STANDARDS REVIEW ON MISSION OF MANAGEMENT INFORMATION SYSTEMS AUDIT

Delia BABEANU
Ph.D, Information System Supervisor, Lecturer,
Faculty of Accounting and Management Information Systems,
University of Economics, Bucharest, Romania

E-mail: delia@cig.ase.ro **Web page:** www.cig.ase.ro

Valerica MARES
Ph.D, Lecturer, Faculty of Accounting and Management Information Systems,
University of Economics, Bucharest, Romania

E-mail: maresvalerica@yahoo.com **Web page:** www.cig.ase.ro

Abstract: *The purpose of auditing is to verify that all hardware and software functions, automated processes, declared and published performance criteria are producing correct results, within the confines of system integrity, security measures and other control mechanisms, in accordance with functionality, originally envisaged, designed or modified.*

Key words: *standards for information systems audit; risks management; information security; IT governance*

Introduction

The scope of an information systems audit may be as far and wide to cover the entire lifecycle of the technology under scrutiny, including the correctness of computer calculations, or a basic test to verify compliance with a specific declared objective. The "scope" is of an audit is dependent on its declared objective, decided upon from the outset.

Audits may be initiated as a result of some concern over the management of assets. The concerned party may be a regulatory agency, an asset owner, or any stakeholder in the operation of the systems environment, including systems managers themselves. Each and every party may probably have an objective in initiating and commissioning the audit. Such an objective may be to validate the correctness of the systems performance or calculations, confirming that systems are appropriately accounted for as assets, to assess the operational integrity of a series of automated processes, to verify that confidential data is not compromised by being exposed to unauthorized persons, or it may even be a multifaceted combinations of the above mentioned aspects in addition to a wider ranging information systems issues of lesser or greater significance to an organisation, which by its very nature, may vary from one place to another. Selected various objectives of an audit will ultimately determine its scope.

The purpose of auditing is to verify if all hardware performances are used according to the software ones, at designed parameters. In order to achieve these normal working

parameters of computer networks have been defined as well as those peripheral devices.

It is important that the audit starts from the results of a previous audit of the company. The existing documents, created by a previous mission, should be analyzed, after which all the subsequent changes to the system will be verified. If these existing documents, as well as the documentation for further changes satisfy the need for information of the auditor, he will proceed to controlling the implementation of the changes.

The time period in which the audit takes place has to be well defined. Collecting samples is done using files that keep the history of the network, user rights, and hardware and software resources.

The audit of information systems is not different from other audits; it consists of the analysis of the systems referring to an activity of the company. In this sense, it is required to define information applications that represent an integrated set of programs, data and administrative procedures. Examples of such applications are: primary accounting applications, salary payment report applications, application for managing stocks, etc. The largest part of information applications are considered processes articulated around various stages like entries, processing, data storing and obtaining results (Nastase, 2007).

Standards presentation

The performed audit is based on current laws, standards and norms. One of these is standards **series 27000**. Standards that can be applied and are part of this series refer to:

The family of standards for SMSI – Information Security Management System (ISO27000 – ISO27010, http://www.iso27001security.com/html/27000.html) which covers the specifications of the system, measurements, an implementation guide, an audit guide and the management of risks.

The following are part of this category:

- **ISO 27000** – fundamental elements and vocabulary (completed at the end of 2008) which:
  - ✓ explain the terminology for all the series of standards 27000 (marketing)
  - ✓ explain basic principles and definitions that vary from one country to another
  - ✓ these principles will have an impact on other standards as COBIT (IT processes) and ITIL (Providing IT services – Service Delivery) and eliminates all confusions
- **ISO 27001** – requirements of a SMSI – Certification Process (is based on ISO 27002)
  - ✓ -certifying SMSI – published in November 2005 and operational on January 30 2006 (www.iso27001certificates.com);
  - ✓ -classification/improvement of the requirements of the PDCA process (http://27001.denialinfo.com/pdca.htm), which covers:
    - o -the scope of SMSI (figure 2), evaluating risks, selecting controls, appliance declaration, reviewing risks, SMSI internal audit, real results and measurements, plan for treating risks and controls
- **ISO 27002** – Good practice code for managing informational systems:
  - ✓ it has 11 sections which treat the protection of informational assets (it was published in April 2007)
  - ✓ -133 detailed controls (based on the process of evaluating risks and the business environment)

