Information Systems Security Audit

❖❖ GHEORGHE POPESCU ❖❖
❖❖ VERONICA ADRIANA POPESCU ❖❖
❖❖ CRISTINA RALUCA POPESCU ❖❖

Abstract: The article covers:

- *Defining an information system; benefits obtained by introducing new information technologies; IT management;*
- *Defining prerequisites, analysis, design, implementation of IS;*
- *Information security management system; aspects regarding IS security policy;*
- *Conceptual model of a security system;*
- *Auditing information security systems and network infrastructure security.*

Key words: Information system, information technologies, IT security, basic regulations, standards, norms, automat data processing systems' audit, informational systems' audit, information security management system, IS security policies, firewall.

1. Information Systems – Development, Audit, Security Policies

An ***information system*** (IS) represents a set of human and capital resources, invested within an entity for the purpose of collecting and processing the necessary data in order to produce information, which can then be used throughout all management decisional levels and in controlling the organization's activity.

In the Anglo-American literature, although the distinction is made between "information system" and "computer based information system", due to the technological level reached by USA, all authors after making the said difference, use the term "infor -

mation system", motivating such by the high level of informational activities automation.

Most benefits are obtained in a business by introducing the new **information technologies** (IT). In the case of a IS project, the benefits are not obtained immediately, but throughout the project's life cycle. Along with the business case study, upon the beginning of a project for designing a IS, planning must be performed of the benefits' achievement, which must be then followed-up by means of an efficient management process, which includes:

- Validating the benefits presented in the business;
- Planning the benefits to be achieved;
- Describing the benefits, measuring the outcome and the objective;
- Researching assumptions;
- Setting up key responsibilities for achieving the benefits.

The benefits achievement management is an important component of project management, also involving the project's sponsors.

IS Development is an extremely complex activity. Actual production, consisting in drafting, testing and optimizing the programs, as well as the rules for using such, must be preceded by designing a project, that must establish the necessary details for defining the procedures, however not before establishing which are the necessary programs and in what global cooperation framework (in what environment) will they function. The project design cannot be made without knowing the information prerequisites which the system must meet. All these have already shaped a set of activities to be fulfilled: ***defining the prerequisites, analysis, design, creating the IS***.

Information systems' audit *represents a complex activity for assessing an information system in order to set forth a qualified opinion regarding the conformity between the system and the regulating standards, as well as over the information system's capacity of achieving the organization's strategic objectives, by efficiently using the informational resources and by ensuring the integrity of the processed and stored data.*

Usually, such activity must be carried out by a competent person, trained and qualified in the field of information systems' control, security and management, person who is named "IS auditor". Such sort of licensing is granted by **ISACA**, by means of the **CISA** (*Certified Information System Auditor*).

Under such circumstances, **IT security** implies implementing specific IT environment protective measures (computers, networks, information systems, and data bases) both against accidental damaging actions, and against intended attacks, such as espionage, sabotage, murder etc. Taking into consideration the said risks, in 2000 the International Standardization Organization (ISO) adopted as international standard the **British Standard BS 7799**, by publishing it under the name of ISO 17799 – ***"Practical Code for Information Security Management"***.

The said **Standard** allow for 36 control objectives and 127 control elements to be identified, grouped in ten categories:

1. security policy;
2. continuous business planning;
3. controlling the access to the system;
4. system development and maintenance;
5. physical and environmental security;

6. conformity;
7. personnel security;
8. organization security;
9. computers and network management;
10. information resources classification and control.

In order for the **ISO 17799** standard to become operational, the creation was necessary of the **BS 7799-2** standard. Its advantage lays in the fact that it allows for an information security management system to be implementing by successively fulfilling the following phases:

a) defining the information security management system and afferent policies;
b) setting out responsibilities and necessary resources;
c) assets specification and risk management;
d) risk administration;
e) controls selection;
f) applicability;
g) implementation.

According to this standard, the **IT Governance Institute** functioning under the wing of **ISACA**, provides ***the best practices*** for the IT processes by the **"COBIT"** paper – ***"Control Objectives for Information and related Technology"***. **COBIT** structures the IT processes into four areas:

a) planning and organization;
b) acquisition and implementation;
c) functioning and support;
d) monitoring and evaluation.

In reality, these four areas include 220 controls, classified into 34 high level objectives.

The **security policy**, central part of the security plan implies research and rigorous informing before applying own controls to the IT environment. The security policy comprises the description of purposes and intents, representing a difficult process imposing for adaptation to each organization's specific features. A first step in implementing the security plan is represented by establishing the systems, applications, data and entities to be securitized. Once the security policy is clearly defined, it is mandatory for the users to be trained.

A well defined security policy must exactly specify aspects regarding:

- organization's security related objectives, which implies that the data protection must be ensured against information leaking towards external entities, data protection against natural calamities, ensuring data integrity or ensuring business continuity;
- the personnel designated to ensure security, which can be represented by a small working group, a management group or by each employee;
- the whole organization's involvement in ensuring security, exactly establishing who will provide training on security matters, as well as the modality in which the security aspects are to be integrated in the organizational structure.

