Comparative analysis of the us ISO and NIST standards on assessing the risk of information leakage in communication systems

Sergey Salnyk [*] [A]; Pavlo Sydorkin [A]; Sergey Nesterenko [A]; Alexander Zaytcev [A]; Mykola Konotopetc [A]

[A] Institute of Special Communications and Information Protection National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", 4, Verkhneklyuchevaya str., Kyiv, Ukraine

Received: December 02, 2020 | Revised: December 6, 2020 | Accepted: December 31, 2020

DOI: 10.33445/sds.2020.10.6.4

Abstract

The reliability of any system was always defined by its level of stability and by availability to have in responsible security persons or specialists' disposal necessary preventive measures, which are adequate to the threats risks and which are not yielded to easy elimination or demolishing. There was always in the world competition for the information ownership and according to it there was always the rivalry for ability to preserve effectively this ownership from the "outsiders" and much more from competitors.

The protective systems are as effective as they include completely all the possible and theoretically probable processes, which are going on within the information system (IS) or can be caused by outside influence, or when they appeared accidentally. Therefore, risk controlling management model for the IS must reflects all the variety of events and also the processes of resources distribution and using. Making the analyses of available for today published works on this occasion it's possible to come to a conclusion that all of them (standards) contain in themselves a great deal of engaging of methods and tools, which are sufficient for to discharge the setting tasks. But in the information field the life is also going on and appearing of the new risks is inevitable as the necessity to search for the new standard means of counteraction to them. The theme of this article is the comparing analyses of two main standards, which are appealed to create secure conditions in information space for the owners of information and for their working without hindrances within their network, and for their outside partners and consumers.

Key words: information security management, threats for the information security, risk control system, identification of the threats, risks appraisals, information system susceptibility.

Introduction

Given the importance of this issue against the background of the incessant struggle for ownership of information assets, this article is extremely relevant and will undoubtedly remain significant as long as there is competition in the global information space.

Communication systems are created and operate in close, constant and smooth cooperation with third-party consumers / partners, with such format a priori requiring a rapid-fire response to possible threats. Working conditions are complicated by the fact that a productive activity presupposes full disclosure and swift decision-making, on the one hand, whereas the issues of information security (IS) require time and proper processing in order to minimize the risk of information leakage, on the other hand.

[*] **Corresponding author:** Candidate of Technical Sciences, Deputy head of the special department, e-mail: s.sergey@i.ua, ORCID: 0000-0003-4463-5705

The variety of methods for assessing the risk of information leakage in communication systems prompts us to investigate the pros and cons of some of them carefully. Currently, the US ISO and NIST (National Institute of Standards and Technology) are the most frequently used standards in the world's leading countries. Both standards contribute to the effective risk management with regard to the threats to information systems and help making the information security services more transparent. Therefore, the purpose of this article is to reasonably guide prospective users regarding the choice of the most useful method, thus granting the desired result. The specialists responsible for IS organization are guided by standards developed by reputable institutions.

Formalization of this article by bringing it into compliance with one or several standards (Law of Ukraine) enhances its efficiency, makes the results predictable and corresponds to the legal requirements (Cabinet of Ministry), subsequently streamlining these processes.

With the high-level number of probable threats or risks of such threats, the required number of standards and specifications (as evidenced in practice) should be sufficient offering its consumers a wide range of methods and means of action aimed at achieving maximal results in a short time.

The ISO/IES 27005;2008 is one of such standards being part of the ISO/IEC 27000 series of information security management standards (Bobov P.K.). As a rule, new revisions of this document are issued annually taking into account new challenges for information systems as well as new means of countering them.

