Audit Characteristics for Information System Security

Marius POPA, Bucharest, Romania, marius.popa@ase.ro
Mihai DOINEA, Bucharest, Romania, doinea_laurentiu@yahoo.com

The paper presents the main aspects regarding the development of the information security and assurance of their security. The information systems, standards and audit processes definitions are offered. There are presented the most important security standards used in information system security assessment.
Keywords: *audit, information system, security.*

Information Systems

The information systems are complex structures and they suppose the development of the following activities in order to accomplish them [IVAN05]:

- allocation of important financial resources;
- complex and stable team building formed by analysts, designers, code programmers and personnel;
- objective establishment;
- definition of a strategy for development, exploitation and maintenance;
- acquisition of equipments, tools necessary for processing, connections and external flow development;
- human resource training for a correct and efficient system use.

An information system is a system, automated or manual, that comprises people, machines, and/or methods organized to collect, process, transmit, and disseminate data that represent user information [WWW1].

Other statement defines the information system as any telecommunications and computer related equipment, interconnected system or subsystems of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice and/or data, and includes software, firmware, and hardware [FS1037].

In computer security, an information system is described by the following objects:

- repositories, which hold data permanent or temporarily;
- interfaces, which exchange information with the non-digital world;
- channels, which connect repositories;
- services, which provide value;
- messages, which carries a meaning.

The repositories, interfaces and channels represent the structure, and the services and messages represent the behavior of the information systems.

In [BAIC06], the information system is defined as a set of hardware and software components interconnected in networks, the organizational and administrative framework in which these components are working. The interconnection of these components is made on two levels:

- the physical one – it supposes the connection through different devices of the equipments in order to build the system;
- the functional one – it is made on the software level as to assure the system functionality through software modules collaboration.

The objective for the development and implementation of an information system is to process, to transfer and to store the information.

An information system includes hardware, software, information, data, applications, communications, and people. The information system security assurance assumes the development of engineering activities for information system security as follows:

- discovering the information protection needs;
- definition the system security requirements;
- design system security architecture;
- development the detailed security design;
- applying the system security;
- assessment the information protection effectiveness.

The aim of the information system security compliance is to assure protection of the physical and logical components and of the data stored in system towards the threats that exploit the vulnerabilities of the system.

2. Security Standards for Information Systems

The standards are developed by different organizations or groups of specialists for usage within the organization, by the specialists groups or organizations or by an entire industry. The objective for standard development is to assure the uniformity character of the different aspects measuring within organization, thus making comparative evaluations.

A standards organization is any entity whose primary activities are developing, coordinating, promulgating, revising, amending, reissuing, interpreting, or otherwise maintaining standards that address the interests of a wide base of users outside the standards development organization [WWW1].

There are some organizations that unintentionally acquired a status as the standards setter when a standard developed by them for internal use has become widely used and recognized as the de facto standard.

The information security has the origin in military information protection.

One of the most known security standards is Orange Book (Department of Defense Trusted Computer System Evaluation Criteria). That standard was replaced by the system FIPS – Federal Information Processing Strategy.

The standard BS7799 has been used since 1995 in Europe. It was adopted as international standard under the name ISO 17799. It contains common elements with the Orange Book, but being more flexible and adaptable to any organization. The standard has known successive improvements, the latest version being adopted in 2005. The ISO 17799:2005 standard structure contains 11 security controls. They are depicted in table no. 1.

As internal use, ISO 17799:2005 has the purpose of:

- measuring mean;
- control menu;
- to do objective;
- internal standard.

Table no. 1 Security controls in ISO 17799:2005

Security Control	Number of Security Category
Security Policy	1
Organizing Information Security	2
Asset Management	2
Human Resources Security	3
Physical and Environmental Security	2
Communications and Operations Management	10
Access Control	7
Information Systems Acquisition, Development and Maintenance	6
Information Security Incident Management	2
Business Continuity Management	1
Compliance	3

From the point of view of the organization's relationship with the business environment, the standard is:

- a reference point;
- a requirement for the partners;
- a part of a auction or an offer;
- a part of insurance document;
- a part of the service offered by a provider;
- external audit standard.

There are other security and audit standards for the information systems.

ISACA - Information Systems Audit and Control Association developed different audit specifications for information systems. The ISACA document contains the following auditing standards of the information systems [ISACA]:

- S1 – Audit Charter;
- S2 – Independence;
- S3 – Professional Ethics and Standards;
- S4 – Competence;
- S5 – Planning;
- S6 – Performance of Audit Work;
- S7 – Reporting;

- S8 – Follow-Up Activities;
- S9 – Irregularities and Illegal Acts;
- S10 – IT Governance;
- S11 – Use of Risk Assessment in Audit Planning;
- S12 – Audit Materiality;
- S13 – Using the Work of Other Experts;
- S14 – Audit Evidence.