- ✓ -covers outsourcing purchasing and delivery services, current issues and management issues, security services at employment and during a contract of an employee, a guide for risk management and managing incidents, mobile remote or distributed communications,

- **ISO 27003** – SMSI Implementation Guide (will be available in 2009)
  - ✓ Implementing the guide that will provide support for the new requirements of the standard
    Annex B of BS7799 Standard - The second part has the following stages: overview, the responsibilities of the management, conformity with governance and rules, human resources and personnel security, managing assets, availability/continuity of business processes, managing informational incidents, access control, case studies for risk management (http://17799.standardsdirect.org/iso-17799.htm)
  - ✓ Implementing a PDCA implies identifying assets, identifying threats, evaluating and treating risks, analyzing and improving controls.
- **ISO 27004** Metrics and measurability of SMSI (at the end of 2008). The objectives of this standard are:
  - ✓ a real evaluation of SI controls and objectives
  - ✓ a real evaluation of a SMSI
  - ✓ offers indicators for management assistance
  - ✓ improving SI facilities
  - ✓ provides entries for SI audit
  - ✓ real communication at the information systems management level
  - ✓ input the process of risk management
  - ✓ output for internal comparisons and benchmarks (i.e. measuring controls and processes performance)

Figure 1. SMSI Planning stages

- **ISO 27005** SMSI risk management (end of 2008)
  - ✓ -a new risk management standard for information security
  - ✓ -risk analysis, evaluating risks from informational security (identifying assets, threats and vulnerabilities
  - ✓ -treating informational security risks (presented in figure 1)

    Annex a – goal

    Annex b – identifying and evaluating assets

    Annex c – common vulnerabilities (http://www.27001.com/catalog/7)

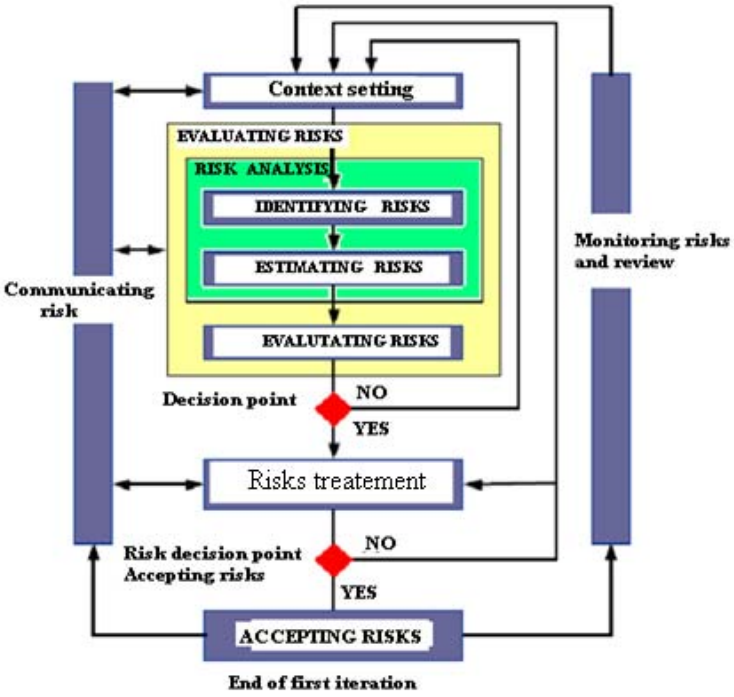

Figure 2. Risks treatment of information security
(**Source:** draft ISO 27005)

