The Optimization Method of the Integrated Management System Security Audit

Ilya Livshitz
ITMO University
St. Petersburg, Russia
livshitz.il@yandex.ru

Pavel Lontsikh, Sergey Eliseev
Irkutsk National Research Technical University
Irkutsk, Russia
palon@list.ru, eliseev_@inbox.ru

Abstract—**Nowadays the application of integrated management systems (IMS) attracts the attention of top management from various organizations. However, there is an important problem of running the security audits in IMS and realization of complex checks of different ISO standards in full scale with the essential reducing of available resources.**

I. Introduction

Recently, the application of integrated management systems (IMS) attracts more top management attention. Nowadays there is an important problem of running the audits in IMS and particularly, realization of complex checks of different ISO standards in full scale with the essential reducing of available resources. In a greater degree this problem is illustrative of supporting IT-Security security audit program, as far as negative consequences can lead to essential damage. The realization of IT-Security management systems (ISMS) gets more application in practice.

Moving to analysis based on risks provides the increasing of interest to rational exploitation of modern risk-oriented ISO standards. Studying the problem with realization of IT-Security audits makes the essential interest also the search of ways of IMS audit program optimization that are based on principles of continuous adaptation in the process of incoming data during one micro cycle of audit. It is supposed that new method of security audit program optimization will let us to provide more rational acceptance of the IT-Security solution.

II. Problem description

To provide stable development of modern organizations in the context of risks of different origin, it is appear to be reasonable to apply risk-oriented standard and implement the IMS [1], [7], [9]. From the point of view of controlling the IMS audits in supposed method we should notice the necessity of solution of next important practical tasks [4]:

1) The task of resources allocation for audit program;
2) The task of account of factors that influence on the depth of audit-leak program, incidents, the appearance of criminal actions, revealed earlier mismatches and in this way the volume definition of audit program;
3) The task of collection of verifiable information;
4) The task to provide the auditors with special knowledge and skills either to invite engineers.

It is necessary to admit that we should be aware of recommendations PAS-99 in IMS [9], that allows to take into account the specific requirements of carrying out combined audits, the account of risks, flexible controlling of security audit program volume with the account of last results and the importance of processes [4], [5].

At creation of the IMS the minimum requirement of the 2nd and more management systems are considered, for example: Quality management system (9000 ISO series), ISMS (27000 ISO/IEC series) and energy management systems (EnMS, 50001 ISO series). In this process, the management can accept as “basic methodology” of IMS various standards containing requirements to safety of business processes in broad economic interpretation of this term. It is known that at creation of modern IMS, besides known problems of cooperation within management systems requirements, it is necessary to provide “integrated compliance” to requirements of business.

In terms of “integrated compliance” system effectiveness of safety on criterion function of minimization of expenses and not less significant enclosed task are considered – formal compliance to legislative requirements of various regulators (so-called “compliance,” for example, of Russian State Law 63 “Digital sign,” Russian State Law 152 “Personal data,” Russian State Law 256 “Safety requirements for fuel complex objects”). It is in addition offered to use the ranks of “leaders” of branches presented in work.

III. The analysis of the existing approaches of assessment

The budget on IT-security providing, by different estimates, makes up to 10% of IT budget (budget estimates on IT-security providing are given in range from 3.6% to 3.8% from the IT budget during the period of measurements of 2010-2014). It is characteristic that the maximum value of the IT-security budget makes 6.9% in industrial branch by information for 2014.

At the same time, it should be noted that these estimates do not correlate with an assessment of dynamics of growth of incidents number: For example, the average number of the detected IT-security incidents increased in branch of power from 1.179 (2013) to 7.391 (2014), i.e., to 526%.

Pay attention to statistics of ISMS certification on the ISO 27001 standard on ranks “leaders” (Requirements of the Various Systems of Standardization – ISO 27001 and STO

Gazprom). Research showed that growth of number of the issued ISMS certificates rank from 17% to 22% for “leaders” of the 1st, over 35% for “leaders” of the 2nd rank and from 19% to 27% for “leaders” of the 3rd rank.

