 2006, *http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf*

21 Pedrosa, I.; C. Costa; "Computer Assisted Audit Tools and Techniques in Real World: CAATT's Applications and Approaches in Context," *International Journal of Computer Information Systems and Industrial Management Application*, vol. 4, 2012, p. 161-168, *www.mirlabs.org/ijcisim/regular_papers_2012/Paper18.pdf*

22 *Ibid.*

23 *Op cit*, NIST, "Risk Management Guide for Information Technology Systems"

24 ISACA®, "IT Standards, Guidelines, and Tools and Techniques for Audit and Assurance and Control Professionals," 1 March 2010, *www.isaca.org/knowledge-center/standards/documents/it-audit-assurance-guidance-1march2010.pdf*

25 The Institute of Internal Auditing, *Practice Advisories Under International Professional Practice Framework (IPPF)*, July 2011, *www.theiia.org/bookstore/downloads/freetomembers/0_2032.dl_pas.pdf*

26 Kamat, M.; "Matrices for Asset Valuation and Risk Analysis," ISO 27000 Implementers' Forum, 2009, *http://gseguridad.unicauca.edu.co/estandares/ISO27k-Matrices-for-Asset-Valuation-and-Risk-Analysis.pdf*