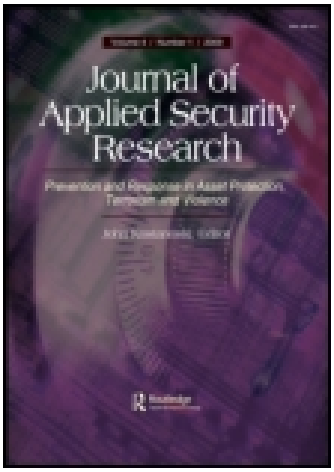
This article was downloaded by: [Bulgarian Academy of Sciences], [Kiril Stoichev]
On: 26 January 2015, At: 21:27
Publisher: Routledge
Informa Ltd Registered in England and Wales Registered Number: 1072954 Registered office: Mortimer House, 37-41 Mortimer Street, London W1T 3JH, UK



Journal of Applied Security Research
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/wasr20

Selection of an Alternative Method for Establishing Security Levels

Kiril Stoichev[a]
[a] Institute of Metal Science, Equipment and Technologies with Hydroaerodynamics Centre, Bulgarian Academy of Sciences, Sofia, Bulgaria
Published online: 22 Jan 2015.

CrossMark
Click for updates

To cite this article: Kiril Stoichev (2015) Selection of an Alternative Method for Establishing Security Levels, Journal of Applied Security Research, 10:1, 48-59, DOI: 10.1080/19361610.2015.972269

To link to this article: http://dx.doi.org/10.1080/19361610.2015.972269

PLEASE SCROLL DOWN FOR ARTICLE

Taylor & Francis makes every effort to ensure the accuracy of all the information (the "Content") contained in the publications on our platform. However, Taylor & Francis, our agents, and our licensors make no representations or warranties whatsoever as to the accuracy, completeness, or suitability for any purpose of the Content. Any opinions and views expressed in this publication are the opinions and views of the authors, and are not the views of or endorsed by Taylor & Francis. The accuracy of the Content should not be relied upon and should be independently verified with primary sources of information. Taylor and Francis shall not be liable for any losses, actions, claims, proceedings, demands, costs, expenses, damages, and other liabilities whatsoever or howsoever caused arising directly or indirectly in connection with, in relation to or arising out of the use of the Content.

This article may be used for research, teaching, and private study purposes. Any substantial or systematic reproduction, redistribution, reselling, loan, sub-licensing, systematic supply, or distribution in any form to anyone is expressly forbidden. Terms & Conditions of access and use can be found at http://www.tandfonline.com/page/terms-and-conditions

Journal of Applied Security Research, 10:48–59, 2015
Copyright © Taylor & Francis Group, LLC
ISSN: 1936-1610 print / 1936-1629 online
DOI: 10.1080/19361610.2015.972269

Routledge
Taylor & Francis Group

Downloaded by [Bulgarian Academy of Sciences], [Kiril Stoichev] at 21:27 26 January 2015

Selection of an Alternative Method for Establishing Security Levels

KIRIL STOICHEV
Institute of Metal Science, Equipment and Technologies with Hydroaerodynamics Centre, Bulgarian Academy of Sciences, Sofia, Bulgaria

On July 14, 2014 in Journal of Applied Security Research *an article was published named "Security Levels of Critical Infrastructure." It presented a vision for the creation of a unified methodology for integrating existing standardization, normative, and institutional tools to build higher levels of security for critical infrastructures. But this is only the frame to be filled with content. This content, however, may be the result of different approaches to formulate the packages of requirements for the separate elements of an integrated security system for the organizations, detailed in the generally accepted levels of security and protection. The focus of this publication is to show the positive and negative effects of the choice of the alternative to create a single document, with the standardization requirements for building a comprehensive, unified system for security and protection of sites of the critical infrastructure based on a clearly defined and documentary secured matrix of ascending levels of security for the organizations.*

KEYWORDS Security levels of critical infrastructure, standardization document for security levels of critical infrastructure, alternative approaches, integrated security management system

INTRODUCTION

The security that can be achieved through technical means is limited, and should be supported by appropriate management and procedures (ISO/IEC 27002, 2005).

Address correspondence to Kiril Stoichev, Institute of Metal Science, Equipment and Technologies with Hydroaerodynamics Centre, Bulgarian Academy of Sciences, 67 Shipchenski Prohod Blvd. Sofia, Bulgaria 1574. E-mail: kstoichev@ims.bas.bg

Color versions of one or more of the figures in the article can be found online at www.tandfonline.com/wasr.

