Characteristics for Development of an Assessment System for Security Audit Processes

Marius POPA
Academy of Economic Studies, Bucharest, Romania
Department of Computer Science in Economics
marius.popa@ase.ro

The paper highlights some aspects regarding the auditing issues of security for distributed informatics systems, identifying the conceptual framework for conducting of IT&C audit processes, identifying the characteristics of quality and security of distributed informatics systems, the principles and standards that underpin the assessment of quality for systems that are in operation and those under development stage. Also, the paper presents some aspects regarding techniques used to build assessment systems for evaluation processes, in general, and audit processes of the distributed informatics systems, in particular. Parts of the building process for assessment system are highlighted.

Keywords: audit process, quantitative assessment, informatics security

1 Characteristics of the Distributed Informatics Systems

A *system* represents a set of dependent elements forming a single unitary entity. A particular type of system is the *economic* one, which defines economic components and mechanisms such as a company, an industry, a field of the national economy and so on. Even the national and worldwide economies can be seen at a global economic level as being complex economic systems [9].

An economic system receives an *input* of production factors. This input is processed and an *output* is provided in the form of products and services provided to the market. The accurate transformation of the *input* into *output* is made by a *feedback loop*, figure 1.

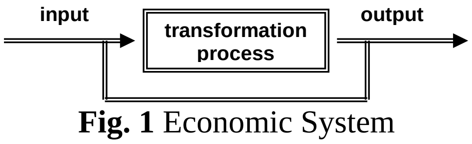

Fig. 1 Economic System

The transformation process takes place into a dynamic way that makes the system to progress according with to a specific route. The state of the system describes the system degree of evolution.

A system can be defined by the following elements: inputs, outputs, transformation process and system structure and its state.

An informatics system utilizes automatic methods and means for data collecting, transmission, storage and processing for information capitalization in the organization management process [8].

The information system resides in all the informational flows and circuits and all the methods, techniques used to process the data needed by the decision system. The informatics system is the middle layer between the decision and information systems and the communication between these layers is made in all possible directions. Also, it records, processes and transmits the information from the operating system to the decision one [8].

A distributed informatics system is a component of the informational system. This kind of information system collects, processes, transmits, stores and presents data by using computing systems. Also, it is responsible for automatic processing of the data by using various methods and techniques.

The resources involved by an information technology system can be divided into the following groups [8]:

- Activity: it is subject of the system and the primary data from inside;
- Methods and techniques: they are used to develop the IT system;
- Hardware: it is implicated in collecting,

processing, transmitting, storing and presenting the final results;

- Software applications: they are responsible for the efficient use of the hardware resources by finding the solutions for the specific problems;
- Human resources: they are very important for the health of the system.

A system is called distributed because its components are placed in different logical and physical locations.

In [1], the informatics 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:

- Physical level: it supposes the connection through different devices of the equipments in order to build the system;
- Functional level: 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 informatics system is to process, to transfer and to store the information.

The informatics systems evolved as new technologies were developed. Therefore, new categories of informatics systems appeared and some examples are [12]:

- Transaction processing systems: they automate the handling of data about business activities or transactions;
- Management information systems: they are subsets of the overall internal controls of a business to accomplish specific goals or objectives;
- Decision support systems: they include knowledge-based systems that support decision-making activities;
- Expert systems: they are software products that attempts to reproduce the performance of one or more human experts;
- Business intelligence: it refers to skills, technologies, applications and practices used to help a business acquire understanding of its business context.

In computer security, informatics system is described by the following objects [8]:

- 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 informatics systems.

An informatics system includes hardware, software, information, data, applications, communications, and people. The security assurance of the informatics systems assumes the development of engineering activities for informatics system security as follows [10]:

- 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.

In [7] it is highlighted a framework for security assurance. The main activities in security assurance are:

- Risk assessment: the vulnerabilities and their potential impacts are determined;
- Vulnerability management and remediation: the flaws are identified and fixed;
- Security standards for development and deployment: introduction of vulnerabilities is prevented;
- Ongoing assessment and assurance: monitoring and auditing by management level.