As it turns out, the relationship between consumers of the Internet products has somewhat changed recently. Instead of the atmosphere of trust discernible during the creation of network protocols that are relevant to this day, and in connection with or as a result of investment development, the priorities have shifted towards the development of new features and to the detriment of the security level of such innovations due to the emergence of the more "advanced" functionality. However, the threats to information security are constantly and rapidly increasing. Their agents include viruses, worms, various "Trojan horses", unauthorized attempts to imitate the connection thus violating the integrity of the security system, and identity theft, to make it worse. Hence, building a risk management system as an essential part of a cyberspace security system is an ongoing process of predicting new approaches to securing information systems, networks, applications and assets (Dorofeev D.I.). At the same time, the very purpose and activity patterns in the world network, their interconnection with all other operators as well as the need to use the advantages being offered to the users make each of the operators vulnerable to negative influence from other operators, competitors, rivals, and opponents. The complexity of building a security system lies in not hindering the rapid promotion of business, and the availability of services rendered (Gulyakin V.V., 2009). In this business world with its need for constant information exchange, internal and external spaces do not have a clear demarcation and the perimeter of such organization becomes merely conditional. Therefore, the use of a multi-level activity organization with appropriate security systems will significantly complicate the infiltration and the destruction of information systems in general (Andrew Prozorov, 2013).

Material and methods

The purpose of this article is to compare the ISO and NIST standards with regard to the secutity system's ability not only to timely counteract, but also to adjust its work and change its priorities.

The object considered is the process of organizing a risk management system to prevent unauthorized interference with the information system/network and the procedure for taking the necessary preventive measures.

The subject analized is a comparison of the advantages and disadvantages of the two main standards in preventing threats to information system vulnerabilities and the actual ability of the users to prevent such threats.

Results and discussion

For the purposes of this article, it is appropriate to describe the main stages of the risk management process according to both standards, starting with the NIST SP 800-30.

This document of the US National Institute of Standards and Technology is called "Risk Management Guide for Information Technology Systems" with its content fully corresponding to its name and having the following schematic form:

