SERIOS: A Security Model and Framework for Implementing Information Security

Marius MIHUȚ
Babeş-Bolyai University of Cluj-Napoca, Romania
mariusmihut@yahoo.com

Each organization is interested in protecting informational assets held (information and associated infrastructure). In many organizations, they are considered critical resources, whereas the existence of the organization depends on how they are protected. This paper proposes a multidisciplinary approach to security, from a managerial and technical perspective and introduces methods and tools from other fields, which can be used in security field. The main objective of this paper is to present the SERIOS security model and framework concepts and elements as well as the security metrics system used to evaluate the state of organization security.

Keywords: *SERIOS Security Model and Framework, Information Security Metrics System, Pareto Principle, 1-10-100 Rule and Montesquieu Principle Applied in Information Security*

1 Introduction

In the information society, protection of information is a key factor for the success of any organization. However, implementing an information security system in an organization is delayed due to the complexity of the process and lack of necessary resources (time, personnel and financial resources).

The current situation in the security of information systems is:

- information systems of organizations are interconnected with other networks, including public networks, leading to an expansion of vulnerabilities associated systems;
- in many cases, organizations address security issues "reactive" (as a reaction to an event) and without a clear and consistent approach;
- security costs are among the top candidates, when there is the need for costs cuts;
- implementation of information security systems is difficult and expensive.

Common characteristics of information security systems extracted from ISO [1], [2] and NIST [3] standards, are:

- programmatic approach: security is a path not a target, so implementing security is done through a program (defined as a platform of principles, means, methods), not by a plan (defined as a sequence of activities performed for achieving a goal);
- approach based on risk management: risk reduction is essential in ensuring information security;
- systemic approach: security measures are designed / integrated in a system;
- approach based on process improvement: the security is improved by improving existing processes or creating new ones. The main process in security management is the management of risk;
- integrated approach: IT security is included in information security;
- cyclical approach: the sequence of processes and activities is repeated in the same order and is a closed circle;
- iterative approach: improvement of security is done by periodically iterations of processes;
- open approach: it is encouraged the expansion of the security management system with new features that are specific to organization;
- concern for efficiency: not all security measures are implemented, but only those considered appropriate after a cost-benefit analysis;
- concern for alignment with other standards and management systems of the or-

ganization: IT security is considered a subdomain of organization governance, aiming to align security operations with the objectives of the organization;
- concern for performance evaluation: there is a need for creation of security metrics that can measure the performance of the security system.

These characteristics must be added with the following objectives:
- risk management must be included in organization security management;
- security system should provide support for management decisions.

2 Security Concepts Defined in Security Model

Security model is a representation of the goals, principles and security policies. It is based on several key concepts presented below.

