Requirements for Development of an Assessment System for IT&C Security Audit

Marius POPA

Department of Computer Science in Economics,
Academy of Economic Studies
Pta. Romana 6, Bucharest, ROMANIA
marius.popa@ase.ro

Abstract: IT&C security audit processes are carried out to implement information security management. The audit processes are included in an audit program as decision of the management staff to establish the organization situation against to the planned or expected one. The audit processes require evidence to highlight the above issues. The evidences are gathered by audit team and some automation processes to increase the productivity and accuracy of the audit are needed. The paper presents some issues of the requirements for development of an assessment system with some considerations for IT&C security audit. The emphasized issues are grouped in the following sections: IT&C security audit processes, characteristics of the indicators development process and implementation issues of an assessment system.

Key-Words: assessment system, security audit, information security management.

1. IT&C Security Audit Processes for Information Security Management

The *audit* is the process through competent and independent persons collect and evaluates proofs to set an opinion on correspondence degree among the observed things and some pre-defined criteria [1].
The distributed informatics systems are complex constructions. They are designed, implemented and maintained to resolve different business tasks in companies. Having in mind the human and financial resources consumption to develop a distributed informatics system, it is necessary to carry out some activities that lead to proposed objective. Also, the proposed objective must be reached in time with the established quality level and within the budget limits [2].
Principles that underlie the audit process are [3]:

- *Independence*: auditors freely develop the audit program; information deemed to be relevant is examined and the content of the report is related to the scope of examination;
- *Use of audit evidence*: it is the information that an auditor uses it for underling the conclusions and to draw up the audit report.

Principles that the auditors must follow are [3]:

- *Ethical behavior*: it is governed by independence, integrity, objectivity, professional competence, confidentiality, professional behavior and technical standards;
- *Correct reporting*: the auditing report is written by persons with professional skills and high experience in the audited field; its content is based on audit evidences and information recommendations for the audit client;
- *Professional responsibility*: auditors have the obligation to respect the principles of the audit process and to assume the consequences if they don't do that.

An IT&C system differs of a manual one through the way in which the results are obtained, the level of security and control, the risks associated to the processing. The potential impact of the risks is minimized through high standards of security and control [3].
In [4], there are presented some common instances of computer fraud and abuse:

This is a post conference paper. Parts of this paper have been published in the Proceedings of the 2nd International Conference on Security for Information Technology and Communications, SECITC 2009 Conference (printed version).

ISSN 2067 – 4074

- Unauthorized disclosure of confidential information;
- Unavailability of key IT&C systems;
- Unauthorized modification/destruction of software;
- Unauthorized modification/destruction of data;
- Theft of IT&C hardware and software;
- Use of IT&C facilities for personal business.

The IT&C security audit evaluates the instances of computer fraud and abuse on the base of security standards. The result of such audit process is the image regarding the vulnerabilities of the analyzed system and the risks that can appear during the system exploitation. Also, the audit process is concretized into an auditing report which contains evaluations of the risks and recommendation to reduce the security vulnerabilities.

During an IT&C audit process, the auditors develop a structured approaching to evaluate the risks and to assist the audited organization to improve its IT&C activities. The requirements of the audited organization aim the independent assessment of its IT&C systems that assist the business processes of the organization. The goal is to find the lacks in IT&C systems, especially the security ones to prevent the possible computer frauds and abuses.

To cover the requirements of the audited organization, the auditing team examines the following IT&C areas:

- *IT&C strategy*: the level of alignment between business and IT strategies, so that to form a direction, common goals and objectives, to delivery the timely services required by IT&C department;
- *IT&C organizing*: compliance of the IT&C organizing to supports all processes and systems deemed critical, having the personnel with necessary professional skills;
- *Application management*: management and maintaining of the application systems to support critical business processes optimally and efficiently;
- *Service management*: internal management of the services, quality parameters assumed by IT&C department to deliver services appropriated to the organization needs;
- *Data and database management*: management and maintaining the data and databases to support optimally and efficiently the critical business processes, assuring the data protection;
- *Computer network management*: management and maintaining the computer networks and communication systems to support optimally and efficiently the critical business processes to deliver correct and timely data to the appropriate destinations;
- *Hardware and workstation management*: management and maintaining the servers, mainframes and operating systems to support optimally and efficiently the critical business processes, applications and data, assuring the data processing within the established parameters and time periods;
- *Computer operation management*: planning and logging the operational activities in data centers and other data processing facilities so that the activities that must optimize and execute the operations that support critical systems are executed correctly and timely;
- *Security management*: management and maintaining the physical and logical access to the IT&C resources to protect the information against unauthorized access;
- *Business continuity management*: process of planning, maintaining and improvement of the security procedures to continue the service delivery within organization;
- *Asset management*: inventorying, management, configuring and maintaining the IT&C assets, including the systems, applications, data and infrastructure components;
- *Change management*: changes in IT&C architecture to assure compatibility, feasibility, planning, correct and timely implementation of the proposed modifications within the components of the IT&C architecture;
- *Solution development and implementation*: process of analyzing, designing, development, configuring, testing, acceptance and release of the IT&C solutions, including the

