SocioBrains
ISSN 2367-5721, JOURNAL HOMEPAGE: WWW.SOCIOBRAINS.COM
INTERNATIONAL SCIENTIFIC REFEREED ONLINE JOURNAL WITH IMPACT FACTOR
ISSUE 42, FEBRUARY 2018

FORMALIZATION OF PROCESSES IN THE SYSTEMS FOR RISK MANAGEMENT IN CYBERSECURITY

Abstract: This article represents an attempt to systemize published, generally accepted frameworks for risk management in cybersecurity systems, with the aim to supplement and further develop the existing methodologies.

Author information:

Kamen Kalchev
Associate professor Ph.D.
Department: Communication and Information Systems
Military Academy "G.S.Rakovski" – Sofia
✉ kamenstanev@abv.bg
Bulgaria

Keywords:
Cybersecurity, risk, risk assessment, risk management, Cybersecurity Framework, ISO- 27001, NIST SP 800-53.

A significant part of the organizations which realize their processes through information systems, pay considerable attention to the systems for cybersecurity. Also recognizing the significant impact of the information systems for achieving their goals, most of the organizations use a specific risk management system as a main approach for information security.

There are many existing, well described and standardized methods for risk management as part of a system for cybersecurity - Mehari (MEthod for Harmonized Analysis of RIsk), EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité - Expression of Needs and Identification of Security Objectives), ISO 27005, NIST SP 800-53 and others. All of them, even though they are developed in much detail, do not exclude the human factor in the management. The management on a strategic level (often times by the cybersecurity administrator) realizes a permanent iterative intervention in the risk management process, which is the main carrier of subjectivity in this management [1].

It is not always possible to totally ignore the human factor in the risk management process, especially in human-machine systems. However, there is a general tendency towards completeness of the formalization of this process as one of the steps for its automation.

The purpose of this article is to present an idea for formalizing part of the processes in these systems by analyzing the standard ISO 27005 and NIST SP 800-53 frameworks for describing risk management systems. Most of all, this would allow to ignore the human factor as much as possible and to create an opportunity for making the risk management automatized.

The framework for description of the processes of risk management in the cybersecurity systems (Cybersecurity Framework - Version 1.0), provided by the National Institute of Standards and Technology, is concentrated on the key role of the strategic guidance for managing the organization [2]. According to the recommendations of this document risk management is a continuous iterative process of identification, evaluation and response to the risk. To manage the risk, the organizations must understand the probability for the occurrence of an event and the consequences which follow it.

The risk management process itself is present in the identification function (Identify) and in the categories: assets, business environment, management, risk assessment and strategy for managing the risk. The schematic description of the process (fig. 1) explicitly emphasizes the role of the strategic

leadership in the perception of the risk and the solution for the way to prevent it; for example, by risk mitigation, transfer of the risk, avoiding the risk or accepting the risk. These actions are in relation to the potential impact on the provision of critical services.

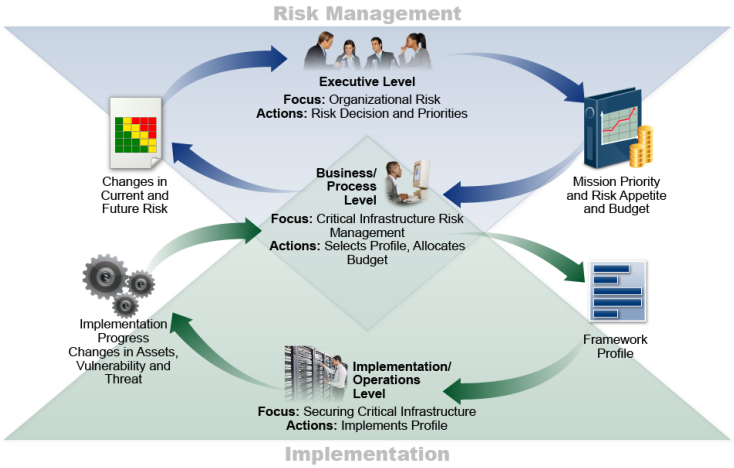

Fig. 1 Notional Information and Decision Flows within an Organization - Cybersecurity Framework - Version 1.0.

The framework also focuses on the use of strategic leadership for guiding the cybersecurity system by reporting the risks over it as part of the processes for risk management in the actual organization.

In the publication NIST SP 800-53 the processes concerning the risk management and their realization are shown in detail [3]. This is described in chapter two (2.1 MULTITIERED RISK MANAGEMENT) where the main steps in the risk management are schematically are presented (fig. 2).