The specifications from the mentioned standards are recognized at the global level as source for the assurance of the information system security and for the audit processes carrying on.

3. Information System Audit

The auditing of the informatics systems and economic information are branches of the general audit.

The literature includes the following concepts of the audit [CAPS06]:

- *Audit of Information Systems* – it aims the assessment of the information systems, the practices and operations regarding these ones;
- *Audit of Computer Information Systems* – it has the same significance with information system audit in an environment based on computer usage;
- *Computer Auditing* – it has many meanings: computer usage as instrument for auditing, audit in an environment based on computer usage or special investigations connected to financial audit.

The responsibility for prevention and detection of the inconsistency and frauds in an information system depends on the management staff. The latter has to be sure that this responsibility will be achieved through appliance of an adequate internal control system.

The internal control system represents the entire control system established by management staff in order to make the organization's processes orderly and efficiently. Thus, it assures the conformity of the management methods, the protection of the capital and the completeness and accuracy of the records.

The technical auditor assures the management staff that the planned controls are being made. In his activity, the technical auditor needs the standards and the procedures used to evaluate the system. I

Also, he is involved in solutions' elaboration and system design from the early stages of the system development.

The technical auditor has the following roles:

- taking into account all the functional risks;
- IT security audit;
- system audit and software application development.

The system security audit aims [IVAN05]:

- the management responsibility;
- the incompatible function segregation;
- the access control;
- the physical security control;
- the disaster effect prevention control.

The ISO 17799:2005 standard includes some specifications regarding the audit process for information system security assurance. Thus, the following guidelines should be observed [ISO17799]:

- audit requirements should be agreed with appropriate management;
- the scope of the checks should be agreed and controlled;
- the checks should be limited to read-only access to software and data;
- access other than read-only should only be allowed for isolated copies of system files, which should be erased or given appropriate protection;
- resources for performing the checks should be explicitly identified and made available;
- requirements for special or additional processing should be identified and agreed;
- all access should be monitored and logged to produce a reference trail;
- the use of time stamped reference;
- all procedures, requirements, and responsibilities should be documented;
- the person(s) carrying out the audit should be independent.

It is necessary to protect the access to information systems audit tools and to prevent the misusing or compromising of them. If the audit of the information system security is made by third party, it is necessary to take

into account the risks regarding the use of the audit tools by this third party.

4. Conclusions

The development of the audit processes in order to assess the security level of the information systems that are working in an organization is a very important aspect that must be taken into account.

The organizations are safe from the informational point of view they implement information systems in accordance with the security standards recognized as the best.

The audit processes establish the difference between the standard specifications and the reality from the organization. Also, some proposals regarding the information security improvement are made on the base of the audit process conclusions to the management staff of the organization.

References

[BAIC06], Floarea BAICU, Andrei Mihai BAICU – *Auditul şi securitatea sistemelor informatice*, Victor Printing House, Bucharest, 2006

[CANO06], Sergiu CAPISIZU, Gheorghe NOŞCA, Marius POPA – *Informatics Audit*, The symposium with international participation „The 37th International Scientific Symposium of METRA", Bucharest, May 25-26, 2006, „The 37th International Scientific Symposium of METRA", Bucharest, 2006

[CAPI06], Sergiu CAPISIZU, Gheorghe NOŞCA, Marius POPA – *The Informatics Audit – Basic Concepts*, International Workshop „Information Systems & Operations Management", Romanian-American University, Bucharest, March 1-2, 2006, „Information Systems & Operations Management", 2006, Universul Juridic Publishing House Bucharest, pp. 350 – 357

[CAPS06], Sergiu CAPISIZU – *Modele şi tehnici de realizare a auditului informaţiei economice*, ASE Bucharest, 2006, PhD Thesis

[FS1037], Federal Standard 1037C

[ISACA], Information Systems Audit and Control Association – IS Standards, Guidelines and Procedures for Auditing and Control Professionals, 7th of September, 2006

[ISO17799], ISO 17799:2005 Standard

[IVAN05], Ion IVAN, Gheorghe NOŞCA, Sergiu CAPISIZU – *Auditul sistemelor informatice*, ASE Printing House, Bucharest, 2005

[WWW1], www.wikipedia.org