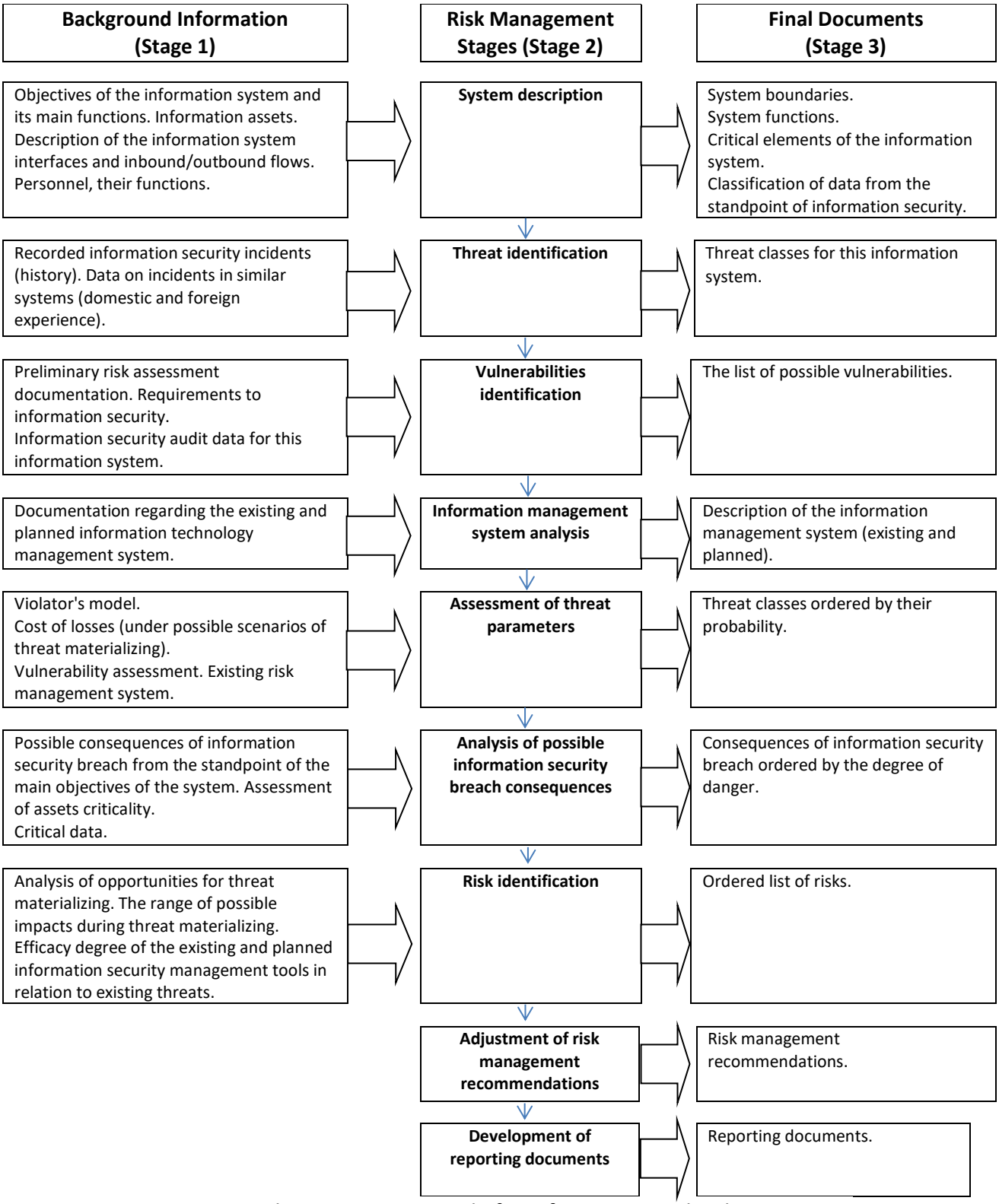

Figure 1 – Risk Management Guide for Information Technology Systems

The NIST standard algorithm has three stages in each direction. For a more visual representation of its operating principles, it is advisable to depict the whole process in sections, which, like a protective wall, will keep all the necessary secrets of the given organization and will call for greater focus on the most applicable direction.

Section 1 lists information system objectives, its main functions and available information assets (ISO/IEC 15288:2002). The description of information system interfaces and inbound/outbound information flows, personnel composition and their functions. The second stage of Section 1 includes risk management stages. In particular, it serves as the "system description" for the above section. The third stage contains the results of the measures taken during the second stage, therefore it is called "Outbound Documents". Regarding the description of the system, it includes the system boundaries, functions, information system critical elements, and classification of data from the standpoint of IS (information security).

Section 2 focuses on information security incidents as well as information data presented as analogies taking into account domestic and foreign experience (IEEE/EIA Std. 12207.1: 1997). Risk management stages in this section provide for threat identification, whereas the source document will be the definition of threat classes for the given information system.

Section 3 includes the analysis of previous experience, documentation of risk assessment (Andon, F.I., 2007), as well as IS requirements and IS audit data on a particular information system. Management is provided by identifying the areas that are easily affected. Outbound documents here include the list of potentially vulnerable areas.

Section 4 deals with source information and documentation concerning the existing and planned information technology management systems. The second stage analyzes these information management systems (Dustin, D., 2003). The third stage summarizes both information management systems as a conclusion.

Section 5 lists the violator's model, the cost of losses under different threat materializing scenarios, vulnerability assessments and the existing risk management system (Raichev, I. E., 2006). At the second stage, this situation is managed through assessing the threat parameters and results in a ranking by the probability of threat classes at the end of this process (the third stage).

Section 6 depicts the possible consequences of IS violations from the standpoint of the main objectives of the system as well as an assessment of the criticality of the available assets along with critical data. The second stage focuses on the possible consequences of information security breach while searching for ways to resolve the issue. It is summed up by ranking according to the degree of danger of such information security breach consequences.

Finally, Section 7 of the document provides the analysis of the possible threat materializing according to the NIST SP 800-30 standard. The range of possible impacts during threat materializing as well as efficacy degree of the existing and planned IS management tools in relation to such threats. The response includes: a) risk identification; b) development of risk management recommendations; c) development of reporting documents. The third stage of Section 7 provides for a) the list of risks by rank; b) risk management recommendations; c) reporting documents (Tkachenko V.).