Downloaded by [Bulgarian Academy of Sciences], [Kiril Stoichev] at 21:27 26 January 2015

Following this maxim, in the article "Security Levels of Critical Infrastructure" in *Journal of Applied Security Research* (Stoichev, 2014), levels of security for critical infrastructure, which could be defined and can be in the base of the development of an Integrated Security Management System (ISMS), were presented. The levels are as follows:

- 1st level–Risk Assessment (1) and Internal Security (2);
- 2nd level–Risk Assessment, Internal Security and External Security (3);
- 3rd level–Risk Assessment, Internal Security, External Security, Quality Assurance (4) and Safety (5);
- 4th level–Risk Assessment, Internal Security, External Security, Quality Assurance and Safety, Information Security (6), Human Resources (7), and Financial Security (8);
- 5th level–Risk Assessment, Internal Security, External Security, Quality Assurance and Safety, Information Security, Human Resources, Financial Security, Environmental Security (9), and Social Corporate Responsibility (10);
- 6th level–All of the above and Business Continuity Management (11).

Of course this is only a conceptual proposal. The structure and content of these levels is still controversial and the scientific and professional communities will determine their final configuration. But that is not the issue. It is essential that after the final levels of security for the organizations[1] are determined, a practical mechanism for their creation and evaluation of their readiness for use is created; that is, to assess the level of security of the organization.

In my opinion, this mechanism can be "dressed" in an international standard in which to describe the requirements for the different levels of security. As for the assessment of their readiness to use and the overall assessment of the security of the organization, it is also necessary to establish a unified methodology, applied by an individual standard or other document which to unify the efforts in this direction. Only in this way we will have an objective assessment and comparison tool for the security systems in the different organizations. At present there is no such approach in the evaluation of various systems in organizations, created based on international standards. For example, in assessing the underlying subsystem[2] in the management of organizations—the system of quality assurance—there is no single document requirement for making this assessment (listed later, ISO 19011 [2011] and ISO/IEC 17021 [2011] regulate the requirements for the preparation of the audit teams and certifying organizations, but do not provide guidance on the objectives that are set during the construction of the various elements of the system and the criteria for assessing the achievement of these objectives). Each certifying organization has developed its own evaluation methodology, which applies in the course of auditing the relevant systems. The result is that thereare huge differences in the

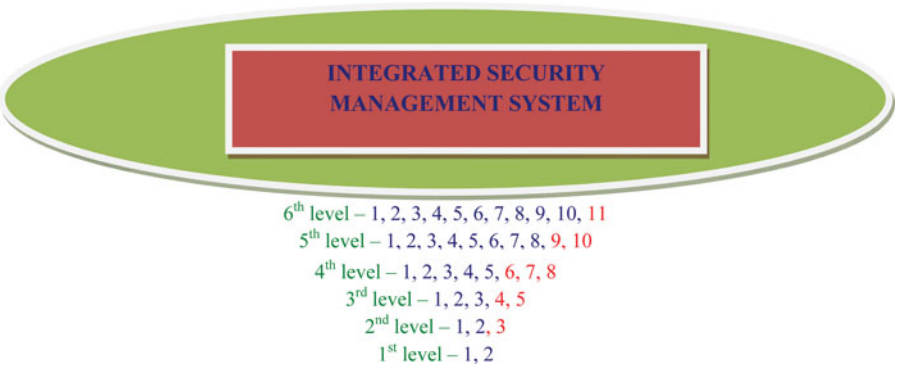


FIGURE 1 Integrated security management system.

functioning of the systems for quality assurance of the organizations, created and evaluated by various consulting and certifying organizations based on different methodologies, although the basic starting point is a single standardized document—ISO 9001:2008 (in 2012, the structure of ISO 9000 is accepted by the International Organisation for Standardization as standard in creating standardization documents regulating the requirements for the subsystems management). If the latter is normal to evaluate the systems for quality assurance in which evaluation with appreciation of poorly functioning system can result in the worst case, loss of market positions, a similar situation is absolutely unacceptable for the evaluation of the security systems of organizations where the results are related to the health and lives of not only those working in the organization, but to the people of the surrounding environment, too.

As a result of these needs, the objective and purpose of this article are formulated, namely, to try to outline approaches to create an international standard document regulating the requirements for a fixed matrix of ascending levels of security for organizations and to present the main points of sample methodology for their evaluation.