- **ISO 27006** – SMSI accreditation guide (certification contents)
  - ✓ necessary for increasing rigors and underlining the contents of certification which is required by the organization (business needs, communications and practice);
  - ✓ Operational from January 2007;
  - ✓ General requirements (impartiality guide);
  - ✓ Organizational structure applying ISO/IEC 17021;
  - ✓ Resource requirements: managerial competence, subcontracts;
  - ✓ Informational requirements – guiding certification results;
  - ✓ Process requirements – guiding SMSI audit.
- **ISO 27007** – SMSI auditing guide (from 2009)
  - ✓ Guide for auditing and SMI auditing content certification accreditation. This family of standards is represented in figure 3: Standards family applicable to a SMSI

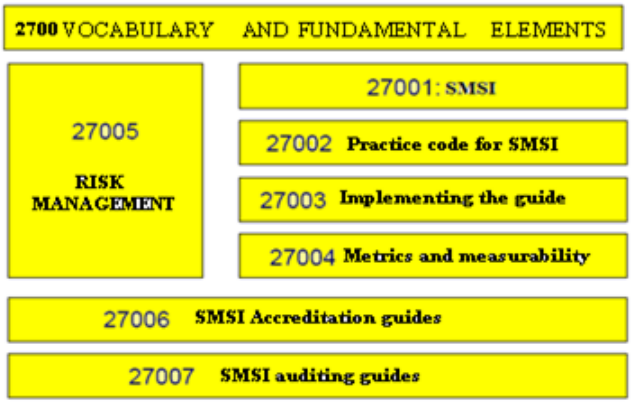

Figure 3. Standards family applicable to a SMSI

- ✓ Specific requirements for certain sectors of the economy (ISO 27011-ISO27030) – Telecom (global) ISO 27011, Health (UK) ISO 27799; Automotive (Germany; Korea; Sweden); Lottery at international level.
- ✓ Operational guide (ISO27031 – ISO27059) for which the publication date has not yet been decided. This series contains:
- ✓ -ISO 27031 ICT standard on business continuity
- ✓ -ISO 27032 cyber security
- ✓ -ISO 27033 - network security.
- ✓ -ISO 27034 - application security.

The pursued objectives can be found in the following table:

Table 1. Informational systems audit objectives

Major objectives	Implementing a good practice
	Evaluating existing or replaceable controls
	Configuring key points for information security
	Reducing frequency/impact of major incidents
Important objectives	Aligning to the internal security policy
	Integrating in the risk management program
	Identification of specific requirements for a certain activity domain
	Increasing existing investments
Other objectives	Increasing competition advantages
	Identification of requirements at the industrial branch level
	Answering a pressure by a third party
	Obtaining a minimum cost

Audit materiality, covered in S12 standard, consists of basic principles and essential procedures clearly identify, which are mandatory together with the guide for the elaboration of these procedures.