When describing in accordance with the NIST SP 800-30 standard, it is necessary to provide information about the information system hardware, its configuration and the software used. Subsequently, one needs to provide information about system interfaces, that is, about external and internal communications from the standpoint of information technology, as well as data and information types (especially critical data types and information processes). Finally, one needs to provide full information about the personnel, their job functions, information system functional requirements as well as its mission (main objectives). It is also important to report on the types of consumer categories of the system and the structure of the operating personnel.

In short, this is how the security system works

according to the NIST SP 800-30 standard adopted in the United States in 2002.

It is also necessary to familiarize oneself with the working procedure and the distinctive features of the ISO/IES 27005;2008 standard in order to analyze the methods for assessing information leakage risks and compare the approaches of both standards.

The materials of the standard are presented as a developed model with the description of an object as a set of elements interconnected by certain relationships as its basis. The analysis of the risk levels as well as vulnerability of the components of the system or information system as a whole is done both in the form of several separate stages of risk threats, and in their totality. The first of these two fails to assess the efficiency of each individual stage while the second makes it possible to sufficiently detail the risk threats and assess the measures according to some criteria, but does not take into account external influences and cannot be used to develop models of future threats. The third model divided by graphs allows for assessment of the complexity of information system security breaches based on current data and analysis of the necessary conditions for effective protection in the future.

Risk handling here is based on the following: defining the context, which, together with risk communication, plays a pivotal role in defining the "risk assessment" block of questions consisting of risk analysis, which, in turn, relies upon risk identification and preliminary assessment. The final risk assessment is then reflected in their comparison. Risks are subsequently managed after completing the above works. However, the management process itself must be adjusted in order to improve its effectiveness. Therefore, the data on management measures that have already been adjusted are transferred to the beginning of the processing workflow aiming to notify, monitor and possibly revise potential risks, as well as to influence the definition of the context. That is, preventive risk handling consequently affects the approach to the defining information thus making such security actions more efficient.

Another aspect of risk handling is the organization of protection by protecting structural units, network systems and the like. In this case, security specialists do not simply identify a real or potential risk, but use technologies to protect the external "borders" of a given company, or its perimeter. These technologies prevent unauthorized and unverified persons from accessing from the outside (with unverified persons from within being an exception) as well as establish logical and physical boundaries between the particular areas to be protected and the areas that are open to public use.

This protection technology can be used both for the network as a whole and for a particular technical means. One of the main ways to ensure perimeter protection is content filtering or content control programming restricting the network availability of certain types of data as well as narrowing or prohibiting their distribution on the network (the work is performed according to the [ISO/IEC 10828-3] protocol and, accordingly, does not contradict the requirements ISO/IES 27005;2008.

Throughout any risk identification process, one primarily identifies the set of components that need to be protected in each particular case. That is, the threat is not dangerous in itself, but it is dangerous in how and what it can affect. Here are some examples of potential threats, categorized. This classification will facilitate risk analysis and help save time and money. The first of them should be attributed to security breach issues manifested in the interruption of service, when the user cannot get the necessary service either in the local or in the worldwide network. The second category includes threats of unauthorized access to assets. Unauthorized access may aim at stealing information property or knowingly misuse the infrastructure. The scope of the negative impact in this category of threats depends on their scale and can be rather significant. The third category of any system compromise is the capture of information system components. As a result of this penetration, it is possible to establish control over particular devices with such captured and controlled means subsequently used to further compromise and spread their control over the information system subject to such aggression.

Risk management practices implemented according to the ISO/IES 27005;2008 allow not only to identify existing and potential risks of

threats, but to adjust their analytical assessments and, accordingly, on-line preventive measures. Therefore, the flexibility of such practices is beneficial in response to constant change and innovation on the part of violators. Adjusting the organization of information security throughout its application at the same time allows for calculating the potential risks for our own network.

