Development of Awareness and Competences of Employees in the Processes of Information Security Management System

- guidelines for practical application –

Vitomir T. Miladinović

College of vocational Studies Belgrade Polytechnic, Belgrade, vitomir.miladinovic@gmail.com

A General Survay

https://doi.org/10.7251/JIT2002087M UDC: 004.6.056:[005.334:351.78

Abstract: Based on author's experiencie, in this we will analyze some issues of awareness and competence development of all employees in the organization in the processes of information security management system (ISMS), in accordance with the requirements of the International Standard SRPS ISO/IEC 27001 Information Technology — Security Techniques — Information Security Management Systems — Requirements.

Keywords: data, Secsty, information, awareness, competence.

Introduction

One of the most important characteristics of the modern age is the *collection, storage, preservation, transmission and use of large number of data and information* of all types and significance degrees for the owner of that data, i.e. the individual or legal person to whom the data relate. The significance of these data and information for their owner derives from the type and intensity of the consequences of their unauthorized and/or malicious use by, both entities to which access to this data and information is allowed, and those to which that is not allowed. In this regard, there is a legal, but also, above all, ethical obligation of the subjects (users of data and information) to whom, for any reason, the data of another party (individual or legal person) are available, to handle this data and information in such a way as *to preserve their confidentiality*, i.e. to treat them in such a way that they are not available to (unauthorized) third party without the prior consent of the owner of that data.

Along with the development of information technologies and their increasing availability, a trend of collecting and storing a huge amount of diverse data and information in almost all areas of life and work of modern man emerged. Besides, very often, to put it mildly, the need to collect certain data is debatable, but also problematic, i.e. the purpose of collecting certain data and information in relation to a particular subject or entity (individual or legal person) is often not clear and understandable. At the same time, there is a very pronounced trend of increasing threat to the confidentiality of collected data and information with the aim of their unauthorized and illegal use and misuse for the purpose of obtaining certain, tangible or intangible, benefits. As a result, *damages* (tangible and intangible) to the owner and user of the data can be large, *often immeasurable*. In particular, the impact of these procedures on the viability of the organization's operations, as well as its reputation, should be borne in mind.

One of the key factors influencing the degree of protection of data and information available to the organization, but also the factors of their endangerment is *a man* - a member of the organization (employee) in any position in it. By his *conscious* (inten-

tional) and/or *unconscious* (unintentional) actions, he creates conditions for achieving a certain degree of security of data and information, i.e. the degree of their endangerment by unwanted actions of certain subjects. The outcomes of the actions of employees at all levels in the organization depend, primarily, on:

- ***the degree of their awareness*** of the importance of the data and information available to the organization for:
  - the organization itself,
  - other organizations and individuals in the organization's environment;
- ***the competence of employees*** who, within their responsibilities and authorities, have access to certain data and information and use them in their activities.

Understanding the importance of awareness of all employees in the organization about the need to create and maintain a high level of data and information security, as well as their ***competencies*** in this area, are key factors for effective and efficient implementation of all activities in the organization aimed at achieving and maintaining adequate protection from unwanted effects of data and information that the organization disposes.

An organization that wants to achieve a high level of data and information security that it disposes and uses in its business must develop and maintain an effective and efficient data and information security management *system. Guidance on the establishment and maintenance of such a system is provided by the International Standard SRPS ISO/IEC 27001:2014 Information Technology - Security Techniques - Information Security Management Systems - Requirements*. [3] The requirements related to the establishment and maintenance of the process of developing and maintaining the awareness and competencies of employees in the organization on issues related to data and information security are defined in paragraphs 7.2 and 7.3 of this standard.

How is it possible to meet these requirements of the SRPS ISO/IEC 27001 standard and what can be the benefits of that, that is, what can be the consequences of inadequate level of awareness and competencies of employees regarding data and information security?