The expansion of the informatics systems to the Internet environment introduced new risk levels in their exploitation. Such risks affect the customers trust and successful business operation. Therefore, the informatics system monitoring and auditing must be done to assure the minimum level of trust in business operations.

2 Issues for Development of an Assessment System used in Security Audit Processes

To measure is the most important need for IT&C auditors. The measurement concerns the component, module or product. Depending on the audit purpose, the measurement concerns different aspects established in audit plan. For instance, if the purpose of the audit is security of informatics system, then measurement means to evaluate the security of the components, modules or products [11].

The assessment system is based on metrics. The metrics allow organization to create policies, set standards specify acceptance criteria, compare the results across modules or components. In addition, the metrics allow management to be more efficient in implementation of the security policies [11].

The metrics are used to assess informatics systems:

- Qualitative: the measurement scale has discreet units: very good, good, satisfactory, poor, very poor;
- Quantitative: the assessment is a very precise one and it is a numerical one.
- The metrics computed in an audit process can be classified in the following classes:
- Primary metrics: they are computed in a single audit process, within department/module/component and they aim the primary characteristics of the audited informatics system;
- Aggregated metrics: they are the results of many audit processes, multiple applications or aggregation operations of the primary metrics.

The metrics include models, indicators and their properties and ways of evaluation and validation.

The stages to determine the values of the indicators associated to the characteristics of the distributed informatics systems are [3]:

- Selection of the characteristics in relation to distributed informatics systems that are numerically quantified;
- Quantification of the fundamental characteristics of the distributed informatics systems;
- Primary processing of the gathered data;
- Grouping the obtained information;
- Aggregation of the individual data.

On assessment system, the management obtains information regarding the quality of the informatics system used within organization, the monitoring and measurement compliance with procedures, the efficacy of decisions applied before the last audit process, the trend of the organization driven by IT&C audit process, the allocation more effective of the resources by the managers.

Development of an assessment system used in security audit processes must take into consideration the following characteristics:

- Informatics system architectures: hardware/software components/modules;
- Lifecycle of the informatics systems: development stages;
- Security assurance procedures: security policies, encryption/decryption algorithms, information security management etc;
- Security standards and best practices: rules established by specialists to assure a minimum accepted quality;
- Audit quality: controls must meet minimum requirements.

The assessment system must quantify the vulnerabilities and risks of the informatics system security. For instance, the metrics for a web application must quantify the risks regarding: invalidated sources of input, use of invalidated input, invalidated output streams, flawed authorization and access control, flawed authorization and session management, native code and buffer overflows, dynamic code, weak encryption, application configuration, denial of service, network communications, unsupported application interfaces, improper administrative and exception handling

The assessment system for lifecycle of the informatics system must evaluate the defective specification, design and implementation.

During lifecycle, developers unknowingly inject defects that produce software with security lacks. Implementation of some development practices and security expertise of the development team produces security software. In addition, the assessment system for lifecycle of the informatics system has the goal to evaluate the confidentiality, integrity and availability. Another aim of this kind of assessment is to verify if developers use the process consistently and accurately [13].

The development process of the distributed informatics systems is kept under control through some characteristics quantified by metrics regarding: effectiveness, efficiency, confidentiality, integrity availability, compliance and reliability.

The performance and capability of the IT processes are determines and monitoring by benchmarking, goals and metrics. These assessment methods are used to define and measure the outcome and performance of the IT processes.

The assessment system for security audit is developed both to obtain information from controlled system during the security audit process and to evaluate if the controlled system is according with the legal and quality requirements.

The security improvement of the distributed informatics systems is made on assessment system based on metrics. The metrics provide a view of the results and performances.

The CobiT is a framework that ties the businesses requirements for information and governance to the objectives of the IT services function [6].

In CobiT, the metrics are defined at the following levels:

- How to measure them the business expects from IT;
- How to measure the IT processes that support IT's objectives;
- How to measure the needs insight the process to achieve the required performance.

The two types of metrics defined in CobiT 4.1 are [6]:

- Outcome measures: indicate whether the goals have been met; these can be implemented after the fact;
- Performance indicators: indicate whether goals are likely to be met; these can be implemented before the outcome is clear.