In order to achieve security objectives and obtaining a high protection level, the security plan should be developed and implemented on levels. Thus, the conceptual model of a security system will include the following levels:

- ***application security***, first of all implying the security of the software products which can be used in order to develop business applications, such as web servers, SSL (*Secure Sockets Layer*) etc.;

- ***system security***, implemented on the level of system commands, and which will control all software functions of the system. The users are identified and authenticated on a system level by a single security mechanism, for all operations they might perform on the system;
- ***network security***, integrant part in designing such, including controls by fire - walls, VPN (*Virtual Private Network*) and *gateways*;
- ***physical security***, aiming for systems protection, backup devices and supports, including access controls, uninterruptible power supplies, redundant communication lines;
- ***organization security***, responsible for all aspects of the organization's security plan, incorporating security policies, taking into consideration the training in the field of security, organization's business systems, and also the planning for recovering in case of disaster.

It is mandatory for the security plan to establish a working framework for making specific decisions such as deciding upon the defense mechanisms to be used, and consequently on the modality of configuring the provided services. It must be mentioned that planning a security system and managing vulnerabilities are activities implying compromises and successive optimizations. The conclusion can be drawn that planning security measures can be also defined as the art of reaching a compromise between the relative value of the information, the cost for protecting such and the probability for them to be attacked.

The main security objectives, defined like such by the prerequisites of any business environment, are:

- **confidentiality** – assumes preventing unauthorized access to information. By con - fidentiality it is ensured that the information, either in transit or stored, is accessible only to entities which are authorized to access those resources;
- **integrity** – information is protected from losses or modification is unauthorized; by using adequate procedures and methods, by means of the integrity it is ensured that information, either in transit or stored, cannot be modified;
- **availability** – it ensures that authorized entities have access to information re - sources only when they need them; for in - stance, preventing DoS (Denial of Service) attacks;
- **conformity** – with applicable laws, regulations and standards.

Obviously, implementing an information security management system provides numerous **advantages**, amongst which we mention:

- gaining the trust of business partners (either suppliers or clients);
- improving prevention systems and response systems in case of incidents;
- minimizing the risk for information theft, corruption or loss;
- safely accessing information (by employees and customers);
- justifying and optimizing costs necessary in order to implement security control;
- proving the management's involve - ment in and commitment to information security;
- proving the conformity between own security practices and recognized standards;
- compliance with legal prerequisites, regulations and local regulations;
- ensuring that risks and controls are permanently revised;
- business continuity.

At the present moment, the **audit and evaluation tools** are expressly focused on those basic aspects of information systems and networks, without paying enough attention to the problems existing in organizations, namely the applied policy and procedures, or human aspects, calling for adequate management, culture, and knowledge. It is not surprising or inevitably that such are factors the influence of which can prove dramatic for information infrastructures' security.

2. Information Systems' Security Audit

Information systems' security audit implies both physic access audit and logic access audit. Moreover, specific techniques must be used (aiming to test the security) and investigation techniques. Consequently, **phases** are fulfilled, such as:

- reanalyzing the entity's specific policies, procedures and standards;
- security policies regarding physical access;
- security policies regarding logic access;
- awareness and permanent training of the users on security policies;
- establishing the data owners and users;
- establishing the data in custody;
- establishing the security administrator;
- defining new users;
- establishing former employees' access;
- establishing authorization procedures for accessing documents;
- establishing basic security measures, implying: defining the working environment, antivirus software to be used, access passwords for every level, the way in which backups are going to be made, vulnerabilities definition, minimizing services that can be provided by the service, modality of patching the system, involved IT personnel;
- standard access.

Logic access audit implies:

- determining those security risks regarding transactions processing;
- evaluating controls regarding system access paths;
- evaluating the control environment in order to establish to what extent that control's objectives are achieved by the test results;
- evaluating the security environment, by revising the used policies, practices and procedures.

Obviously, in order to obtain a clear situation of the environment's security and of risks evaluation, the logic access audit needs first of all good knowledge of the IT environment. In this respect, a determinant element is represented by the researching of the access paths, and more exactly establishing the logic way for each individual user towards information. Also, the access to the system's components, for an efficient control, imposes most times the use of specialists in this field. They can provide data regarding system's security, and that is why they are regarded as a valuable source for the auditor. Consequently, the **auditor** is entitled to request an interview with those specialists, hence determining to what extent the managerial policies are vulnerable, or to what extent the logic security and confidentiality are complied with in that particular entity. Also, there must not be neglected by the auditor the analysis reports regarding the control of access to software, nor the analysis applications of manual system operations.

The techniques used by the auditor in testing the security are different. Some of them involve:

- keys and card verification;
- terminal identification;
- users identification and authentication;
- resources control;
- entering the working session and reporting unauthorized access;
- investigating unauthorized access;
- uncontrolled security and compensation controls;
- access controls analysis and passwords administration.

Techniques investigation also involves investigating the evidences' protection, the modality of custody obtaining, and the existence of crime in computer networks.