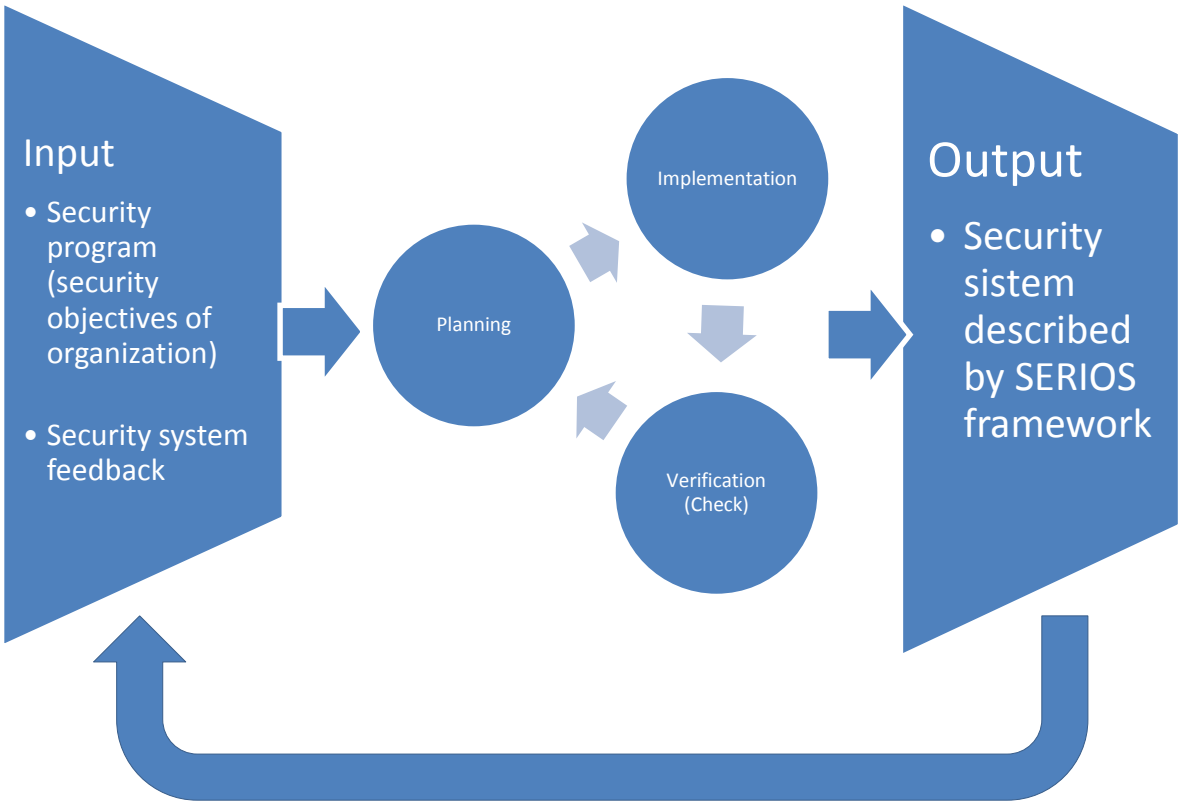

Fig. 1. Security model for SERIOS framework

Security level is the degree of protection of informational assets, assured by a security system. The level of security depends on security measures, security costs, level of staff training, residual risk and is expressed as:

$$NS = f(Ms, Cs, Ni) / Rr$$

where:
- NS is the security level;
- Ms is a parameter that depends on the implementation of security measures;
- Cs is a parameter that depends on the effectiveness of security costs;
- Ni is a parameter that indicates the level of staff training;
- Rr is the residual risk.

Informational asset is information and associated infrastructure (information resources, utilities and hardware and software resources) that must be protected. Also, operational environment (areas, rooms, and offices) are considered as informational assets.

Security management process consists of activities undertaken to ensure information security. This will interact with other processes of the organization.

The *inputs* of the process are:

- security objectives of organization;
- requirements of stakeholders;
- legal norms;
- contract obligations;
- organizational culture;
- results of the verification of the security system.

The *outputs* of the process are:

- security system (described by SERIOS framework).

Table 1. Security management process and sub-processes for SERIOS Framework

PLANNING
Organizing and administering the security management process
Risk management
Design of security system
IMPLEMENTATION
Identify the organization's informational assets
Authorization and staff training
Implementation of security metrics
Implementation of security metrics
Implementation of security tools
Implementation of management tools
VERIFICATION
Real-time monitoring
Response to events
Security system audit
Security scans
Security tests
Security evaluation

Security management process is based on iteration of 3 steps / sub-processes: planning, implementation and verification. Security management process should be resumed when one of its inputs is changed. Security system outputs are connected as inputs (as feedback) of the process.

Security policy is the description of protection goals and mechanisms that ensure security. Security policy derived from the organization's policy. The fundamental objectives of security policy ensure the confidentiality, integrity and availability of informational assets.

Information security system is that part of the organization's management that provides planning, implementation and verification of a coherent set of policies and processes to protect informational assets. The ISO / IEC 27001: 2005 management system is called the Information Security Management System (ISMS).

Information security program is the set of principles, goals, activities, tasks and resources required to ensure information security. Within the organization a security program must be implemented, that is different from a security plan in that program sets a framework (a path) to reach and maintain an optimal level of security, while the plan has limits and precise objective (target).

Protection of informational assets aims to ensure confidentiality, integrity and availability of information, regardless of the media on which it is stored (electronic, magnetic, optical, paper or other) and regardless of its state (stored, transmitted or archived).
Security measures, countermeasures and controls (mechanisms) are the means by which security risk is reduced. Term measure is equivalent to the term countermeasure and it is represented by any means used to ensure security, while security control (mechanism) is described as a structure that includes the definition / description of security measures, implementation and verification instructions and criteria for assessing the maturity level.