applications, programs, systems and infrastructure components.

To establish the maturity level of each area, the audit team has to follow some objectives described below:

- Tactical alignment: degree in which the organization covers the requirements of a particular process;
- Stability, availability and degree of safety: how stable and safe it is a particular process, including the support systems, data and infrastructure;
- Processes: how well-defined are politics, standards and procedures;
- Automation and technological coverage: degree in which a process is sustained by available technological resources;
- Results assessment: how the process results are reported, managed and assessed; the way in which the results produce a feedback and a continuous improvement;
- Human resource: degree in which the needs are covered with personal, organizational structure, skills and professional competence of the personnel involved in a particular process.

Specifications regarding the IT&C security audit are included in security audit standards. For instance, the international standards ISO/IEC 17799 approaches audit issues regarding:

- Information technology;
- Security techniques;
- Code of practice for information security management.

The standard ISO/IEC 17799 establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization [5].

The following controls are considered to be common practice for information security, as they are defined in [5]:

- Information security policy document;
- Allocation of information security responsibilities;
- Information security awareness, education, and training;
- Correct processing in applications;
- Technical vulnerability management;
- Business continuity management;
- Management of information security incidents and improvements.

ISO/IEC 17799 International Standard contains 11 security control clauses [5]:

- Security Policy;
- Organizing Information Security;
- Asset Management;
- Human Resources Security;
- Physical and Environmental Security;
- Communications and Operations Management;
- Access Control;
- Information Systems Acquisition, Development and Maintenance;
- Information Security Incident Management;
- Business Continuity Management;
- Compliance.

Each main security category includes:

- A control objective stating what is to be achieved;
- One or more controls that can be applied to achieve the control objective.

COBIT framework – Control Objectives for Information and related Technology – is used as a source of best practice guidance. COBIT includes set of controls and control techniques for information system management. In the IT&C audit processes, it must select the appropriate elements from COBIT in order to evaluate IT&C processes and consideration of information criteria [3].

The organizations that use information technology and communication facilities to reach their objectives are more successful than the ones that do not use them. The IT&C use introduces other challenges within organization. As consequence, the organizations must understand and manage the associated risks and critical dependence of the business processes on IT&C facilities.

2. Characteristics of the Indicator Development for IT&C Security Audit

Information security management aims all methods and techniques of management, use of specific tools and procedures to ensure protection of the information. In modern organizations, information is an essential asset to ensure business

ISSN 2067 – 4074

continuity, minimize business risks and maximize the return of investments.

To reach these goals, the management staff must have information about information security to adjust its methods and techniques of management and to select the most appropriate tools to adjust the level of information protection. This information results from data gathered from audit programs implemented within organization. To ensure information security and to adjust the management actions, it is necessary to implement an information security audit program.

The new information security threats are more sophisticated what it imposes continuous measures to protect the information asset. Because the modern organizations use IT&C tools for their business processes, implementation of IT&C security audit program is a very important requirement.

The security requirements have three main sources [5]:

- Risk assessment: threats to assets are identified, vulnerability is evaluated and potential impact is estimated;
- Legal, statutory, regulatory and contractual requirements: they results from business and social-cultural environments;
- Particular principles, objectives and business requirements: they are developed by organization to support its operations.

The implementation of an IT&C security audit is made by an auditing team in accordance with audit standards, procedures and guidelines. During the audit process, the auditors gather data about audited object to state conclusions in the audit report.