They are:

Step 1 – categorizing the information systems;

Step 2 – selection of precautionary measures;

Step 3 – realization;

Step 4 – evaluation;

Step 5 – authorization (giving a mandate, permission);

Step 6 – monitoring the processes.

The methodology for realization of these steps is recommended in the so-called SECURITY CONTROL IDENTIFIERS AND FAMILY NAMES like PM (Program Management) - 8, PM – 9, PM – 11, PM - 14.

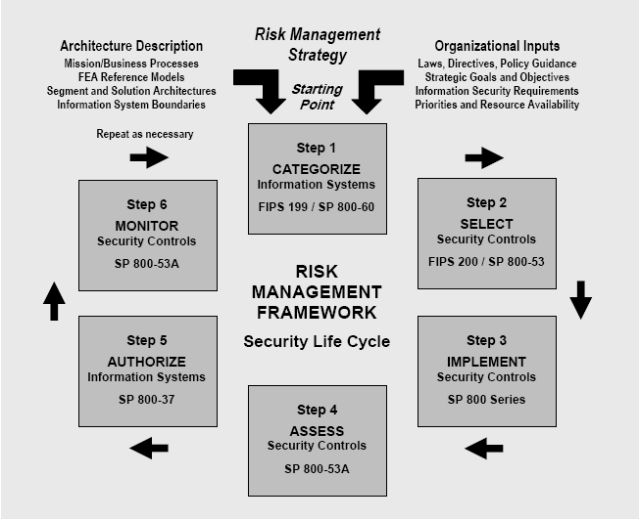

Fig. 2 (RISK MANAGEMENT FRAMEWORK) - NIST SP 800-53.

PM – 8 (Program Management - 8)

This is a requirement for the organization to keep an up-to-date documentation of the critical infrastructure and a plan for protecting key resources.

PM – 9 (Program Management - 9)

Here the recommendations are split into three paragraphs:

- availability of an overall risk management strategy (for the entire organization);
- application of this strategy;
- periodical review and update of the risk management strategy.

In this paragraph there is also a recommendation for the structure of the risk management strategy like: unambiguously defining the level of perception of the risk; methodology for evaluating the risk; methodology for deciding in situations demanding choice of actions related to the treatment of the risk; approaches for observing the risk.

PM – 11 (Program Management - 11)

For this element the recommendations are presented in two paragraphs:

- defining the relation between the goal (the task) of the organization and the risk which the information processes bring by accompanying the achieving goal and performing the task;
- defining the needs for protection of the information, resulting from the already defined goal (task) / information processes.

PM – 14 (Program Management - 14)

Here the main recommendations are:

- presence of plans for testing the system and training;
- these plans are performed and periodically are actualized.

Another frequently used framework for implementing a risk management strategy is ISO/IEC 27005.

This standard includes a description of the process of the risk management in so-called clauses (sections) [4]:

Clause 5: Background

Clause 6: Overview of the information security risk management process

Clause7: Context establishment

Clause 8: Information security risk assessment

Clause 9: Information security risk treatment

Clause 10: Information security risk acceptance

Clause 11: Information security risk communication and consultation

Clause 12: Information security risk monitoring and review

The process of risk management in cybersecurity includes determining the significance of the risk (section 7), evaluation of the risk (section 8), handling of the risk (section 9), approval of the risk (section 10), exchange of information (section 11), monitoring and review (section 12).

This process is graphically presented in fig. 3.

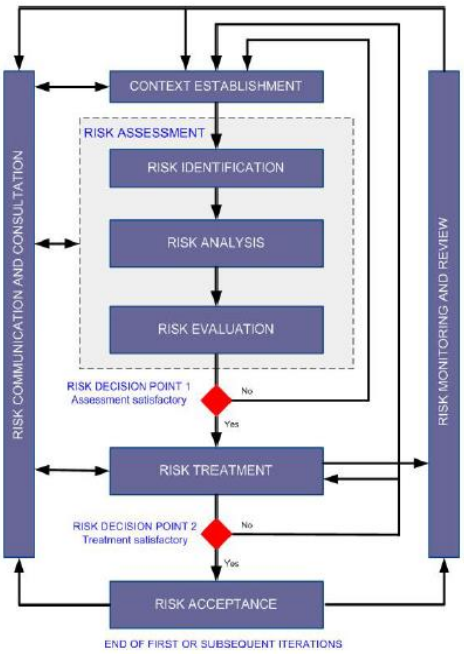

Fig. 3. Risk management process ISO/IEC 27005.

Here again the leading role is transferred to the strategic leadership of the organization, whose responsibilities are: determining the impact of the risk and making decisions at the two crucial points in the process (point 1: acceptance of the risk assessment; point 2: deciding whether the treatment of the risk is satisfactory).