One of the possible answers to these questions will be given later in this paper by interpreting the content of the requirements, ways of their application in practice and possible effects, based on the author's experience gained through practical application of International Standards for management systems [1], [2], [3], [4] and others in production and service organizations of the Republic of Serbia and the Republic of Srpska, as well as teaching work in higher education.

INTERPRETATION OF STANDARD REQUIREMENTS SRPS ISO/IEC 27001

Terms and definitions

In this paper, we have used the terms defined in the International Standard *SRPS ISO/IEC 27000:2018 Information Technology - Security Techniques - Information Security Management Systems - Overview and Vocabulary* [2], as well as *SRPS ISO/IEC Guideline 73:2002 Risk Management - Vocabulary - Guidelines for Use in Standards* [4], and *SRPS ISO 9000:2015 Quality Management Systems - Fundamentals and Vocabulary* [1].

Competences of employees

The requirements of the SRPS ISO/IEC 27001 standard regarding the ***competences*** of employees in the areas of data and information security are defined in paragraf 7.2, and regarding ***awareness*** in paragraf 7.3 of the standard.

The term *competence*, according to the definition given in the International Standard SRPS ISO 9000:2015 Quality Management Systems - Basics and Vocabulary [1] implies *"ability to apply knowledge and skills to achieve intended results".* In other words, this term implies *a set of characteristics of the employee from which his ability and convenience to be assigned responsibilities and authorities to perform certain tasks are derived*. These are:

- knowledge acquired through formal education (education),
- knowledge acquired by acquiring knowledge other forms (courses, trainings...),
- skills necessary to perform certain tasks (e.g. driving a motor vehicle, handling certain types of tools and machines...),
- experience gained by performing the same and/or similar tasks,
- ability to follow, understand and accept

changes and innovations in the field they deal with and in relation to it,
- psychophysical abilities in accordance with the requirements of the workplace,
- other, in accordance with the requirements of a particular job.

From the aspect of data and information security, the necessary competencies of employees can be divided into two groups:
- competencies that must be possessed by employees who are professionally engaged in data and information security, and
- competencies that must be possessed by all other employees in the field of data and information security, depending on their status in the organization and the assigned powers and responsibilities.

What does the standard [3] require of the organization and what is required for the requirements to be met?

1. The organization must *determine the types and degree of necessary competencies* of all persons performing tasks that, within its activities, are managed by the organization, and which affect the security of data and information.

Satisfaction of this requirement is the basis for satisfying all other requirements related to the competence of employees, but also for satisfying some other requirements of the standards related to information security. Why?

The first question that arises when considering this request is: To which employees does this request apply? Here, the organization can make a mistake if this requirement is understood as referring ***only*** to those employees *who have defined* ***direct*** *responsibilities and authorities for the implementation of certain tasks related to the functioning of the data and information security management system*. The right answer to this question is that ***all employees****, in accordance with their powers and responsibilities, in some way affect or can affect the security of data and information*. In this case, the term ***all employees*** means *permanent or temporary employees in the organization* (members of the organization) and members of other organizations who, on any basis, perform tasks for which the organization is responsible.

From this follows a conclusion that the organization must define the competencies of all its employees necessary for proper action regarding data and information security, in accordance with their status in the organization. In practice, this fact is often overlooked, which results in ***"holes"*** in the information security management system.

By defining and providing appropriate competencies of all employees, the organization creates the necessary preconditions for proper and timely actions of employees in relation to data and information security. This is especially important in situations where there is a certain level of risk in terms of data and information security *(information security risk)* and when it is necessary the employees effectively respond in the event of certain *events or incidents related to information security* that affect or may affect *information security*.

To meet this requirement of the standard [3], it is necessary for the organization to identify *all information security risks*, i.e. the possibility of occurrence of *events or incidents related to information security* that affect or may affect *the security of information*, as well as their possible consequences and the intensity of those consequences. This includes a detailed analysis of all processes and activities in the organization from the aspect of endangering the security of data and information during their implementation. One of the results of that analysis must be the definition of the necessary competencies of employees related to the considered problem.