Data gathered in an audit process are in accordance with the professional skills and competence of the auditors. A part of these data can be quantified through indicators. Indicators are included in an assessment system and they are classified in following classes, depending on their applied scope:

- Indicators of audit process quality: are implemented to evaluate the quality level of the audit process; they are useful to evaluate the audit program developed within organization and to decide further performing of the audit program;
- Indicators of auditing object: are used to get data about the object of the control; they aim the elements of the control that can be quantified; as effect, the gathered data are in accordance with reality and the audit team has objective data to state its conclusions.

The assessment system is very useful because obtained data are correct and precise if its quality characteristics are met. The quality characteristics of an assessment system aim the following issues:

- Indicators are correctly developed in accordance with requirements of a such process;
- Indicators do not use important quantities of resources: human, time and financial.

In [6], a template for defining and documenting an indicator is provided. In accordance with that template, the following fields are included [6]:

- Precise objective of the indicator: description of the purpose of the indicator;
- Inputs: list of the data elements that are used in indicator applying;
- Algorithms: the algorithm or formula required to combine data elements;
- Assumptions: business environment, business processes and so forth, as conditions for collecting and using the indicator;
- Data collection information: description of how, when, how often and by whom data are to be collected; also, if a standard form is used to collect data this is referenced;
- Data reporting information: specification of who is responsible to report data, who is going to do reporting and to whom it is going, how often the data will be reported;
- Analysis and interpretation of results: identifying the meaning of the different values for indicator.

Definition of an indicator is more difficult and much more important due to multiple sites and business units of the organization.

In [7], a table for contents of the metrics collection form is provided, table 1.

Table 1. Metrics Collection Form [7]

Metric Title	Brief Description	
Link to Goals/ Objectives	Decision(s) based on analysis	Who makes decision(s)
Who collects data	How is data collected	How often is data collected
Who reports data	How and to whom is data reported	How often is data reported
Who analyzes data	How is data to be analyzed (formulas and factors)	
Lowest acceptable value	Highest acceptable numeric values	Expected values
At what point will you stop collecting this metric		

A definition checklist is used to explicitly define the indicators. In Table 2, a definition checklist template is depicted as it is presented in [6].

Table 2. Definition Checklist [6]

Identification Section			
Attribute #1 Value 1 Value 2 … Value n	**Includes**	**Excludes**	**Optional**
Attribute #2			
…			
Attribute #m			

Identifying the indicators is made on a methodology as it is presented in [6]. The steps of the methodology are [6]:

Step.1 Identifying the goals;
Step.2 Identifying what it wants to know;
Step.3 Identifying the sub-goals;
Step.4 Identifying the entities and attributes;
Step.5 Formalizing the measurement goals;
Step.6 Identifying the measurement questions and indicators;
Step.7 Identifying the data elements;
Step.8 Defining and documenting measures and indicators;
Step.9 Identifying the actions needed to implement measures;
Step.10 Preparing a plan.

Depending on measurement scale, the indicators used to assess IT&C security audit are classified in the following classes:

- Qualitative: the measurement scale has discreet units as very good, good, satisfactory, poor, very poor;
- Quantitative: the assessment is a very precise one and it is a numerical one.

Depending on aggregation level, the indicators included in an assessment system are classified in the following classes [8]:

- Primary indicators (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 indicators: they are the results of many audit processes, multiple applications or aggregation operations of the primary metrics.

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

In COBIT, the indicators are defined on the following levels [9]:

- 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 indicators defined in COBIT 4.1 are [9]:

- 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.

ISSN 2067 – 4074

In relation to the reaching of the organization goals, in [6] three classes of indicators are identified:

- Success indicators: are used to establish if the goals are met; they are developed from defined success criteria;
- Progress indicators: are used for tracking the execution of tasks; a successful execution of the all tasks does not guarantee the accomplishment of the organization goals;
- Analysis indicators: assist the analyzing the outputs of the tasks; they help to judge the success or progress.

Operational aspects to implement an assessment system are highlighted in [6] and they aim the following issues:

- Forms for collecting and recording data;
- Data storage and access tools;
- Operators for collecting, storage and access data;
- Tools to aid in collection and analysis;
- Roll up procedures;
- Training.

Development and implementation of an assessment system must take into account the following requirements [6]:

- Identifying the indicators based on a methodology;
- Specifying the goal of the assessment system;
- Indicator traceability back to the goals;
- Clear understanding of the type and purpose of each indicator;
- Small start point for assessment;
- Indicators for detecting the trends and hidden tradeoffs;
- Customizing the indicator template;
- Use of definition checklist;
- Dissemination of the unambiguous information;
- Privacy issues of the indicators;
- Respecting the needs of involved people;
- Identifying the adequate solutions available if there is no consensus;
- Using of pilot implementation;
- Planning some assessment on short term;
- Maximizing the relevant information and minimizing the collection effort;
- Testing of the assumptions;
- Taking into account the unintended consequences and the perspectives of different stakeholders.