Table 2. The structure of a security control

Definition	*Control name* *Control purpose* *Requirements and restrictions (legal, organizational, technical or other)*
Description	*Describe how associated security risk can be reduced*
Implementation	*Provides instructions for implementing security measure*
Verification	*Provides instructions for monitoring and assessing security measure*
Maturity level	*It includes criteria for assessing the level of maturity of the control:* *- Level 1: security measure is established and implemented;* *- Level 2: security measure is formally defined;* *- Level 3: control is implemented and its functionality has been verified.*

Measurement is any mean used to assess security, while *metric* is a description of a measurement, together with the interpretation of it.
The *metric* is described as a structure that includes the definition / description of its security measures, implementation and verification instructions and evaluation criteria of maturity.

Table 3. The structure of a security metric

Definition	*Metric name* *Metric purpose*
Measuring	*Provides information about associated metric measurements*
Implementation and functionality	*Provides instructions for checking the implementation and functionality*
Maturity level	*It includes criteria for assessing the level of maturity of the metric:* *- Level 1: the implementation of security metric was verified;* *- Level 2: the functionality of security metric was verified;* *- Level 3: security metric is periodically monitored and calculated.*

The *framework* is a conceptual structure used to address and describe the complex issue of information security.
The framework will define, plan and evaluate the implementation of information security.
The security framework SERIOS is proposed by the author as part of his PhD thesis. SERIOS stands for:

- safe: from a security perspective;
- efficient: from an economic perspective;
- rapid (fast): in terms of implementation;
- integrated: in terms of processes and objectives of the organization;
- operational: from the perspective of ensuring optimal conditions for implementation;
- supportive: from the perspective of support provided for management.

The framework has the following characteristics:

- it is based on an approach of "tabula rasa" in an organization (this approach is described in [4]);

- it is based on key concepts described above: protecting informational assets, risk management and measurement of security;
- strategic approach of security model aims to align framework to processes and objectives of the organization and bringing the organization's security system at an optimum maturity level;
- tactical approach of security model is based on periodic iterations of the following processes: planning, implementation, verification;
- operational approach is based on applying at the first iteration the Pareto Principle, for the selection of risks and countermeasures, and the Critical Path Method to implement countermeasures. The goal is to reduce the implementation time of security system and also to get an acceptable level of security, as soon as possible.

Each chapter of the framework will be structured as follows:

Table 4. The structure of each chapter of SERIOS framework

Requirements	*Description of the security requirements related to this section*
Content	*The contents of this chapter, which may be included in the security documentation*
Maturity level	*It includes criteria for assessing the maturity level of the content of this chapter:* *- Level 1: chapter was included in the security documentation;* *- Level 2: all security requirements of the chapter were treated;* *- Level 3: content of the chapter has been verified and correlated with other chapters.*

SERIOS framework is the tool for implementing a security system based on security model described above. The framework has 19 chapters. For each of them, key elements are presented in Table 5:

Table 5. Chapters of SERIOS framework

	Chapter name	**Key element**
1.	Purpose	Introduction of *maturity level* concept
2.	Terms and definitions	Glossary containing 53 terms
3.	Objectives	Statement of 10 objectives
4..	Principles	Statement of 16 principles
5.	Organization of security	Using the principle of separation of powers (Montesquieu)
6.	Responsibilities and duties	Definition of individual tasks and structures
7.	Processes and activities	Definition of security system
8.	Security documentations	Evidence of documentation elements
9.	Informational assets identification	Definition and evidence of informational assets
10.	Staff authorization	Definition of authorization scheme
11.	Staff training	Definition of levels and goals of training
12.	Risk management	Using generic catalogues of threats and vulnerabilities
13	Security measures and	Using generic catalogue of security measures

	controls	
14.	Security measurements and metrics	Definition of *security metrics system*
15.	Maturity levels	Definition of evaluation scheme for maturity levels
16.	Security tools	Definition of requirements for using security tools
17.	Management tools	Definition of requirements for using management tools
18.	Verification of security	Definition of requirements for security monitoring
19.	Response to events	Definition of requirements for response to events

The security metrics system of SERIOS framework is complete and can be used as a useful tool for security evaluation. It is presented in the next chapter.