The possible outcome measures are [6]:

- Number of incidents causing public embarrassment;
- Number of actual IT incidents with business impact;
- Number of actual incidents because of un authorized access;
- Frequency of review of the type of security events to be monitored.

Also, the developed metrics must meet the following characteristics [6]:

- A high insight-to-effort ratio;
- Comparable internally;
- Comparable externally;
- Good metrics vs. low-quality metrics;
- Easy to measure.

In [2] it is provided the development process and requirements that must be met by an assessment system.

3 Techniques Used to Build an Assessment System for Security Audit Processes

The assessment system for security audit processes increases the degree of the automatic evaluation for audit processes.

In accordance to [4], the building process of an assessment system must follow the below stages:

- Defining the objective indicators that can be measured in a distributed informatics system;
- Establishing the methodology to record the objective indicators and database building of the distributed informatics system;
- Development of the models in which the objective indicators are independent variables and the result variable will emphasize the qualities of the audited distributed informatics system;
- Assessment of the result variable for given values of the independent variables extracted from database;
- Classification of the informatics system in a class established in accordance to

audit criteria;

- Recording the further behavior of the distributed informatics system and comparing its behavior with the experimental values of the metrics; if the behavior of the informatics system is anticipated by metric then the metric is validated.

The metrics of the audit processes are defined on the characteristics of the distributed informatics systems. In an audit process, there are many issues that cannot be automatically quantified by metrics. So, the auditors' experience, competence and skills are very important to reach to correct conclusions.

If the hypothesis regarding the building and using the metrics are carefully defined then the metrics are consistent and they are used by the most part of the auditors in audit processes. Also, another strong reason to use a metric is given by its using costs. The costs are represented by finances, human resources and time.

During the audit process of an informatics system, the most frequent operations are controls, assessment and testing the informational means as it follows [1]:

- Identification and assessment of the risks in the system;
- Assessment and testing the control in the system;
- Control and physical assessment of the informational behavior;
- Control and assessment of the informatics system management;
- Control and assessment of the informatics applications;
- Control and assessment of the security for computer networks;
- Control and assessment of the plan and procedures for disaster recovery and business continuity;
- Testing the data integrity.

The development process of an assessment system for security audit processes must consider the above directions in which the audit process must be carried out.

Assessment system for security audit processes is developed to reduce the subjectivity introduced by auditor in audit process. The assessment system is based on metrics that must be validated before their using. The metric validation is made depending on characteristics and in accordance with requirements.

To assess a metric, it must consider all factors of influence. The model associated to a metric has a list of independent variables. The structure of this list is given by factors of influence and the relations among the factors of influence.

In [3], some kinds of metrics are identified:

- Metrics with direct factors of influence;
- Metrics with indirect factors of influence.

The graph of direct influence for the factors F_i, i = 1, 2, …, n is depicted in figure 2 [5].

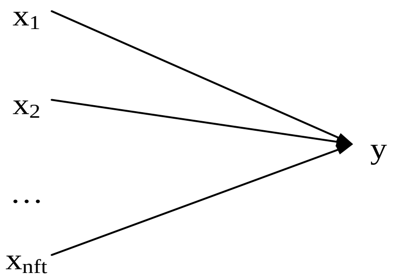

Fig. 2. Graph of direct influence

The x_i, i = 1, 2, …, n are values associated to the factors F_i, i = 1, 2, …, n. The associated model is [3]:

$y = a_1 x_1 + a_2 x_2 + \ldots + a_n x_n$

The indirect influences are emphasized in the figure 3 [3].