Problems of a risk management for CIF is convenient to arrange as realization of the cycle PDCA (or Deming’s cycle):

1) “P” (plan) – Formation of regulatory base, development of regulations, passports of risk, definition of scales of an assessment of risks, criteria of acceptance of risks, forming of summary card of risks for the organization.
2) “D” (Do) – Development of actions complex for probability reducing (alleviation of the consequences) at emergence of risks.
3) “C” (Check) – Control of completeness, timeliness and efficiency of realization of actions of complex risk management for the organization.
4) “A” (Act) – The analysis of productivity of complex of actions risk management at the level of the decision-maker and forming administrative solutions for management system for the organization optimization.

The following important question: End circuit of a cycle PDCA taking into account offered risk-focused approach. It seems reasonable for CIF to recommend:

1) Planning and carrying out internal (including technical) audits – taking into account risk-focused standards (for example ISO 27001 or the new ISO 9001 version) [6-9].
2) Formation of the unified register of discrepancies in the integrated system of management by all types of audits and the analysis of this register from a risk management position (identification of critical points of refusal, the analysis of “cascading” of risks, studying of statistics and so forth)
3) Formation of system of expeditious informing the management (for example, based on the standard of management of a business continuity – ISO 22301 or as a part of IMS)
4) Accurate distribution of responsibility and powers on each task in the approved program of internal audits, the plan of processing of risks and so forth.

The risk-focused approach is the main standard for realization the ISO standard series 31000. This standard contains the scheme of a risk management processes which reflects the closed risk management cycle consisting of the main stages – definition of a context, assessment of risk, impact on risk, of monitoring and revision, an exchange of information and consultation (see Fig. 1).

Process of an assessment of risk consists of three consecutive stages – identifications of risk, the analysis of risk and estimation of risk. Preliminary formation of scales for quantitative or qualitative estimation of risks, comparisons of the received estimates to the criteria formed earlier and preparation of the register of risk for processing necessarily is supposed.

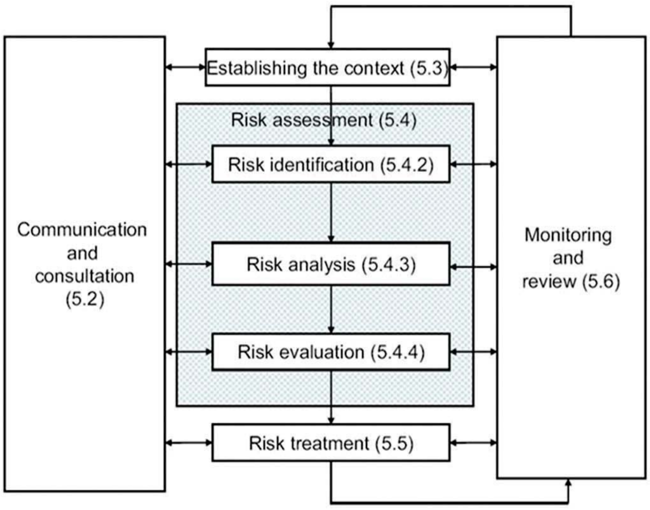
Communication and consultation (5.2)
Establishing the context (5.3)
Risk assessment (5.4)
Risk identification (5.4.2)
Risk analysis (5.4.3)
Risk evaluation (5.4.4)
Risk treatment (5.5)
Monitoring and review (5.6)

Fig.1. Process of a risk management of ISO 31000

It is known that the term “Risk” (according to item 2.1 of the standard) means “influence of uncertainty on the purposes.” Thus in five notes it is specified that influence can be positive and/or negative; the purposes of the organization can have various aspects (for example, financial); the risk is often characterized by the reference to potentially possible events, consequences or their combinations, and uncertainty is the state consisting in insufficiency of information concerning an event, its consequences or its opportunity. All modern standards (such as ISO/IEC 27000 series are based on risk-oriented approach) [1-3].