The main challenge in developing a risk management system for both standards (ISO/IES 27005;2008 and NIST SP 80-30) is to assess the threats in order to optimize their application. Assessment offers the possibility to reasonably establish the scope and direction of such procedures and programs. This is associated with the cost of using information system and its increase due to the need to integrate a security system. Correctly and prospectively identified threats will reduce the cost of the security system. For example, prioritization will make it possible to ignore some potential threats as their use by the violator will not be effective or financially justified leading to the detection of such violator instead.

Summing up this section, it can be noted that despite the similarity of the objectives and uniformity of the operation methods, the ISO/IES 27005;2008 and NIST SP 80-30 are still different (otherwise they would be combined into one document). The difference between the approaches to handling both existing and potential risks can be seen even in graphical thinking: in the NIST standard, the structure has a rectangular shape with stages inside like floors in a building. Each section is being processed separately having their own assigned tasks. Thus, information from one section does not directly affect the consideration of information in another section and, possibly, does not distort the employee's impression preventing them from "turning a blind eye on" a specific issue.

At the same time, the ISO/IES structure is centric, with everything being concentrated on risk assessments and each direction directly affecting the others and adjusting their content. In other words, the NIST has everything independent, the ISO/IES, on the contrary, has everything interconnected.

In order to come to a final value judgement on each of these two standards, it is necessary to conduct an in-depth study of their processes. Therefore, we will thoroughly examine the risk management process proper for the NIST SP 800-30 standard.

In the course of work, one should consider IS formal requirements applicable to a particular information system. This refers to legislation, departmental standards, etc., as well as the subsystem architecture and local network topology. Typically, IS software and hardware together with all data flows are monitored with information management system taken into account, that is, the existing job descriptions, information system planning as well as out-of-schedule process management, namely backup, emergency response procedures, IS instructions, IS compliance monitoring, and more. Physical security of the personnel is also carefully organized by managing and controlling the external environment, that is, climatic parameters, the method of power supply, protection from accidents and exposure to aggressive substances.

According to the requirements of this standard, it is recommended to conduct surveys and interviews with the management and service personnel as well as to analyze the documents of the given company/institution, and to use process-specialized tools in the course of such work, namely scanners for drawing up a diagram of an information system, and programs for a structured description of information systems allowing to create the required reporting forms.

When analyzing all the outlined processes for the information system risk management, we can confidently conclude that both the virtual world (electronic media, software products and information transport networks) and the real world (personnel, technical organization of work together with emergency solutions and the accumulated "paper" component such as instructions, functional responsibilities, legal framework relating to this type of activity) are carefully considered.

In particular, Section 2 according to the NIST SP 800-30 standard, which focuses on incidents that have occurred in the past taking into account the comprehensive experience of these phenomena,

gradually transforms into the processing of this information in the second stage by identifying the threats and consequently results in specific measures taken in Section 5. In practice, for this purpose one should develop the violator's model describing the possible intruder, their motives and capabilities, and the probable scenario of the threat. As a result, we have a list of current threats to the information system.

The output of identifying the information system vulnerabilities is their exhaustive list. Several sources are examined during the compilation of such list for an existing system, namely network vulnerability scanners and relevant directories from other organizations (third party experience). Rating assessment of vulnerability levels involves the existing procedures and methods ensuring information security such as internal audit data and analysis findings regarding the incidents that have occurred.

In the future, one can select the required scale to assess the risk parameters. A complex scale with several gradations would be better for a clearer definition. It is also reasonable to assign such task to experts. The severity of IS violation as well as the likelihood of threat materializing are established based on the determination of the risk parameters on the scale. Risk levels are subsequently determined by combining the probability of their occurrence with the severity of their consequences. Moreover, risk levels depend on the level of threats as well as vulnerabilities and the cost of possible consequences. Risks can also be ranked by the degree of danger.

The next step in risk management is the development of the relevant management recommendations. It is logical and vital to reduce risks to an acceptable level. Recommendations on ensuring efficiency should be comprehensive and take into account the possible application of measures of different levels.