Here it may be noted that the establishment of security levels of the sites of critical infrastructure is not an end in itself. The end result of their construction and operation should be the formation of an ISMS for organizations (Fig. 1). Some will say that such a document, which includes regulations establishing such a system, will be available after the development and approval of ISO/DIS 34001 Security Management System. Unfortunately, now it should be noted that the procedure described in this standard methodology does not exceed the limits of risk assessment (RA) and risk management (RM). Of course, these two tools are the first and indispensable condition for creating and ensuring the security of the organization, but by no means are the only. At the same time they should not include any extraneous elements

Downloaded by [Bulgarian Academy of Sciences], [Kiril Stoichev] at 21:27 26 January 2015

to them, just to justify the theory that RA and RM are sufficient to guarantee the security of the organizations. Assuming such an approach, it will be difficult to answer the question whether the organization has established the required level of security to ensure the continuity of their business.

The proposed approach in this article, to build an integrated security management system, recognizes the basic fundamental nature of RA and RM, while covering all security components/subsystems of the management system of the organization and focuses on detailed individual requirements as for these elements and builds on the basic levels of security. That is, there are two main "pillars," comprehensiveness and detail.

Downloaded by [Bulgarian Academy of Sciences], [Kiril Stoichev] at 21:27 26 January 2015

APPROACHES TOWARD THE CREATION OF STANDARDIZATION DOCUMENT FOR SECURITY LEVELS

There are at least three alternative approaches to define the requirements for different levels of security and their integration into a single mechanism or standardization document to become a guiding tool for building ISMSs for organizations:

- Formation of the different levels of security by building the subsystems of the management system of the organization based on existing international standards. For example, if you want to build a sixth level of security you must build the subsystems Risk Assessment, Internal Security, External Security, Quality Assurance and Safety, Information Security, Human Resources, Financial Security, Environmental Security, Social Corporate Security and Business Continuity Management, using the existing standardization documents for them;
- Using the approach "tailoring," that is, out of the existing standards only including those requirements that we believe relate to the establishment of appropriate levels of security in the organization's internal safety management processes;
- Creating an entirely new international standardization document that incorporates the requirements for the creation of security levels and the development of a comprehensive ISMS for organizations.

The first approach is seemingly easy and its implementation would expedite the process of putting into practice the idea of building levels of security of organizations as a key tool to enhance their security. But is this so? Let us look at it and comment on the positive and negative sides.

We can formulate the following positive effects of its implementation, but not limited to:

- Requirements to individual subsystems of the management of the organization are standardized and easily accessible (everyone can buy the relevant standards).
- There are clear rules and established practice of the application of those standards.
- There are well-trained consulting organizations that successfully consult with organizations wishing to establish such subsystems based on existing international standards.
- There are proven-in-time national and international certification organizations that are able to provide a relatively accurate assessment of the readiness of organizations to use the corresponding built subsystems.
- There are streamlined systems for staff training that build and maintain the subsystems of the management system of the organization.
- The construction of these subsystems and their inclusion as elements in the levels of security for critical infrastructure is an objective criterion for assessing the readiness of organizations to provide the needed level of security.

However, there are a number of negative aspects that must be considered when assessing this approach:

- The construction of these subsystems (based on international standards)—their certification and commissioning requires a long period of time (a minimum of 2 years for each of the subsystems).
- This will require significant funds for the construction, certification, and maintenance of the subsystems (for each of them tens of thousands of euros), in which case no one can guarantee that the expected results in terms of security will be obtained.
- Finally, it will require additional efforts to integrate these subsystems into a single ISMS.

The most important of the positive effects is the one in which one can create conditions for an objective assessment of the readiness of organizations to provide the needed level of security, but it is only at first sight. In my opinion, in order to make a decision with respect to this approach, the necessary additional efforts to integrate these subsystems into a single ISMS must be defined. In many cases, depending on the knowledge and skills of the staff who will maintain these systems, the effect of linking the subsystems may be a mechanical collection of requirements without providing their real and full commitment to the objectives of enhancing the security of the organization. Adding that this process will be difficult and from the unequal structures of standards that describe the requirements for each subsystem, we will see that this approach can bring us false reassurance and in no case will achieve the main objective of the organization—to enhance its security to

Downloaded by [Bulgarian Academy of Sciences], [Kiril Stoichev] at 21:27 26 January 2015

the extent necessary to ensure continuity of its operations in all situations and conditions.