IV. PRINCIPLES OF ORGANIZATION OF FLEXIBLE AUDITS

The suggested method of optimization of the IMS audit program is based on next basic principles [10 – 12]:

1) We input the concept of integral evaluation of IT-Security that includes the specific group index of evaluation of all submitted for IT-Security audit processes - $R_{\mathbf{ISMS}}$. This group index defines with the help of specific indexes – $R_{PR,}$ multiplied on their weight coefficient in dependence of process importance in the IT-Security organization for the concrete object of evaluation.
2) After running the basic IT-Security audit, its condition is valued for the purpose of accordance with demands of audit criteria, and also its influence on IT-Security integral evaluation of concrete object of evaluation.
3) Next IT-Security audits are held by the given method that uses flexible approach: those processes, that have the most priority in the IT-Security for the concrete object of evaluation, and where the essential mismatches of last audit were revealed, are exposed of more detailed check.
4) Frequency and detail, which must be differentiated for different checked processes, comports with IT-Security too. For example, definite groups of processes, that have priority meaning in integral evaluation (for example, it depends on the model of actual threats of IT-Security), are exposed more detailed and often with

audits. The processes, that have the lowest priority in the integral evaluation for the concrete object of evaluation, are checked seldom and less detailed.

5) The depth of check and frequency of audits, each time for k-audit in micro cycle PDCA, defines in dependence of oncoming function of integral evaluation for the concrete object of evaluation to some stated objective index – Rtarget for complex evaluation of concrete object of evaluation security.

In addition we should note the importance of implementation of new standard, ISO 55000 [6-8] – as many assets are not ruled in a proper manner. Accordingly, the appliance of demands of one implemented standard (for example, modern ISO 27001) substantially relieves the solution of standard problems of security, that are solved simultaneously, therefore they must be checked simultaneously within the context of combined audits for IMS in organization (for example, ISO 9001, ISO 50001, ISO 27001) [1-4], [5-8].

V. Statement of the Problem

For the evaluation of a degree of providing ITSM conformance on the IMS audits to presented requirements of IT-Security we use private and group IT-Security indexes.

For the purposes of realizing IMS audits in the aspect of providing IT-Security we suggest to use the index of effectiveness of MS IT-Security $R_{\mathbf{ISMS}}$, which we can calculate in each cycle of k-audit using the additive formula with the account of α-weight coefficients and index of effectiveness of each concrete process of IT-Security – $R_{\mathbf{PR}}$:

$$R_{ISMS} = \sum_{i=1}^{n} \alpha_i \bullet R_{\Pr i} \qquad (1)$$

in this case :

$$\sum_{i=1}^{n} \alpha_i = 1$$

In its turn, indexes of effectiveness of each concrete i-process of IT-Security – $R_{\mathbf{PR}}$ are calculated by additive formula with the account of β-weight coefficients and indexes of IT-Security metrics for each concrete i-process of IT-Security – K_{KPI}:

$$R_{\Pr_i} = \sum_{j=1}^{m} \beta_j \bullet K_{PKIj} \qquad (2)$$

in this case:

$$\sum_{j=1}^{m} \beta_j = 1$$

The coefficients of relevancy of private indexes of IT-Security, that are used by calculation of IT-Security group indexes, must be equal to 1 that provides ritualization of all indexes in additive formula above (1) and (2). Accordingly, the final index of effectiveness of MS IT-Security $R_{\mathbf{ISMS}}$ must maximize reaching 1:

$$R_{ISMS} = \sum_{i=1}^{n} \alpha_i \bullet R_{\Pr i} \to 1 \qquad (3)$$

In the process of IMS audits, the constant measuring of current nonconformance for k-audit RISMS is measured as discrepancy with the objective (maximal) index:

$$\Delta R = 1 - R_{ISMS} = \sum_{i=1}^{n} \left[\alpha_i \bullet (1 - R_{\Pr i}) \right] \qquad (4)$$

Regarding the results of all audits, that are carried out in a strict accordance with IMS audit program, we fill in the following matrix with the account of IT-Security processes – PR, IT-Security audits – k-audits and IT-Security metrics – KPI.

VI. Basic optimization cycle of IMS audit program

In terms of known audit standards (in particular [4,5]), we offer a method of multistage optimization of IMS audit processes for the complex industrial facilities, which let us to provide the system of coordination, distribution of recourses and system of effective reduction of results of IMS audits till the person who takes decision.

This method consists of scientifically grounded and object-oriented immediate functioning of IT-Security subsystem within IMS and it differs from existing methods with cyclic continuous evaluation of effectiveness on the basis of optimal system of IT-Security numeral indexes (metrics). The offered method consists of two connected cycles of optimization of IMS audits program that differs with the existence of:

1) Basic optimization cycle, which characterizes the effective carrying out of IMS audits in terms of evaluation of efficiency for each PRi- IT-Security process, each KPIj – IT-security metric, and also it defines cycles of resources optimization in audits program: of depth (“Scope”), size of auditor’s sample, number of involved auditors (engineers) and etc.