The risk management process itself is continuous and includes four stages. The first one on the list is risk assessment interpreted as identifying and prioritizing the threats. The second is decision support, that is, the search and evaluation of control decisions. The third is control implementation presupposing the implementation of risk-reducing control decisions. The fourth is evaluating the program effectiveness, analyzing the efficiency of the risk management process and ensuring such control elements provide the required level of security.

Each of the stages has several steps. During the first stage (risk assessment), three steps must be taken, such as planning, collecting risk data and prioritizing risks. The second stage (decision support) also requires three steps, namely defining functional requirements to mitigate risks, choosing possible control decisions and checking the suggested control elements for their compliance with functional requirements. The third stage (control implementation) requires two steps, namely the involvement of personnel, processes and technologies in addressing the issue of risk neutralization, and streamlining the decisions on risk neutralization within the enterprise/institution/company. In a similar manner to the third, the final fourth stage (assessing the effectiveness of the risk management program) includes two steps necessary to accomplish its tasks, such as developing a system of risk indicators, their levels and changes; evaluating the effectiveness of the risk management program and identifying the opportunities for its improvement.

The main purpose of risk assessment is to identify and streamline them. Planning is extremely important as it pinpoints the scope/area of such assessment and helps gain management support. Each risk requires determining the likelihood of its occurrence as well as the scope of associated losses. One way to collect the necessary information is to interview employees. In this way, assets, threats, vulnerabilities and control elements are identified. Eventually, the entire list of risks is arranged on a scale with gradation into three degrees of danger: high risk (indicated in red), medium risk (yellow) and insignificant risk (green).

Further on, priorities are set in order to neutralize risks. However, after prioritizing the risks, analytical work is still in progress with quantitative methods being used to identify the most significant of them.

The result of the work is reflected in the reporting documents as a whole or in stages.

Often, threat assessment is displayed as a list of areas (infrastructure components) and specific IS tasks assigned in a particular area. For example, a priority for the infrastructure perimeter area is the security protection at network boundaries where the internal network connects to the outside world. It is the first area to be possibly affected by violators. For the authentication area, there are strict authentication procedures for its users, administrators and remote users preventing third-party access to the network through local and remote attacks. Management, supervision and proper logging are critical to maintaining and analyzing IT assets in the area of management and supervision. They are even more important for post-attack incident analysis. When it comes to the workstations area (if any), securing each of them is a major factor in securing any environment, especially if remote access is permitted. Security measures for such stations should also prevent the possible spread of attacks. When distributing and using add-ons, for example in the manufacturing sector, security protection along with the availability of these add-ons and servers are crucial for this area. Continuous servicing is essential for the elimination of errors. Another area in infrastructure is add-on design. This measure is capable of comprehensively addressing the security issues of authentication, authorization and data verification. Successful design will be an obstacle for violators preventing them from gaining access to critical information.

On the whole, the integrity and confidentiality of data is one of the biggest concerns for any institution, enterprise or organization with information priorities. Their loss or theft can shatter not only profitability, but also their image in general.

A similar, well-defined approach is clearly demonstrated by the authors of a later document of a respectable American institution officially called the NIST SP 800-53 (rev 4 04-2013) "Security and Privacy Controls for Federal Information Systems and Organizations". It clearly stipulates the purpose, objectives and target audience. In addition, the purpose of the document is given in its parts and annexes. There is also mapping with other information security standards such as the ISO 27001 (2005) and ISO 15408.

The structure of the document is extremely simple (consisting of only three chapters: "Introduction", "Basic Principles" and "Process").

Effective operation under this standard is based on the model of continuous improvement of information security. The list of tools includes the following measure groups: access control, awareness and training, audit and accountability, and many others. In total, the document contains 18 measure groups necessary for ensuring information security. Such number of directions and their clear focus on a specific problem allows us to cover all the tasks, and the order of priority ("first of all", "next step", "at the end") makes the implementation of these tasks even more efficient.