I do not focus on the other negatives mentioned previously, but it is not without significance that the essential financial, human, and material resources should be provided for the formation of security levels and this may be disincentive for the organizations. So despite the fact that the negative moments are less than the positive ones, their relative importance is considerable, and that determined my opinion that this approach should not be used for the purpose of constructing an ISMS based on the established security levels.

The second approach, which takes from the existing standards only those requirements that I believe relate to the establishment of appropriate levels of security (tailoring), is extremely flexible and adaptable, but when it is observed we still obtain both positive and negative effects. Its positives can be reduced to the following:

- As already mentioned, flexibility and adaptability, both of which are extremely valuable in taking the specifics of the respective organizations. The latter is important in view of the fact that, in this case, success can also be given with a cost-effective approach, i.e., to find the best option, in which the planned results are to be obtained by the best combination of financial, human, and material resources.
- It should also be noted the shorter terms (compared to the first approach) in which appropriate levels of security and the ISMS can be set up.
- Relatively smaller amounts of funds are necessary to build the levels of security and system, as well as for their maintenance.

The negative effects can be outlined in the following frame:

- The need for numerous, highly qualified personnel to build levels of security and of the integrated system.
- The lack of a single, unified, and hence an objective tool to assess the readiness of the organization to implement and maintain appropriate levels of security and ISMS.
- As a consequence of the latter, there will be a lack of confidence by the relevant state and insurance authorities in respect of the security of the organization.

Leaving the insurance system for the purposes of achieving an acceptable level of security of critical infrastructures in the short term, we can with a high degree of certainty note that this approach is preferable to the first approach described previously. Moreover, there are numerous and highly qualified specialists in the law-enforcement authorities that can be trained very quickly and proceed immediately to the construction of ISMSs. But at

Downloaded by [Bulgarian Academy of Sciences], [Kiril Stoichev] at 21:27 26 January 2015

first why don't insurance agencies and organizations use this approach? For them, and for the business organization that seeks to insure its business, it will be useful to use this approach to create a security, which will be much better and will bring many more benefits than the lack of established levels of security or ISMS.

The third approach combines both positive and negative sides of the first two approaches. Positive results from its use can be summarized in the following directions:

- There will be created a focused standardization document that unlike the first approach, which adjusts for security requirements in other documents for other subsystems, will ensure that all aspects of the process are covered to ensure the security of an organization.
- There will be an objective tool to assess the readiness of the organization to achieve and maintain a reliable ISMS.
- The funds to build the levels and the system will be relatively smaller than in the application of the first approach.
- The use of such standardization documents of organizations will increase and strengthen their credibility by public authorities and insurance companies.

But the approach also has its negatives such as:

- This also requires an extended period of time for a single international standard that describes the requirements for the security levels and the creation of an integrated security management system for organizations. This will slow down in short term the increase of the security of critical infrastructure.
- There will be the need to develop new training programs for all who are involved in the preparation, development, evaluation, and maintenance of the levels and the ISMS (but this is typical and for the first two approaches).

Ultimately, this approach solves most of the problems of the previous approaches, a significant negative effect of the implementation is relatively lengthy period that is required for the establishment of international standard and its practical application. But on the other hand, if the approach is adopted, then we will have a long-term strategic vision of how to create conditions for a continuous process of improving the security of the organizations.

Why is this approach preferred, aside from the previously mentioned positive effects? The answer is in itself—it is a systematic approach that ensures a very high level of reliability obtained as a result of its use. Compared to the other approaches, it would be extremely useful for the insurance bodies which on its basis can improve their best practices and increase planned

Downloaded by [Bulgarian Academy of Sciences], [Kiril Stoichev] at 21:27 26 January 2015

profits (by reducing the expected loss due to the higher level of security to the insurance organizations).

In conclusion of this section, it is necessary to note that you need in the fastest possible way to start the training of specialists in the field of security toward their learning and use of a systematic approach in the implementing of the ISMSs in the organizations. We must be convinced that only RA and RM, however they may be accompanied by a well-developed plan for crisis management, are not enough to say with reasonable certainty that we are ready to adequately respond to the colorful palette of daily increasing and evolving threats to life and health of our employees and the general public.

METHODOLOGY FOR ASSESSING SECURITY LEVELS

This stage of the creation and development of an ISMS is extremely sensitive.