2) Fast block of evaluation of efficiency of correction measures and corrective actions in current k-audit, that touches the changes each of next process of IT-Security and next k+1 audit program. It is also provided fast transfer to evaluation of efficiency indexes of IMS – $R_{\mathbf{ISMS}}$ in k-audit and k+1 audit for the constant and effective optimization of all IMS audit program.

Let’s consider the basic optimization cycle of IMS audit program that was built with the account of audit’s formal ISO standards requirements and ISAGO standards supported with new components (see Fig. 2):

- Formation efficiency evaluation of each k-audit;
- Formation of fast efficiency evaluation of correction(corrective actions);
- Formation of quick back link in the current audit cycle;

- Formation of system reaction – complication or easing depending on current integral evaluation in current audit cycle;
- Formation of integral evaluation of IMS security.

Preconditions (data inputs) for the start of basic optimization cycle of audit program are given:

- T_0 – basis period of IT-Security audits;
- S_0 – basic (planned) price of IT-Security audits;
- V_0 – basic volume of IT-Security audits (number of units);
- F_0 – basic list of functional questions of IT-Security audits;
- O_0 – basic list of attended IT-Security audit objects.

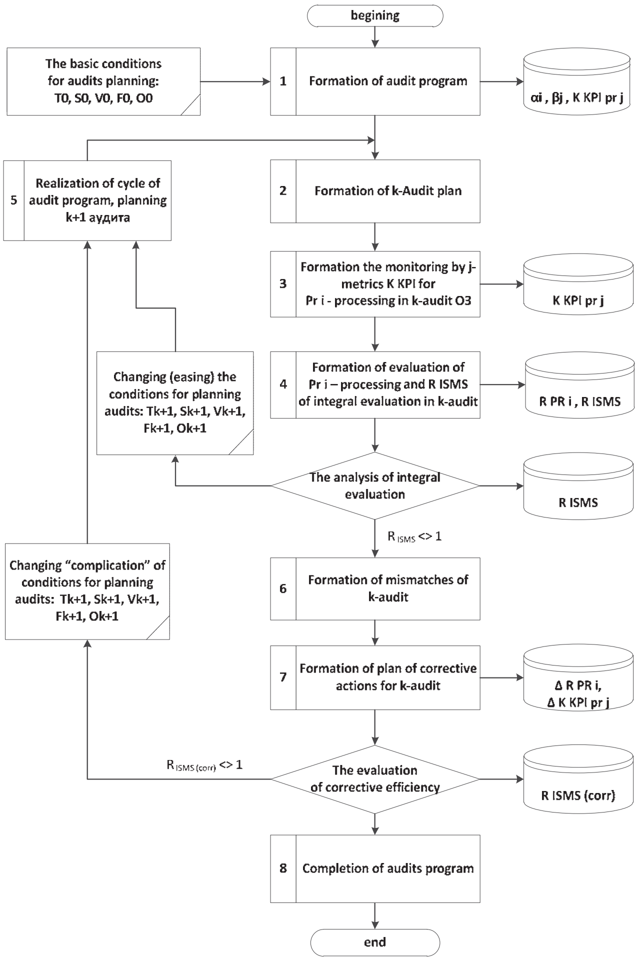
begining
The basic conditions for audits planning: T0, S0, V0, F0, O0
1 Formation of audit program
αi , βj , K KPI pr j
5 Realization of cycle of audit program, planning k+1 аудита
2 Formation of k-Audit plan
3 Formation the monitoring by j-metrics K KPI for Pr i - processing in k-audit O3
K KPI pr j
Changing (easing) the conditions for planning audits: Tk+1, Sk+1, Vk+1, Fk+1, Ok+1
4 Formation of evaluation of Pr i – processing and R ISMS of integral evaluation in k-audit
R PR i , R ISMS
The analysis of integral evaluation
R ISMS
R ISMS <> 1
Changing "complication" of conditions for planning audits: Tk+1, Sk+1, Vk+1, Fk+1, Ok+1
6 Formation of mismatches of k-audit
7 Formation of plan of corrective actions for k-audit
Δ R PR i, Δ K KPI pr j
R ISMS (corr) <> 1
The evaluation of corrective efficiency
R ISMS (corr)
8 Completion of audits program
end

Fig.2. Basic optimization cycle of IMS audit program

VII. THE QUICK BLOCK OF EFFICIENCY EVALUATION OF IMS AUDIT PROGRAM

The quick block of efficiency evaluation of correction measures and corrective actions in the current k-audit, which touch the changes of next process and also the following in the k+1 audit program and quick move to the evaluation of efficiency indexes of IT-Security MS – $R_{\mathbf{ISMS}}$, is shown in the Fig.3.