We suggest a newer document stipulating the procedure for risk management in information systems as it is not a fundamentally new instrument but rather an improved revision of the previously adopted NIST SP 800-30 standard, which takes into account all the successful measures taken over the years when applying the previous regulations and requirements (see Table 1).

Conclusions

Thus, based on the results of the analysis, the users will choose a more convenient and affordable risk management standard. But objectively, a reliable system is the simplest primarily because it is predictably applicable when the errors are minimized and the human factor does not have such a big impact. Therefore, the decision is up to the consumers. The consumers will decide which standard will best meet their needs.

Table 1 – Comparative Table of Advantages/Disadvantages of the Two Standards: NIST SP 800-30 and ISO/IES 27005;2008

NIST SP 800-30		ISO/IES 27005;2008	
Description of the Action Format	Assessment of Effectiveness	Description of the Action Format	Assessment of Effectiveness
The organization of risk management is based on 7 sections/directions and consists of three stages: collecting information in this area, analyzing information using specific techniques, and the output information.		The organization of risk management is an interconnected system with a stage-by-stage approach and close relationships between its elements.	
Section 1. The work within each of the stages is carried out independently based on the fundamental decisions with regard to the assigned tasks.	Conclusion: This approach is reminiscent of the work of an independent expert who knows how to properly operate and does not pay attention to various side effects. This method is the most effective in relation to Section 1 for classifying the system and identifying its fundamental shortcomings.	The description of the system and its components is almost identical to the description according to the standard of the American Institute. However, the work is not divided into stages being an ongoing process.	Conclusion: This approach is closer to the actual functioning of the information system where its operation is not divided into sections and stages but is an ongoing process.
Section 2 deals with incidents or threats that have happened in the past as well as their identification and gradation of incidents/threats by class.	Conclusion: when considering this material, external experience is also taken into account, that is, not only the "rule", but also practice.	Assessment of risks and their threats is given in stages as well as in the aggregate, it is quite detailed without taking into account external influences.	Conclusion: a two-pronged approach allows for better consideration of the threats and definition of the specifics, but it makes it barely possible to simulate future threats.
Section 3 focuses on vulnerabilities of this system and the results of IS system audit.	Conclusion: vulnerability diagnostics allows focusing on the vulnerable areas without diffusing the efforts throughout the network.	The analysis of vulnerabilities ("weaknesses") is given in a similar way to risk analysis, that is, in sufficient detail, but without taking into account external information.	Conclusion: it helps create a coherent picture of vulnerabilities but is not useful for any forecasting.
Section 4 analyzes the information management system at a given time and for a pre-planned period.	Conclusion: the comparison of the involved and the planned management systems helps foresee the possible issues and adjust the plans in advance.	The analysis of the information management system is given together with the analysis of the IS system.	Conclusion: greater brevity is convenient since IS is inseparable from the information system, and in general, its existence is necessary for the latter, therefore it is