3 Security metrics system

The goals for developing a system of metrics and security measures are:

- evaluation the maturity of security system;
- evaluation of security level of the organization;
- providing the support for decisions for management.

The security metrics system groups the metrics into three categories [5]:

- implementation metrics;
- verification metrics;
- ascertainment metrics.

Each group will contain a metric for each security control. The metric will measure the implementation degree or the functionality of the control.

Implementation metrics will measure the implementation degree of security controls. Verification metrics will measure the functionality of the controls, determined after an operation of: security audit, vulnerabilities scanning or security testing.

Ascertainment metrics will measure the functionality of the controls, determined after a security event took place.

The implementation degree for a security control can take one of the values [5]:

- 0: the security control is implemented;
- 0,5: the security control is partially implemented;
- 1: the security control is not implemented.

The functionality of a security control can take one of the values [5]:

- 0: the security control is functional;
- 0,5: the security control is partially functional;
- 1: the security control is not functional.

The value of implementation degree, respectively of functionality will be multiplied by a weight, which can take one of the values [5]:

- 1: for implementation metrics;
- 10: for verification metrics;
- 100: for ascertainment metrics.

The weights for metrics where chosen based on 1-10-100 Rule, which is described in [6].

The metric will measure the deviation of a security control, using the formula [5]:

$$\text{Metric} = \text{Value} * \text{Weight}$$

The aggregate indicators for implementation metrics, verification metrics and ascertainment metrics are defined as follows [5]:

$$I_{ai} = \frac{1}{m*n} * \sum_{i=1}^{n} Implementation\ metric_i$$

$$I_{av} = \frac{1}{m*n} * \sum_{i=1}^{n} Verification\ metric_i$$

$$I_{ac} = \frac{1}{m*n} * \sum_{i=1}^{n} Ascertainment\ metric_i$$

$$I_{ss} = I_{ai} + I_{av} + I_{ac}$$

where:

- I_{ai} is the implementation aggregate indicator;
- I_{av} is the verification aggregate indicator;
- I_{ac} is the ascertainment aggregate indicator;
- I_{ss} is the aggregate security indicator;
- m is maturity level of security system;

- n is the number of security measures / controls.

Implementation metric for security control *„i"* is:

$$Implementation\ metric_i = Implementation\ degree_i * 1$$

where:

- the implementation degree indicates that security measures have been implemented or not and can take one of the values 0 - measure is implemented, 0.5 - measure is partially implemented or 1 - the measure is not implemented;
- the weight for implementation metrics is 1 because, by analogy with the 1-10-100 rule, this phase is equivalent to design or production. Identifying problems of security measures implementation at this stage allows hotfix them with a low consumption of resources.

Verification metric for security control *„i"* is:

$$Verification\ metric_i = Functionality\ degree_i * 10$$

where:

- The functionality degree indicates whether security measure is working or not and can take one of the values 0 - measure is functional, 0.5 - the measure is partially functional or 1 - the measure is not functional. Functionality is determined in security monitoring activities carried out internally within the organization;
- The weight for verification metrics is 10 because, by analogy with 1-10-100 rule, this phase is equivalent to testing. Identify issues of security during verification phase involves the use of additional resources for security system redesign. This must be reflected in the level of security, thus the weight metric is an order of magnitude greater than the metric for the implementation.

Ascertainment metric for security control *„i"* is:

$$Ascertainment\ metric_i = Functionality\ degree_i * 100$$

where:

- the functionality degree indicates whether security measure is working or not and can take one of the values 0 – the measure is functional, 0.5 - the measure is partially functional or 1 - the measure is not functional. Functionality is determined after the occurrence of security events;
- the weight for ascertainment is 100 because, by analogy with 1-10-100 rule, this phase is equivalent to eliminate the defect of a product that was delivered. Identify implementation issues of security during ascertainment phase involves both consumption of resources for security system redesign and significant costs to reduce the negative effects of the event. This must be reflected in the security level, thus the weight metric is two orders of magnitude greater than the metric for the implementation.

4 Security Model Verification

In designing and verifying security model proposed in the paper, were taken into account the characteristics of ISO and NIST standards.

The SERIOS framework was developed in two main directions:

- redesign the common elements of security standards;
- improve of security systems deficiencies.