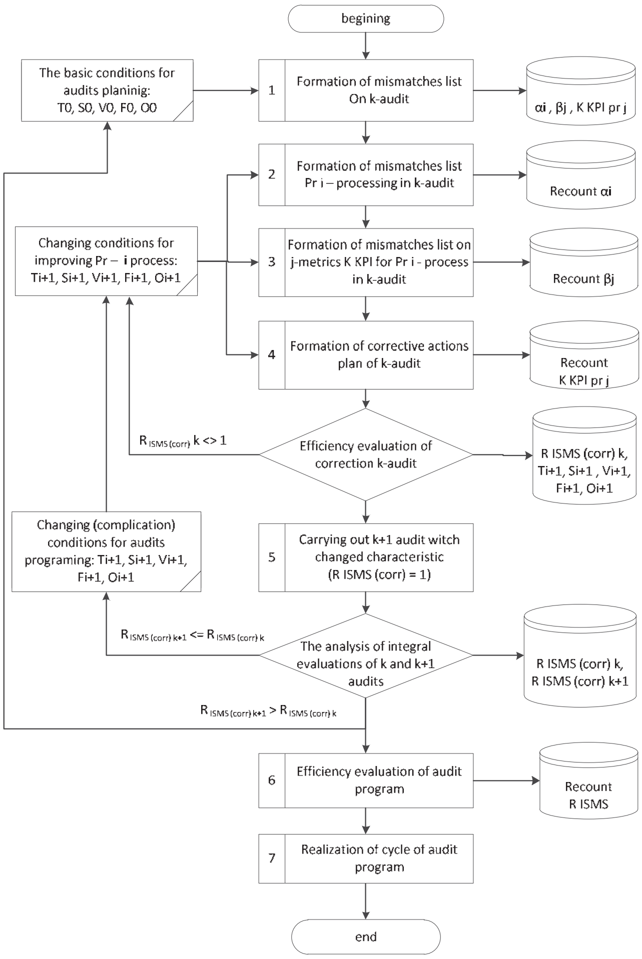
begining
The basic conditions for audits planinig: T0, S0, V0, F0, O0
1 Formation of mismatches list On k-audit
αi , βj , K KPI pr j
2 Formation of mismatches list Pr i – processing in k-audit
Recount αi
Changing conditions for improving Pr – i process: Ti+1, Si+1, Vi+1, Fi+1, Oi+1
3 Formation of mismatches list on j-metrics K KPI for Pr i - process in k-audit
Recount βj
4 Formation of corrective actions plan of k-audit
Recount K KPI pr j
R ISMS (corr) k <> 1
Efficiency evaluation of correction k-audit
R ISMS (corr) k, Ti+1, Si+1 , Vi+1, Fi+1, Oi+1
Changing (complication) conditions for audits programing: Ti+1, Si+1, Vi+1, Fi+1, Oi+1
5 Carrying out k+1 audit witch changed characteristic (R ISMS (corr) = 1)
R ISMS (corr) k+1 <= R ISMS (corr) k
The analysis of integral evaluations of k and k+1 audits
R ISMS (corr) k, R ISMS (corr) k+1
R ISMS (corr) k+1 > R ISMS (corr) k
6 Efficiency evaluation of audit program
Recount R ISMS
7 Realization of cycle of audit program
end

Fig.3. The quick block of efficiency evaluation of IMS audit program

VIII. THE BASE MODEL FOR THE ISM AUDITS

The IMS model contains all the basic content for performing audits (criteria, evidence, object surveillance audit). It allows to create assess the IT-security level [8-9]. The following important question: End circuit of a cycle PDCA taking into account offered risk-focused approach. It seems reasonable for CIF to recommend:

- Planning and carrying out internal (including technical) audits – taking into account risk-focused standards (for example ISO 27001 or the new ISO 9001 version).
- Formation of the unified register of discrepancies in the integrated system of management by all types of audits and the analysis of this register from a risk management position (identification of critical points of refusal, the analysis of "cascading" of risks, studying of statistics and so forth)
- Formation of system of expeditious informing the management (for example, based on the standard of

management of a business continuity – ISO 22301 or as a part of IMS)

- Accurate distribution of responsibility and powers on each task in the approved program of internal audits, the plan of processing of risks and so forth.