3. Auditing Network Infrastructure Security

Controls regarding network infrastructure security audit involve verification by the auditor of the network architecture's identification, determining the efficiency of applying security policies, determining the used standards and procedures, identifying the personnel in charge with network security, reanalyzing the network administration procedures, in case vulnerabilities are noticed. In this respect, auditing involves the audit of distance access, the audit of the points where the computers network interacts with the internet.

Combining these procedures can be found in the so-called penetration tests *or* of network intrusion. These tests are of many kinds, depending on their purpose, objective and nature, such as: external tests (simulating attacks and external controls, an access way being the internet), internal tests (similar to the external ones: intranet), "blind" tests (that test is limited or has no information regarding the system) and double "blind" tests, of particular purpose.

The phases of the penetration tests are: planning, revealing, attack and reporting. In the penetration testing there are taken into consideration the network evaluation analysis, the LAN network evaluation, the development and authorization of network changes, and authorized changes.

4. Security Measures in the Entity – Client Relationship

Security of commercial transactions

The matter of security concerns the client, the network, the information site of the company trading its products or services on the internet. The risks arising on the client's behalf are closely connected to disclosing confidential information, and also to unlawful use. The security issues on a network level are concretized in terms of performances represented by the response time, data traffic etc. An important risk that can be faced by the entity is that regarding the information environment penetration from the very internet site, finding authorization solutions in all possibilities of using such.

Buyer-seller connection security

Ensuring trading transactions security is not only a matter of security of the internet connection between the customer and the seller, but it is equally a matter of the client service. The client's information environment should be different than the seller's informa-

tion environment. An internet connection between a browser and a web server can be established by using the logic SSL module (*Secure Sockets Layer*). SSL is integrated into the browser and ensures confidentiality.

The main credit card operators promote SET (*Secure Electronic Transaction*). In this case, the transaction and client's credit card number are enciphered by the application and it is only then that they are sent to the seller. The seller, in its turn will reimburse its identification number and message returning figure before being sent to the bank. Upon receipt, the bank will decode, authenticate and identify the user, in the same time delivering its agreement to the seller which in its turn will perform the requested transaction or not. At no moment during the transaction will the credit card be made public or will the seller be identifiable.

Server securitizing

Securitizing the server involves controlling the requests addressed to such and securitizing the information system to which it collaborates in order to return the service requested by the customers. Grounded on the strict system configuration, its protection against the exterior is usually made by a ***firewall***. A ***firewall*** configuration is made by the security criteria established for filtering the covered traffic and thus a control policy is applied over the system access. Therefore, data protection consists of limiting access to such, as well as of placing them to the disposal of authorized clients.

In this respect businesses can also use companies that are specialized in creating data securitizing models or even specialized experts in this field. Nonetheless, network administrators will not be able to implement and maintain the functionality of the designed plan. Organizations must ensure material and financial conditions in order to train their own network administrators, thus avoiding unpredicted situations.

In reality, there will never be possible for an information system to be totally securitized, because hackers will always discover security vulnerabilities you couldn't think of, which they will use in order to break the system. Depending on the hackers' purpose, they will affect the system or they will only attract the attention over the respective "fissures". In time, the organization's information system evolves and expands by new hardware and software components. Along with the system's evolution, other vulnerabilities will also appear for which new securitizing solutions should be developed.

In **conclusion**, we can assert that only by permanently investing into a complex security model we will be able to have safer IT systems. Therefore, the security solutions and also the security policy should be considered globally, and not just punctually. There must not be neglected the fact that the security level of the entire system is represented by its weakest link, and that is why the security policy should be updated periodically.

REFERENCES:

1. **Oprea, Dumitru,** *Analysis and Design of Economic Information Systems* (Romanian: *Analiza şi proiectarea sistemelor informaţionale economice*), Polirom Publishing House 1999.

2. **Ivan I., Roşca Gh., Capisizu S.**, *Information Systems Audit* (Romanian: *Auditul sistemelor informatice*), ASE Publishing House, Bucharest, 2005.

3. **Munteanu, A,** *Accountancy Information Systems' Audit* (Romanian: *Auditul sistemelor informationale contabile*), Polirom Publishing House, Iasi, 2001.

4**. Nastase P., Ali E., Nastase F., Stanciu V., Popescu Gh., Gheorghe M., Băbeanu D., Boldeanu D., Gavrila Al**., *Information Systems' Audit and Control* (Romanian: *Auditul si controlul sistemelor informationale*), Economica Publishing House, Bucharest, 2007.

5. **Popescu, Gheorghe,** *Internal Control Proceedings and Financial Audit* (Romanian: *Procedurile controlului intern si auditul financiar*), Gestiunea Publishing House, Bucharest, 1997.

6. **Popescu, Veronica,** *Expert Systems for Auditing Management Information Systems* (Romanian: *Sisteme expert pentru auditarea sistemelor informatice de gestiune*), Gestiunea Publishing House, Bucharest, 2006.

7. www.isaca.org

8. http://cco.cisco.com