Security design elements that have been redefined and redesigned based on other standards are:

- objectives and principles of security;
- organization of security;
- risk management process;
- catalogues of generic vulnerabilities, threats and security measures;
- authorization and staff training;
- security documentation and records;
- verification of security;
- response to events;
- glossary of terms used.

The elements of the security model and framework that are completely new are:

- system security metrics;
- evaluation the maturity of security system;
- identification of security and management tools used in the security system;

- formalization of mathematical concepts.

Security model elements that are common to other standards will ensure independent functioning of the security system and its horizontal integration with other standards.
The new elements of the security model will ensure the integration of security processes in organizational processes and vertical integration of security systems with other IT management systems.

5 Security model validation

Security model validation was done by analyzing the results of the case study described in [5]. Validation aimed at verifying that the security model is correct (i.e. ensuring adequate protection of informational assets) and the system indicates the level of security metrics accurately.
The aggregate security indicator was measured in six situations:

- initially;
- after conducting risk analysis;
- after implementing security measures selected according to Pareto's Principle;
- after conducting a security audit;
- after a scan of the computer network;
- after testing the security system;
- upon the occurrence of a security event.

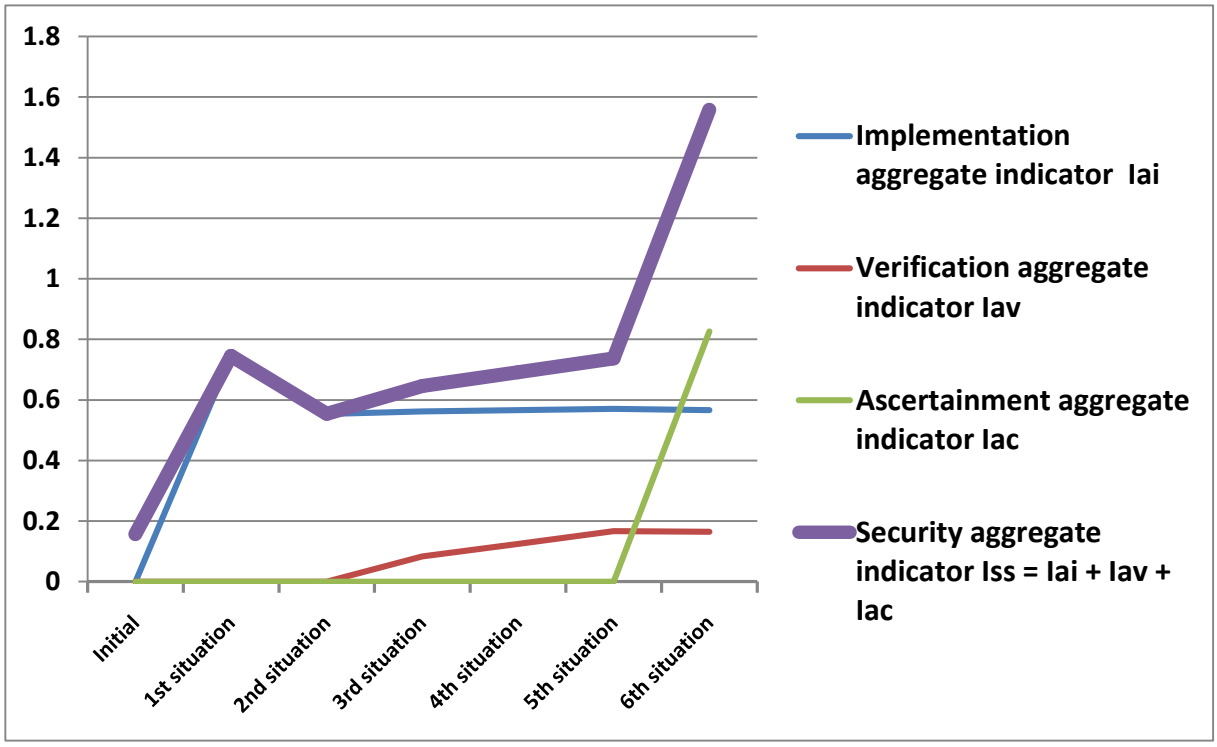

Fig. 2. Aggregate indicators values

Analysis of case study results revealed the following conclusions:

- in the initial situation, the small Iss value (0.151) indicates the lack of information about the state of security;
- after the first step, Iss value increases, indicating the need to implement security measures;
- in 2nd situation, Iss value decreases because the 23 security measures were implemented.
- the value of Iss in 3rd situation shows some shortcomings when implemented (indicated by the higher value of Iai) discovered after verification activity (Iav's value is not 0).
- situations 4 and 5 indicate new problems of security system (security measures not implemented or partially implemented) which were discovered during the verification activities performed internally.
- in 6th situation, Iss indicates major problems (a security event). It is noted that

this finding is due to the ascertainment aggregate indicator - Iac, which also increases sharply, indicating a problem that went beyond the organization. The other two indicators (Iai and Iav) have slight increases, meaning the gaps of implementation and verification.

Also, in Figure 2 one can observe which of aggregate indicators Iai, Iav and Iac contributes to aggregate indicator Iss modification. This fact indicates the "area" that generates the problem (the implementation of measures, verification of measures or a security event).

It is noted that, after the implementation of security measures, the security of organization is improved, which means that security model protects informational assets of the organization.

Also, the aggregate security - Iss accurately reflect the security level of the organization, which means that the security metric system is working correctly. Another function of the indicator unit security - Iss is the auto-adjust of security system (incorrect implementation of security measures will influence this indicator).

6 Conclusions

In this paper was described a security model and SERIOS framework, which is the tool for implementing a security system based on this model.

New conceptual elements of security model are:

- using PIV model for security processes, based on three phases (Planning, Implementation and Verification) instead of a four-phase model (e.g. PDCA);
- introducing the concept of informational asset, in order to indicate the core element to be protected;
- formal definition of the concept of security level;
- introduction of a process for implementation of security tools, in order to determine the precise activities and tools used to monitor security;
- introduction of a process for implementation of management tools, in order to determine the precise activities and tools used as decision support.

New conceptual and structural elements of the SERIOS framework are:

- the concept of the maturity level to indicate the development of the security system (the concept was defined and used to evaluate each chapter of the framework);
- using Pareto Principle to select security measures for rapidly obtaining an acceptable level of security;
- identify and state security principles underlying security model;
- use the principle of separation of powers (stated by Montesquieu) for separation of responsibilities;
- formal definition of the concept of security level;
- presentation of a complete security metrics system that can be used as a tool for security assessment;
- use Rule 1-10-100 within the system metrics for weighting the deviations of implementation and verification of security measures;
- insert a distinctive chapter for security tools, for precise highlighting security monitoring tools;
- insert a distinctive chapter for management tools, for precise highlighting decision support tools.

References

[1] ISO/IEC 17799, *Information technology – Security technics – Code of practice for information security*, International Organization for Standardization, 2005.

[2] ISO/IEC 27001, *Information technology – Security technics – Information security management systems – Requirements*, International Organization for Standardization, 2005.

[3] NIST Special Publication 800-53 Revision 3 (2009), Recommended Security Controls for Federal Information Systems and Organizations, *US Department of Commerce* [Online]. Available: http://csrc.nist.gov/publications/PubsSPs.html

[4] T. Ritter, ”Reaching Out to Protect With-

in: Comparing and Contrasting ISO 27002/27002 and NIST Special Publication 800-Series information security standard*"*, in *IT Compliance Journal*, vol. 2, issue 2, [Online]. Available: http://download.101com.com/pub/itci/Files/ITCi_Journal_V2N2_07Q3_Web_Final_a.pdf

[5] M. Mihuţ "Security Measurement and Visualization: a New Approach", *Proceedings of the 13th International Conference on Informatics in Economy IE2014*, pp. 490-495, Bucharest, May 2014.

[6] B. Boehm "Industrial Metrics Top 10 List", *IEEE Software*, pp. 84-85, Sep. 1987.

Marius MIHUŢ has completed a Master Program at Faculty of Economic Studies and Business Administration from Babeş-Bolyai University Cluj-Napoca, in 2007, with a paper on security of information system. He continue the research as a PhD student of the Doctoral School of Cluj-Napoca Babeş-Bolyai University – Faculty of Economic Studies and Business Administration, in the field of information security.