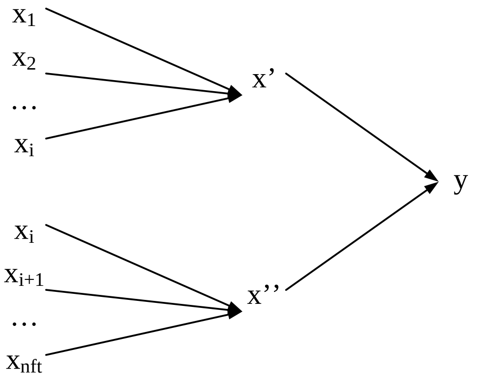

Fig. 3. Graph of indirect influences

The associated model for indirect influences is:

$$y = a_1 x' + a_2 x''$$

Because:

$$x' = a_1 x_1 + a_2 x_2 + \dots + a_i x_i$$
$$x'' = b_1 x_{i+1} + b_2 x_{i+2} + \dots + b_{n-i} x_n$$

the model associated to y after the substitutions is:

$$y = a_1 x_1 + a_2 x_2 + \dots + a_i x_i + b_1 x_{i+1} + b_2 x_{i+2} + \dots + b_{n-1} x_n$$

In the above example, the relations between the factors of influence and result variable are linear. In real world, the relations are not linear because the complexity of the phenomena and processes is very high [3].

In [5], elements considered to build metrics are presented:

- Identifying the factors of influences;
- Intensity measurement between each factor and result variable y;
- Representation of the dependence graph;
- Selection of the factors with significant influence;
- Identifying the analytical form of the dependences;
- Execution of statistical tests to select the factors of influence.
- Metrics used in audit processes have the following functions in accordance with [2]:
- Measurement: object of the audit process is emphasized as value; also, elements of the audit process are emphasized as values;
- Comparison: similarities and differences between audit processes are emphasized in order to establish the quality class of the audited informatics system;
- Analysis: characteristics of the distributed informatics systems are highlighted;
- Synthesis: extraction what it is essential for a distributed informatics system;
- Estimation: possible future evolutions of the behavior for distributed informatics systems are established;
- Verification: supposes validation of the mathematical models associated to the metrics.

In [3], quality characteristics of the metrics are presented and they are:

- Completeness: is a quality characteristics of the metrics in relation to number of factors of influence taken into account and result variables which the indicators were build for; lists of factors and indicators are reduced when data series have identical or proportional values;
- Stability: a metric is stable when the resulted values are not over a threshold value for different data series; stability is given by the following factors: size of data series, value precision, number of data series and threshold value;
- Continuity: building a new metric supposes studying the existing metrics, identifying the used factors, knowledge about independent and result variables; a new metric contains factors and parts of models taken over from the old metrics;
- Generality: a metric meets this quality characteristic when it accepts any data series and the result is in expected value domain of the results; for two different distributed informatics systems a metric is general when the results are different;
- Representativeness: is obtained if:
    - Effort of the data gathering is reduced;
    - Analytical forms of the indicators are simple;
    - Separated nature of the sub-intervals and correspondence between them;
- Sensitivity: emphases the way in which the metric responds to the variations recorded between data series; sensitivity highlights variations of the result variables when independent variables vary; it is a very important characteristic in validation process of the metrics;
- Non-catastrophic character and non-compensatory character: they highlight the cases when the metric does not output a value because data series are particular; In [2], some examples of particular input

data for non-catastrophic character are presented:

- Denominator is null;
- Null or negative values of the logarithmic function;
- Square root of negative values;

The non-compensatory character aims the effects of the simultaneous variations for independent variables on result variables; to validate this characteristic, it is necessary to mark variation of the result variable when there are variations of the independent variations.

Identifying the properties of the mathematical models associated to the metrics represents a critical activity in building process of the assessment system for audit processes [3].

Validation of the metrics is the process to verify if the metrics meet requirements and associated properties.

In [3], two validation techniques are presented:

- Experimental validation: three cases regarding the quality of a metric are highlighted:
  - Metric meets all properties and implementation requirements;
  - Metric meets partially properties and implementation requirements;
  - Metric does not accomplished the established requirements and it is rejected;

  A metric is classified in one of three above classes; if the metric is classified in the second class then the validation process of this one is continued until the metric is classified in class one or three;
- Structural validation: takes into account the elements included in mathematical models associated to the metrics; the elements considered in building process of the assessment system based on metric system are [3]:
  - Lot of factors of influence for characteristic to be measured;
  - Ways to quantify factors of influence;
  - Lot of distributed informatics systems that some characteristics are assessed for;

Work hypothesis regarding the analytical expression of the indicator.