NIST SP 800-30		ISO/IES 27005;2008	
			better to use them simultaneously.
Section 5 simulates the possible threats/risks of threats taking into account the assessment of vulnerabilities and the state of IS (Section 3).	Conclusion: Simulating negative processes is a creative work (theatrical, pictorial), while adjusting the obtained images is identical to the work of a director, editor, critic.	The organization of risk management is based on the definition and adjustment of the defining information, that is, the information obtained as a result of the analysis and preliminary risk assessments.	Conclusion: in contrast to the NIST standard, the "adjustment" of the focus areas as well as the review of the estimates and conclusions is an ongoing process allowing to quickly react to innovations and rectify errors.
Section 6 analyzes the consequences of materialized threats and their impact on the achievement of the main objectives for a particular information system. At the end of this process, one obtains the classification of threats according to the degree of their negative impact on the intended purpose of the system.	Conclusion: as in the situation with identifying the system "vulnerabilities", identifying the most serious threats improves IS efficiency and reduces its cost.	The classification of existing and potential threats is carried out based on studying the system, evaluating the measures taken and comparing these threats in terms of their danger.	Conclusion: system protection by classifying its threats is aimed at protecting its structure and individual parts regardless of the objectives set. This makes the IS system more versatile but less specific.
Section 7 is more of a summary and suggests recommendations for the best organization of risk management.	Conclusion: the advantage is that recommendations are given based on the comprehensive review and analysis of efficiency of the information security system. Disadvantage: in the event the system is tested over a protracted period, such recommendations may be delayed.	Recommendations are not formalized in a special document; the defining information about the state of the system as well as the risks of threats is revised together with the results of the work performed.	Conclusion: The result is comprehensive, with the changes in the directions of work within the scope of information security being made both throughout its implementation and based on the results. Such approach facilitates IS efficiency.
Both standards have much in common and are rather similar as they deal with one and the same problem. While the work according to the NIST SP 800-30 standard allows one to predict the future risks and ensure advance preparation, the work according to the ISO/IES 27005;2008 standard affords an opportunity to respond to new challenges almost on-line by changing procedures and risk management methods if necessary.			

References

Andon, F.I., Koval, G.I., Korotoun, T.M., Lavrisheva, E.M., Souslov V.Y. (2007), "Osnovy injeneriy kachestva programnykx sistem", [Basises for the quality engineering of programming systems], Kyiv: *Akademperiodika*, 672 p.

Andrew Prozorov, independent expert and bloger "A new point of view FSTEK VS NYST 800-53. It's shame to my state", 2013

Bobov P.K. From the materials of the Consulting-expert action report of Bobov P.K., JSC "High-Quality Programmed Decisions" for theme: "Ensuring the informational systems security management"

Cabinet of Ministry of Ukraine order from 11.26.2014 № 1163-p.

Dorofeev D.I. From the materials of the Consulting-expert action report of Dorofeev D.I., JSC "High-Quality Programmed Decisions" for theme: "Ensuring the data technical defence in informational systems

Dustin, D., Reshka, D., Paul G. (2003), "Avtomatizovane testuvannya programnogo zabezpechennya. Vprovadjennya, upravlinnya ta ecspluatatciya", [Program maintenance auto testing. Establishing, controlling and using], translated from eng., Moscow: publishing house "Lory" – 567 p.

From the materials of the Consulting-expert action report of T.R. Yusoubaliev, JSC "High-Quality Programmed Decisions" for theme: "Establishing standard documents and requirements concerned to information defence"

Gulyakin V.V. (2009), "Rozrobka metodykiv ryzikiv informatciynoy bezpeki", [Informational systems risks methods work out], Moscow: RDSU

IEEE/EIA Std. 12207.1:1997. Software life cycle processes – Life cycle data

ISO/IEC 15288:2002. Systems engineering – System life cycle processes.

Law of Ukraine "About standardization" from 06.05.2014 # 1315-VII

Raichev, I. E., Charchenko O.G. (2006), "Contceptciya pobudovi sertefikatciynoy modeli yakosti programnikh system. Problemi programuvannya", [Concept of constructing the program systems certification quality model. Programming problems] №2-3, 275 – 281 p.

Reports thesis' collection from the Consulting-expert action "Arising of informational security in the scientific and innovation activities" Moscow: "Vector-K", 2016. 7 p.

State enterprise "Ukrainian scientific-researching and educational centre of the standardization, certification and quality problems" order from 08.04.2017 № 207 "Concerning the national standard documents accepting harmonized with European standard documents, amendments in national standard documents, national standard documents cancellation"

Tkach I.M. Conceptual principles of military and economic security of the state: monograph. Kyiv, 2018. 312 p.

Tkachenko V. director company "Active audit agency": "Modern approaches to the IT risks estimate (on support the branch informational security standards establishing GSTU SUIB 1.0/ISO/IEC 27001:2010 and GSTU SUIB 2.0/ISO/IEC 27002:2010", Kyiv, 2010.