It is well known that there are three approaches for evaluation of a management system—"internal audits" (first party), "audits conducted by customers on their suppliers" (second party), and third party certification. From the previously mentioned three approaches, only the internal audit or first party certification is acceptable for the respective organization. The other two approaches, at this stage, are unacceptable for critical infrastructure at least because it is not appropriate externally for the organizations in which people have access to their most well-kept secrets.

Certification by a second and a third party are the ways that build trust of the public authorities (talking about critical infrastructure that is under conservatorship by the government) and the general public in the ability of critical infrastructures to fulfill their activities and achieve goals. This trust is impossible if they do not have objective evidence of the security of these organizations, but this dilemma can be resolved. This can be done by creating specialized government structures or empowering existing ones, established by the government to assess the security level of critical infrastructures.

Before we get to this point, however, let's look at the current theory, practice, and tools for assessing the management systems and the elements of a comprehensive security of the organizations.

In the first place, it is vital to note the existence of ISO 19011 (2011), "Guidelines for auditing management systems," which provides guidance on the management of an audit program and on the planning and conducting of an audit of the management system, as well as on the competence and evaluation of an auditor and an audit team. It provides guidance for all users, including small- and medium-sized organizations, and concentrates on first party and second party certification.

At the same time, the second edition of ISO/IEC 17021 "Conformity assessment—Requirements for bodies providing audit and certification of management systems," was published in 2011, which transforms the

Downloaded by [Bulgarian Academy of Sciences], [Kiril Stoichev] at 21:27 26 January 2015

guidance offered in ISO 19011 (2011) into requirements for management system certification audits (requirements for third party certification).

After many years of evaluation of the management of both the organization's internal departments and companies performing audits by a third party on the basis of procedures developed themselves, a uniform and objective basis for a unified approach in preparation for implementing this action was set. That is great because, once again, it goes to show that the unification of approaches, tools and building activities, and evaluation and maintenance of management systems is the right way to establish confidence in their suitability to meet successfully the mission for which they were created. The last is in full force for the security management system of the organization.

But can we use the previous standards for the goals we have set for ourselves, namely, evaluation of security levels and ISMS?

There should not be any obstacles, but this is not yet the methodology for evaluation. Both standards provide guidance only for the teams and the certification bodies for the preparation and conduct of audits, but in terms of their nature, these documents "remain silent."

In support toward the efforts to create a methodology for security assessment of the critical infrastructures comes ISO/IEC 27002 (2005) "Information technology—Security techniques—Code of practice for information security management," which establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization (it comprises ISO/IEC 17799:2005 and ISO/IEC 17799:2005/Cor.1:2007). Generally, in terms of information security, International Organization for Standardization has done much to ensure the integrity and timely access to necessary information.

The very structure of the standard shows that it goes in the same direction with the creation of tools to enhance the overall security of the organizations, namely, the establishment of an ISMS. Briefly the main elements of this structure are:

- 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.

Downloaded by [Bulgarian Academy of Sciences], [Kiril Stoichev] at 21:27 26 January 2015

The existing structure of the above mentioned standard confirms the logic of the approach which I propose, namely, determination of the levels of security for an organization to be made through the integration of interdependent elements which have a direct and indirect impact on security management (in the case of the aforementioned standard it is information security management).

More importantly, "n" number of security categories are included in each of the aforementioned structural elements. The last virtually details every one of the previously mentioned structural elements as set out, the key objectives that must be attained to achieve information security through the implementation of appropriate structural element, and the criteria for assessing the level of success.
Each main security category contains:

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

Control descriptions are structured as follows:

- Control–Defines the specific control statement to satisfy the control objective;
- Implementation guidance–Provides more detailed information to support the implementation of the control and meeting the control objective. Some of this guidance may not be suitable in all cases and so other ways of implementing the control may be more appropriate;
- Other information–Provides further information that may need to be considered, for example, legal considerations and references to other standards.

This is one of my favorite approaches to development and use of a methodology to assess the levels of security of critical infrastructures and the ISMS. It is necessary for each of the identified levels of security to be clearly defined: Control objectives stating what is to be achieved and one or more controls that can be applied to achieve the respective control objective. For the development of this methodology, whole sections of ISO/IEC 27002 (2005) can be replicated to be transformed for the integrated management of security, not just for information security management. For example, Security Policy, Organizing Information Security, Human Resources Security, Physical and Environmental Security, Access Control, Business Continuity Management and Compliance can be fully used as elements of the considered methodology to assess the levels of security and the integrated security management system.