A significant place in the standard is devoted to the process of the risk treatment. Here, as in NIST SP 800-53, there are opportunities for:

- risk modification - this is achieved by changing controls that can protect the assets by correcting, eliminating, preventing, minimizing the impact, deterring, detecting, restoring, reconfiguring, using reserve, monitoring and awareness;
- risk retention - if the risk assessment indicates that the results show that the risk is acceptable, it can simply be saved without having to change the controls;
- risk avoidance - this can be achieved by completely avoiding activities that increase the risk;
- risk sharing - this risk treatment option includes other parties that could monitor the information system against an attack. However, this does not mean that responsibility is shared, as the responsibility for the consequences still lies with the organization (Fig. 4) [6].

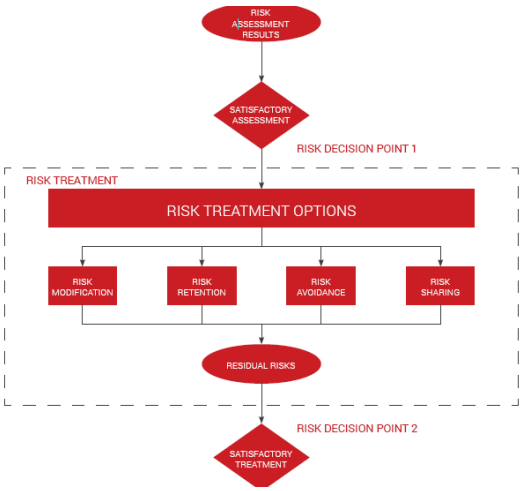

Fig.4. www.pecb.com

The analyses of ISO / IEC 27005 and of NIST SP 800-53, presented above, make evident the subjective position of the strategic leadership in both processes, namely in terms of the risk perception and the decision on how to overcome it.

The key role of the strategic leadership is decision-making. Therefore, we can define the purpose of the study to be finding mechanisms to formalize the decision-making process.

In practice, such tasks are solved by finding appropriate methods which are in line with the input conditions [5].

In this case, we can determine the following entry conditions:

- the strategic leadership holds a set of acceptable alternatives for an impact over the risk $V = \{V_i\}, i = \overline{1,m};$

- the strategic leadership has a set of states of the types of threats and protected objects (environment) $\Theta = \{\theta_l\}, l = \overline{1,k}$;

- the strategic leadership has a set of results $B = \{B_j\}, j = \overline{1,n}$ and the respective matrix of "effciencies" μ_{il} (evaluation of the risk for cybersecurity), which appear at the selection of a particular alternative and environment condition;

- distribution of the probabilities $\rho(\theta)$ in the space of the conditions of the environment $\Theta = \{\theta_l\}, l = \overline{1,k}$.

The solution of this type of task is done by using a specific approach to assess the "efficiency" of the alternatives by introducing the concept of "risk" [5].

In a one-time choice and in non-repetitive situations, strategic leadership should take into account the efficiency versus (cyber-risk) dispersion of each alternative (the different cyber-risk methods). Assuming that the state of the environment is a random variable with a mathematical expectation $M[\theta]$ and dispersion σ^2, at a random sample set $\langle \theta_1, \theta_2, \ldots \theta_N \rangle$ with volume N, the dispersion of the average arithmetic value of the efficiency $\overline{\mu} = \sum_{i=1}^{N} \mu_i(\theta)$ will be determined as follows:

$$\sigma^2[\overline{\mu}] = \frac{\sigma^2}{N}.$$

In the subject area under consideration (cybersecurity risk management), N is equal to "1" because it is not possible to take samples of the state of the environment during the management itself and then to choose an alternative, therefore, at the reduction of the dispersion of the random variable "environment" σ^2, the dispersion of the mean arithmetic value of the efficiency $\sigma^2[\overline{\mu}]$ will also decrease. In such a situation, the following condition may be met: $[M[\mu|\theta] - [\overline{\mu}]] \to 0$.

Then the " efficiency " criterion (the value of the cybersecurity risk) must account for the maximum value of the difference between the mathematical expectation and the " efficiency " dispersion for each of the possible alternatives, i.e.

$$\{M[\mu(V_i \mid \theta)] - K\sigma^2[\overline{\mu}(V_i)]\} \to \max,$$

where:

$M[\mu(V_i \mid \theta)]$ is the mathematical expectation of the " efficiency " (the value of the cybersecurity risk) for an arbitrary environmental condition;

$\sigma^2[\overline{\mu}(V_i)]$ is the dispersion of the average " efficiency " for all possible alternatives;

K - a constant defining the risk aversion of the strategic leadership according to its subjective attitude towards the choice of risky alternatives.