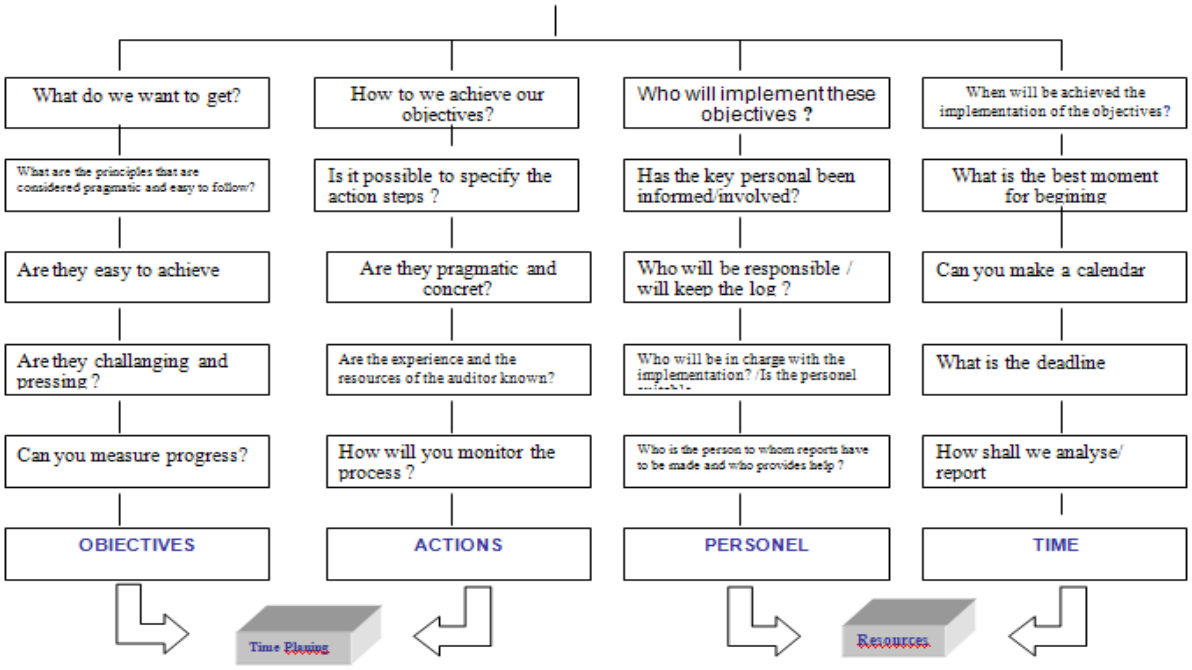

Figure 4. Strategic objectives of the audit
(Adapted for SIG after http://imm.protectiamuncii.ro and http://hwi.osha.europa.eu)

The relevance of materiality consists in the quality of information in a system which a society requires in order to publish all significant information. The materiality threshold is the one from which risks are important in evaluating a society.

This valuation can be done from a quantitative or qualitative point of view and in certain cases (an informational system permanently exposed to risks) a combination of the two methods.

The evaluation of the materiality is a judgment problem and includes considerations over the effect of organization's ability to achieve objectives in events like errors, omissions, irregularities or illegal acts which could substantially modify the results of the controls of threats in the audited area. When evaluating the materiality one has to take into account the errors accepted by the management, by the SI auditor, by the objectives assigned to the system or financial transactions processes, stored information, hardware, architecture and software, infrastructure network. Operating system, development and testing environment (www.isaca.org).

Examples of measures for evaluating the materiality:

- critical business processes supported by the system or applications (data acquiring, processing, reporting etc.)
- databases with critical information from the system or operations
- number and type of developed applications
- number of users that access the informational system
- number of managers, directors that work with classifies information according to their privileges
- critical network communication from within the system or operations
- system or operations cost (hardware, software, personnel, outsourced services, alone or in combinations)

- potential cost of errors (in terms of sales losses, lost guarantee, uncovered development costs, advertising cost required by guarantee, rectifying costs, health and safety, unnecessary production costs, etc)
- number of transactions requested over a period of time
- nature and quantity of manipulative materials
- requirements related to service contracts and costs of penalties
- Other penalties

Reporting materiality supposes determining findings, conclusions and recommendations that are to be reported. Weaknesses control should be considered materiality and reported if the absence of control causes errors in ensuring objectives controls.

Conclusion

Support information and processes, facilities, computer networks and the connection between them are the most important assets of a business. In order to manage these assets and to have business continuities, one has to implement SMSI standards in every company.

We propose transforming the components of the informational system and the information system in values and establishing a threshold for materiality based on value, computed in the respective national currency, which could be taken as the theory of materiality transformed in significance threshold, as is the case of the financial accounting audit.

References

1. Nastase, P., Eden, A., Nastase, F., Stanciu, V., Popescu, G., Gheorghe, M., Babeanu, D., Gavrila, A. and Boldeanu, D. **Auditul si controlul sistemelor informationale,** Ed. Economica, Bucharest, 2007, pp. 17-22
2. * * * http://www.isaca.org
3. * * * http://hwi.osha.europa.eu
4. * * * http://27001.denialinfo.com/pdca.htm
5. * * * http://www.iso27001security.com/html/27000.html
6. * * * http://www.27000.org/
7. * * * http://www.27001.com/catalog/7
8. * * * http://17799.standardsdirect.org/iso-17799.htm
9. * * * http://www.iso27001certificates.com