Determining the metric values is a very important activity in quantitative and qualitative analysis for assessment the quality of distributed informatics systems. The comparative analysis between different distributed informatics systems or different versions of the same distributed informatics system permit conclusion obtaining about the quality levels of these systems.

4 Conclusions

The distributed informatics systems are increasingly complex systems with a wide range of architectures, structures and components. In addition, the IT&C technologies are more complex and heterogeneous. These facts together with legal requirements have determined to evaluate such systems, especially the critical components like the process security.

It must consider the system characteristics, metric defining issues, metric requirements, security requirements, audit process characteristics to develop an assessment system for security audit of the distributed informatics systems. All these things are the subject of the standards, guidelines, procedures and best practices developed by international organizations the gathered the best specialists.

The built assessment system must be validated through specific techniques. The assessment quality depends on the quality of the assessment system.

The paper presented a methodology plan to build an assessment system without to take into account the phenomenon or process which the metrics are developed for.

An assessment system for audit processes permits obtaining the information by auditors in a shorter time and more precise. Thus, the audit process is more accurate and its costs are lower.

The paper was elaborated within the research project with code 1838/2008, contract no. 923/2009 and the title *Implementation of the Quantitative Methods in Distributed*

Informatics System Audit, financed by The National University Research Council – Ministry of Education, Research and Innovation from Romania.

References

[1] I. Ivan, G. Noşca and S. Capisizu, *Auditul sistemelor informatice*, ASE Printing House, Bucharest, 2005.

[2] I. Ivan and C. Boja, *Metode statistice în analiza software,* ASE Printing House, Bucharest, 2004.

[3] I. Ivan and M. Popa, *Entități text – dezvoltare, evaluare, analiză*, ASE Printing House, Bucharest, 2005.

[4] I. Ivan, M. Popa, S. Capisizu, L. Breda and B. Florescu, *Clonarea informatică*, ASE Printing House, Bucharest, 2003.

[5] I. Ivan, P. Sinioros, M. Popescu and F. Simion, *Metrici software*, INFOREC Printing House, Bucharest, 1999.

[6] IT Governance Institute, *COBIT 4.1*, 2007.

[7] C. Le Grand, *Software Security Assurance: A Framework for Software Vulnerability Management and Audit*, Ounce Labs, 2005.

[8] M. Popa, "Detection of the Security Vulnerabilities in Web Applications", *Informatica Economică*, Vol. 13, No. 1, 2009, pp. 127 – 136.

[9] M. Popa, F. Alecu and C. Amancei, "Characteristics of the Audit Process for Information Systems", in *The Proceedings of the International Conference Competitiveness and European Integration – Business Information Systems & Collaborative Support Systems in Business*, Cluj-Napoca, October 26 – 27, 2007, Risoprint Printing House, Cluj-Napoca, pp. 295 – 299.

[10] M. Popa and M. Doinea, "Audit Characteristics for Information System Security," *Informatica Economică*, vol. 11, nr. 4, 2007, pp. 103 – 106.

[11] People Security, *Redefining Software Security Audit*, Ounce Labs.

[12] http://en.wikipedia.org/wiki/Information_system

[13] ***, *Improving Security Across the Software Development Lifecycle*, Task Force Report, 2004.

Marius POPA has graduated the Faculty of Cybernetics, Statistics and Economic Informatics in 2002. He holds a PhD diploma in Economic Cybernetics and Statistics. He joined the staff of Academy of Economic Studies, teaching assistant in 2002 and senior lecturer in 2006. Currently, he is lecturer in Economic Informatics field and branches within Department of Economic Informatics at faculty of Cybernetics, Statistics and Economic Informatics from Academy of Economic Studies. He is the author and co-author of 6 books and over 100 articles in journal and proceedings of national and international conferences, symposiums, workshops in the fields of data quality, software quality, informatics security, collaborative information systems, IT project management, software engineering. From 2009, he is a member of the editorial team for the *Informatica Economica Journal* and between 2003 and 2008 he was a member of the editorial team for the journal *Economic Computation and Economic Cybernetics Studies and Research.*