The all issues presented above must be considered during the development process of an assessment system. They are requirements that must be met during the development process of an assessment system.

Depending on the area in which the assessment system is developed, the indicators are built in accordance with quantified processes, incorporating the elements that characterize those processes.

For instance, the assessment system for IT&C security audit processes contains indicators that measure quantitative elements of the implemented controls. The mathematical models and algorithms associated to an indicator contain elements that characterize the object of the control.

In accordance with the above criteria, an indicator can be placed in different classes depending on classification criteria.

3. Implementation Issues of an Assessment System for IT&C Security Audit

An audit process is based on implementation process of controls. Nothing is controlled whether it is not measured. The indicators offer to the auditors the quantitative representation of the audit object. They are used as tools by audit team to obtain auditing proofs for drawing up the audit report.

The indicators must be selected and tailored to the audit object by the auditors. The audit team has to define program that describes the needed indicators, who need these indicators and the way in which an indicator is calculated. A good measurement program provides the success or failure of the controls implemented in the audit process.

The assessment program in an audit process is based on the goals of the audit process. The program must be carefully planned, implemented and regularly evaluated for effectiveness. It is used as decision tool by audit team [10].

A assessment program includes three major activities as it is presented in [10]:

- Plan development;

- Plan implementation;
- Program evaluation.

The assessment program cycle adapted from [10] is depicted in the below figure.

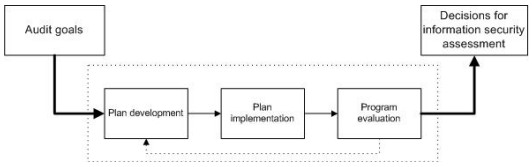

Figure 1. Assessment program cycle adapted from [10]

The goal-question-metric paradigm is the base of the plan development. This paradigm was developed by Victor Basili and it is based on the following concepts [10]:

- Processes have associated goals;
- Each goal leads to one or more questions regarding the accomplishment of the goal;
- Each question leads to one or more metrics to answer to the question;
- Each metric requires measurements to produce the metric;
- Selection of the measurements to produce the metric.

In the plan implementation cycle, there are four activities as it is shown in [10]:

- Collecting data: it is made at specific intervals according to the plan;
- Validation of the data: it is ensured the accuracy of the measurements and data collection consistency;
- Deriving metrics: they are derived from data analysis;
- Making decisions: they are made on metrics delivered for evaluation.

For an audit process, the program evaluation must consider the following issues [10]:

- Adequacy of current metrics;
- Superfluity of the metrics or measurements;
- Interferences with audit work;
- Accuracy of analysis results;
- Data collection intervals;
- Simplification of the metrics program;
- Changes in audit process or organization goals.

The assessment program must be evaluated at regular interval to determine if the measurement needs of the audit team are met.

According to George Jelen of the International Systems Security Engineering Association, the good metrics are those are SMART: **S**pecific, **M**easurable, **A**ttainable, **R**epeatable and **T**ime-dependent.

Information security activities cannot be managed if they cannot be measured. An assessment system helps the security managers as it follows [11]:

- To discern the effectiveness of the various components included in security programs;
- To discern the security of a specific system, product or process;
- The ability to address security issues for which staff or departments are responsible.

As a rule, the size and method of the periodic audits are determined by the size of the informatics system for which the audit is carried out. For large informatics systems, the audit is segmented depending on physical locations, departments and networks.

The scope of an audit and assessment should be well defined and narrow enough. The generated data are assessed and acted upon in a timely enough to avoid exploit and compromise [12]. This issue determines the frequency of the audit processes. The frequency of the audits is classified in the below classes as it is depicted in [12]:

- Periodic: monthly, quarterly, semi-annual and so forth; also, the periodic audits are pre-scheduled events defined within the scope of the audit; they are planned and scheduled as part of the security architecture;
- Event triggered: computer security is very often reactive; thus, mechanisms are defined to trigger or set motion reactive measure that cannot be planned in advance;

In [12], a flow diagram for BASE security assessment methodology is depicted figure 2:

ISSN 2067 – 4074

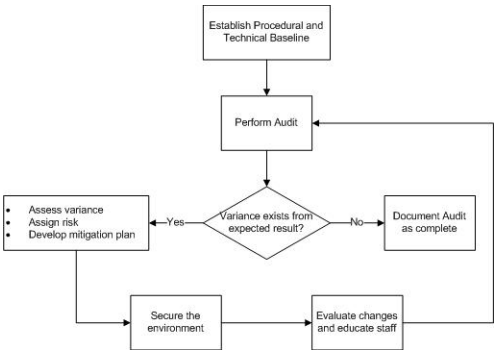

Figure 2 BASE Flow Diagram [12]

BASE – **B**aseline, **A**udit and Assess, **S**ecure, **E**valuate and Educate outlines a basic Information Assurance vulnerability protocol, including the no-cost tools. Its goal is to build a universal information security framework by everyone [12].
The BASE methodology includes the following steps [12]:

- Audit: review the baseline/documented/ expected configuration to establish the operational state versus the planned one;
- Assessment: using the results of the audit process and establishing of the variance; if there is variance, the following activities are carried out:
  - Assign risk: determining the risks based on computer security principles: Confidentiality, Integrity and Availability; the risk analysis is carried out on quantitative and qualitative methods and other risk assessment tools; the results of assigning risks guide decisions and next actions;
  - Develop mitigation plan: establishes the measures which decrease the severity of risk, transfer the risk somewhere else or accept the identified risk because the resources involved in remediation efforts exceed the value of protected assets; these activities are implemented depending on risk assigned to variances;

The implementation process depends on the requirements of the assessment system developed for IT&C Security Audit. This process should be carried out in accordance to international standards for information security management. The result is an assessment system that it is robust and reliable.

4. Conclusion

The information security management should be based on data gathered from information system to establish the situation of the information security against the expected one. These data are obtained from an audit program approved by management staff and developed by independent audit teams to assure high quality of the conclusions specified in the audit report.
The assessment system aims the following levels of evaluation:

- The real situation of the organization;
- Using the indicator system as tool of measurement during the audit process;
- Measurement of the level of quality for audit processes carried out during the audit program implementation.

The indicator system for measurement of the audited system components should accomplish some quality characteristics like robustness and reliability to satisfy the requirements for such assessment system.
The paper was elaborated within the research project with code 1838/2008, contract no. 923/2009, having the title Implementation of the Quantitative Methods in Audit for Distributed Informatics Systems, financed by The National University Research Council – Ministry of Education, Research and Innovation from Romania.

References

[1] S. Capisizu, *Models and Techniques for Development the Economic Information Audit*, ASE Bucharest, 2006, PhD Thesis

[2] S. Capisizu, G. Noşca and M. Popa, Informatics Audit, *The 37th International Scientific Symposium of METRA*, Military Equipment and Technologies Research Agency, Bucharest, May 25 – 26, 2006

[3] M. Popa, C. Toma and C. Amancei, Characteristics of the Audit Processes for Distributed Informatics Systems, *Informatica Economică*, vol. 13, no. 3, 2009, pp. 165 – 178

[4] Barclay Simpson Recruitment Consultant, *An Introduction to Computer Auditing*, London, www.barclaysimpson.com

[5] International Standard *ISO/IEC 17799, Information Technology – Security Techniques – Code of Practice for Information Security Management*, Second Edition, 2005

[6] W. Goethert and W. Hayes, *Experiences in Implementing Measurement Programs*, Software Engineering Measurement and Analysis Initiative, Carnegie Mellon University, Technical Note, November 2001

[7] T. Augustine and C. Schroeder, An Effective Metrics Process Model, *The Journal of Defense Software Engineering*, vol. 12, no. 6, 1999, pp. 4 – 7

[8] M. Popa, Characteristics for Development of an Assessment System for Security Audit Processes, *Economy Informatics*, vol. 9, no. 1, 2009, pp. 55 – 62

[9] IT Governance Institute, *COBIT 4.1*, 2007

[10] T. Perkins, R. Peterson and L. Smith, Back to the Basics: Measurement and Metrics, *The Journal of Defense Software Engineering*, vol. 16, no. 12, 2003, pp. 9 – 12

[11] S. Payne, *A Guide to Security Metrics*, SANS Institute, Whitepaper, June 2006

[12] G. Braunton, *B.A.S.E. – A Security Assessment Methodology*, SANS Institute, Whitepaper, September 2004