Downloaded by [Bulgarian Academy of Sciences], [Kiril Stoichev] at 21:27 26 January 2015

Of course, mathematical apparatus can be applied for the objective evaluation and many other additional elements to the methodology to enhance its practical utility and increase its credibility and the results of its application.

However, the methodology must maintain a balance between excessive complexity and the guarantee of objectivity and accuracy of the results of its application. That is, a widespread opinion is that the more complex a mechanism is, the more "modern" it is. However, in this case, this is not valid. Moreover, it should also take into account the fact that for the application of the methodology, many auditors have to be trained whose precision in performance of their duties is essential to the security of organizations and from there to the health and lives of their employees.

RESULTS

The result of the choice of method for creating levels of security and methodology for their evaluation will be developed and put into practice as a set of standardized documents, procedures, training plans, and generally the whole range of activities supporting the functioning of the management system, in this case, ISMS of critical infrastructures.

In turn, results from the application of these tools will enhance the security of the organizations. Someone will ask, what forms this process, what is its nature? The short answer is this—the system under consideration will enjoy all the benefits of integrated management and, most importantly, will create conditions to multiply the speed and adequacy of the response of the security forces to counter threats of any kind for the life and health of employees and the business of the organization.

CONCLUSION

Issues related to security are intertwined in all areas of the life of an organization. Many of them are considered and documented organizational and provided within the respective area/subsystem of the management system of the organization. For example, information security management is detailed and reliably described in the international standards. This is natural, considering the importance of this type of security and the fact that information technology lies at the core of almost all organizations. (It is hard to imagine life in our company without computers and the Internet.) Among other things, these standards can become the starting point for the development of the documentary basis for ISMS, that is, we will not "go from scratch" and will continue the development of methodologies, procedures, and best practices lying behind these standards in the direction of creating conditions for the development of an integrated security for the organization.

Downloaded by [Bulgarian Academy of Sciences], [Kiril Stoichev] at 21:27 26 January 2015

Downloaded by [Bulgarian Academy of Sciences], [Kiril Stoichev] at 21:27 26 January 2015

In the meantime, however, it is necessary to go a long way to reach the ultimate goal of improving security of the organizations by developing integrated management systems for business security. Numerous issues need to be addressed without the decision of which we will not be able to say that we have achieved this goal. The least we can do is to identify security issues in all control subsystems, to describe them in neat procedures, and follow them consistently. This is in the power of the security bodies in every single organization. As for the formation of security levels and the development into this activity in ISMS, this is an ongoing process that needs to be done by all professionals and those concerned with security authorities and organizations (primarily governmental such).

As was mentioned at the beginning of this article, the security that can be achieved through technical means is limited and should be supported by appropriate management and procedures. Terrorists not only develop new technologies and means of terrorist attacks, but also organizational practices for getting the best results from the use of these funds. Therefore, we must be "one step ahead" of them both in technical and organizational terms to ensure an adequate response to counter their efforts.

NOTES

1. For the purpose of avoiding repetition, the term "organization" ("organizations") will be used instead of "critical infrastructure."

2. In 2012, the International Organization for Standardization accepted the structure of ISO 9000 as standard in creating standardization documents regulating the requirements for the subsystems management.

REFERENCES

ISO 19011. (2011). *Guidelines for auditing management systems*. Retrieved from http://www.en-standard.eu/iso-19011-guidelines-for-auditing-management-systems/?gclid=Cj0KEQiAwPCjBRDZp9LWno3p7rEBEiQAGj3KJgrSg7SIkzLFjEz0HqvxRRIXnwaKxDuTWBoyZ_SmVK4aAnQ38P8HAQ

ISO 9001: 2008. (2008). *Quality management systems. Requirements*. Retrieved from http://www.iso.org/iso/iso_9000

ISO/IEC 17021. (2011). *Conformity assessment—Requirements for bodies providing audit and certification of management systems*. Retrieved from http://www.iso.org/iso/catalogue_detail?csnumber=56676

ISO/IEC 27002. (2005). *Information technology—Security techniques—Code of practice for information security management*. Retrieved from http://www.iso.org/iso/catalogue_detail?csnumber=50297

Stoichev, K. (2014, July). Security levels of critical infrastructure. *Journal of Applied Security Research*, *9*(3), 328–337. doi:10.1080/19361610.2014.913233