The modern ISO standards rely on uniform risk-focused approach (based on ISO 31000). Respectively, important advantage of all modern systems of management is the requirement of continuous improvement of productivity, which promotes proper response to dynamic changes of a situation, especially manifestations of actual threats for CIF:

- Increase in number of leakages of sensitive information (commercial, technical, financial, personal);
- Strengthening of critical consequences of loss of assets, valuable to business;
- Strengthening of degree of consequences of blocking of work of critical systems (financial, transaction, logistic, information and so forth);
- Impossibility of fast replacement, repair or purchase of new expensive import equipment (technologies) or accessories.

The example of realization of process of management of risk for the cycle phase “Plan” “Plan- Do-Check-Act” (PDCA) is shown in Fig. 4.

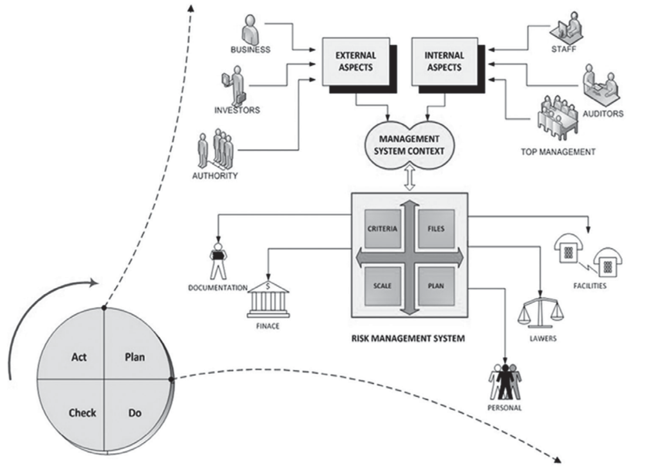

Fig.4. Process of management of risks for the cycle Plan-Do-Check-Act phase “Plan”

IX. Responsibility when working with personal data

Responsibility of senior management, private officials and private individuals established in the following laws and regulations:

Article 24 of the law No. 152-FZ "On personal data" determines the types of liability for violation of Federal law. Persons guilty in violation of requirements of the law "On personal data" shall bear civil, criminal, administrative, disciplinary and other stipulated by the legislation of the Russian Federation responsibility. Consider liability under the above laws with an emphasis on responsibility for violation of requirements on protection of personal data.

In article 17 of the Federal law "On information, information technologies and protection of information" provides that persons whose rights and legitimate interests have been violated in connection with disclosure of restricted information or other misuse of such information, may apply in the prescribed manner for judicial protection of their rights, including claims for damages, compensation for moral harm, protection of honor, dignity and business reputation.

The civil code of the Russian Federation

Civil code Article 946. Secrecy of insurance the Insurer may not disclose received by it as a result of their professional activities, information about the policyholder, insured person and beneficiary, their health, and also about a property status of these persons. For violation of the secrecy of insurance the insurer, depending on the sort of the broken rights and character of infringement bears responsibility in accordance with the rules provided for by article 139 or article 150 of this Code.

The criminal code provides for punishment according to article 137, 140 and 272.

Criminal code, Article 137. Violation of privacy

Illegal collection or dissemination of information about a person's private life constituting its personal or family secret, without his consent or spreading this information in a public statement, publicly shown product or mass media - shall be punished by a fine of up to two hundred thousand rubles or the salary or other income for a period of eighteen months, or by compulsory works for a term of up to three hundred and sixty hours, or correctional labor for a term up to one year, compulsory works for a term of up to two years with deprivation of the right to occupy certain positions or engage in certain activities for a term up to three years or without such, or by arrest for a term up to four months or by deprivation of liberty for a term up to two years with deprivation of the right to occupy certain positions or engage in certain activities for a term up to three years.