Under this set criterion, the "risk" will be minimal in an arbitrary state of the environment.

One of the methods for solving this type of problem uses the so-called "justifiable risk area" in an "alternative - efficiency " coordinate system where an "acceptable" (acceptable) risk area is defined by means of a "σ - indifference" function, Fig. 5.

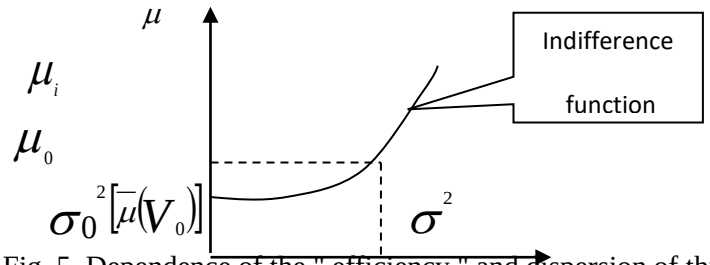

Fig. 5. Dependence of the " efficiency " and dispersion of this "efficiency" for each alternative.

In the present case μ_0, is the guaranteed efficiency of a selected alternative V_0, regardless of the accidental nature of the environment. The problem of the task will be the choice between alternatives that are equivalent $V_0 \sim V_i$ in terms of the strategic leadership. However, the relationship between the "benefits" of these alternatives may not be equivalent and $\frac{\mu_i}{\mu_0} > 1$. Such a task can be solved through a connection between μ and V as a function of the "σ - indifference" which determines the conditions of indifference of the governing body in its choice. The „σ - indifference“ curve and the K-coefficient can be determined on the basis of the subjective assessment $\frac{\mu_i}{\mu_0}$ of the managing authority for the relationship, taking into account the experience gained and the expert assessments, regulatory documents and other sources of a priori environmental information.

The identified acceptable risk for cybersecurity from the “risk assessment” phase of $R_{allowable}$ consists of the so- acceptable risk $R_{acceptable}$ in which the organization accepts the losses and a modified (reduced) risk $R_{modified}$ as a result of the adopted impact methods.

Then

$$R_{allowable} = R_{acceptable} + R_{modified}$$

Therefore, the risk management system will seek to maintain the sum of acceptable and modified risk within the permissible risk to the organization, regardless of the state of the external threats. Graphically this would look like this: Fig. 6.

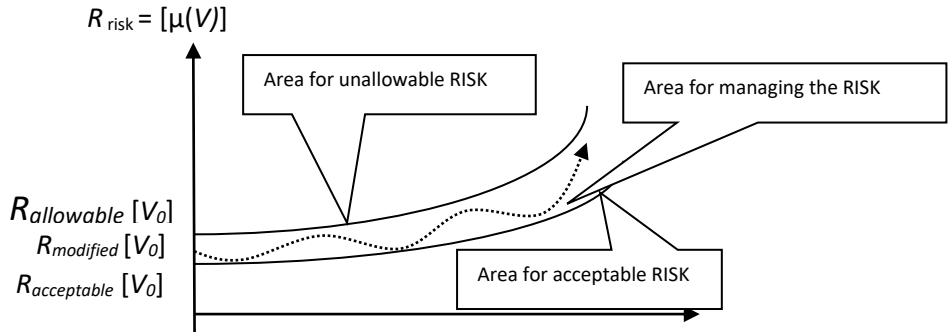

Fig. $\sigma_0^2[\bar{\mu}(V_0)]$ и $\sigma_1^2[\bar{\mu}(V_1)]$ the cybersecu $\sigma_i^2[\bar{\mu}(V_i)]$ agement system taking into account the conc

The methodology is designed to complement the complex cyber-risk management processes. To provide guidance to facilitate the organizational management through the ability to formalize subjective elements in the management processes. The proposed approach is sufficiently formal to be able to undergo automation in the future.

In conclusion, I would point out that the proposed approach does not modify the standards which have been examined and used, but merely complements them by providing opportunities for reducing subjectivity in the complex management process of the organizations.

References:

1. Risk Management for ISO 27005 Decision support - Hanane Bahtit, Boubker Regragui - International Journal of Innovative Research in Science, Engineering and Technology *Vol. 2, Issue 3, March 2013*
2. Cybersecurity Framework - Version 1.0, 2014
3. NIST SP 800-53, Ver 4.
4. ISO 27005
5. Sapundzhiev „Vzemane na reshenie v sistemite za upravlenie" – TU Sofia, 1998g.
6. www.pecb.comwww.pecb.com