X. Model of formation of the value added in the ISM

The management forms the business purposes of the organization proceeding from a wide set of entrance factors impact on which have various interested parties. In the presented model the main interested parties – competitors and regulating boards, which total influence makes the dominating impact on any organization. After formation of the business purposes business processes in the organization are built (it belongs also to processes of an outsourcing and/or out staffing equally). One of the purposes of formation of system of business processes is definition of requirements to resources (for example, involvement of the third-party personnel possessing rare qualification).

The following stage concerns the accounting of assets of the organization (in relation to CIF it is correct to tell about various categories of the equipment, means of communication, licenses for the software, the personnel, etc.). On this stage metrics of an assessment of effective use of assets of the organization have to be offered and coordinated. At the following stage determination of productivity of business processes of the organization on the basis of the coordinated metrics because of operating process is possible only on the basis of reliable estimates, factual (ISO/IEC 27001:2013) [1].

In end of a cycle, it is necessary to execute an assessment of productivity of business processes of the organization and to make the adequate administrative decision – is it enough to carry out routine procedure of continuous improvement, without essential changes, or cardinal actions for optimization of activity of the organization are necessary.

XI. Conclusion

Refined security model of complex industrial object on the basis of a risk-based approach both for the energy complex and airport; while noting the importance of the “closing” principle of PDCA cycle in the creation and evaluation of management systems.

Given method of IMS audit program optimization is based on the modern ISO risk-oriented standards and let to provide the constant optimization of carrying out the IT-Security audits on the basis of joined flexible adaptive algorithms.

References

[1] ISO/IEC 27001:2013. Information technology. Security techniques. Information security management systems. Requirements, International Organization for Standardization. 2013. p.23.

[2] ISO/IEC 27000:2014. Information technology. Security techniques. Information security management systems. Overview and vocabulary, International Organization for Standardization. 2014. p.31.

[3] ISO/IEC 27004:2009. Information technology. Security techniques. Information security management systems. Measurement, International Organization for Standardization. 2009. p.55.

.

[4] ISO19011:2011.Guidelines for auditing management systems;

[5] ISO 17021:2011. Conformity assessment – Requirements for bodies providing audit and certification of management systems;

[6] ISO 55000:2014 Asset management – Overview, principles and terminology // International Organization for Standardization, 2014. 19 p.

[7] ISO 55001:2014 Asset management – Management systems – Requirements. International Organization for Standardization, 2014. p.14.

[8] ISO 55002:2014 Asset management – Management systems – Guidelines for the application of ISO 55001. International Organization for Standardization, 2014. p.32.

[9] PAS-99:2012 «Specification of common management system requirements as a framework for integration»

[10] Livshits I. The urgency of the application of information security metrics to assess project performance information security management systems. *Quality Management*, 2015, Vol. 1. pp.74 - 81.

[11] Livshits I. Approaches to solving the problem of taking into account losses in the integrated management system. *Informatization and Communication*. - 2013, № 1. pp 57 - 62.

[12] Livshits I. The approaches to the use of an integrated management system model for the audit of complex industrial facilities - airport complexes. *Proceedings SPIIRAS*. - 2014, Vol. 6. pp.72 – 94.

[13] Livshitz, I. (2014), Approaches to the application of the integrated management system model for carrying out audits for complex industrial facilities – Airport complexes. *Trudy SPIIRAN*, Vol. 6, pp. 72-94. (In Russia).

[14] ISO 22301. (2012), Societal Security – Business Continuity Management Systems – Requirements. Geneva, Switzerland: International Organization for Standardization.

[15] ISO/IEC 20000-1. (2011), Information Technology – Service Management - Part 1: Service Management System Requirements. Geneva: International Organization for Standardization.

[16] Federal law of Russian Federation 256-FZ. Available from http://base.garant.ru/12188188. [Last accessed on 2016 Jul 01].

[17] Il’in, V., Sadovnichi, V., Sendov. B. Theory of limit. Mathematical Analysis. Vol. 1. Ch. 3. Moscow: Prospect. p. 672. (In Russia).

[18] ISO/IEC 27005. (2011), Information Technology – Security Techniques – Information Security Risk Management. Geneva, Switzerland: International Organization for Standardization.