Deviation from the satisfaction of this requirement of the standard [3] will not lay a solid foundation for the development and operation of data and information security management systems. If the competencies of employees related to data and information security are not defined in accordance with the real *risks of information security* and other influencing factors, adverse events can be expected with high probability as a result of insufficient or inappropriate competencies of employees, with all the consequences can be produced.

The competencies of employees, according to the considered requirement of the standard [3], must be ***the result of appropriate education, training or experience***.

The manner of satisfying this requirement arises from the type of activity of the organization and the qualification structure of the employees in the organization. Accordingly, the organization must define:

- jobs that require a certain type and level of education,
- jobs for which adequate training is required and sufficient, and
- jobs for which, in addition to education and/or training, appropriate experience is required.

The manner and scope of meeting this requirement is directly related to the satisfaction of the previous: Depending on the status of the employee in the organization, primarily in terms of their powers and responsibilities arising from their impact on data and information security, the organization should, in determining the necessary competencies ***at the same time*** *determine* ***the manner and forms of acquiring*** *these competencies*. The next step is for the organization to ensure *that the competencies of the employees are acquired in an appropriate (determined) way.* This means that organizations *will entrust the performance of key professional tasks related to information security* ***only*** *to persons who possess competencies acquired in a certain type and level of education*. Possession of appropriate skills and relevant experience will also be mandatory elements of the competence of these employees. For other employees, in accordance with their powers and responsibilities, the organization will require competencies acquired in another, appropriate, way that ensures sufficiently reliable and quality execution of certain activities related to data and information security.

The main consequence of not meeting this requirement is the following: Key professional tasks in the field of data and information security ***are not performed by competent professionals*** and, therefore, the achievement of full effectiveness, efficiency and reliability of data and information security management systems is questioned. Such personnel are a weakness of the organization and, therefore, *the risk of information security* is increased, with all the consequences that arise from it.

2. If the employees do not possess the appropriate competencies or those competencies have not been acquired in an appropriate manner, the organization must *take appropriate measures for the acquisition of competencies*. It can be, e.g. employment of competent persons, organization and implementation of appropriate forms of acquiring the necessary competencies (education, training, trainings, etc.). In doing so, the organization must *evaluate the effectiveness and efficiency* of these measures and, based on the results of that evaluation, define, plan and take appropriate measures in order to achieve the necessary competencies of employees.

To meet this requirement, it is necessary to establish *a process of continuous monitoring, measurement and improvement of competencies of employees in the field of data and information security*. This stems from the fact that procedures and resources related to data and information management are constantly changing, along with the constant changes in the manner and intensity of endangering the security of data and information. The result of all this must be the appropriate *ability of the organization* to respond effectively to all forms of threats to data security and information at its disposal. This ability of the organization primarily depends on *the competence* of its employees to implement all activities related to data and information security.

The process of monitoring and measuring employee competencies must be based on the development and application of appropriate ***indicators*** of the degree of satisfaction of requirements related to employee competencies (policy implementation, achievement of goals, etc.), as well as ***criteria*** for drawing conclusions in this regard. These indicators and criteria must be harmonized with the real situation, needs and capabilities of the organization, in order to enable obtaining the results applicable in the processes of improving the data and information security management system.

3. If it does not meet this requirement of the standard, the organization will not have insight into the actual competencies of its employees, and the existing competencies will be far below the required ones. Therefore, the level of data and information security will be insufficient, with real possibilities of endangerment and harmful consequences that may result from it.

The organization must keep evidence of the competencies of its employees. These are appropriate documents that confirm and prove that a certain person is competent to perform certain tasks on the basis of knowledge and skills acquired in an appropriate manner. This requirement is realised as part of the implementation of *the human resources management process* and no special explanations are required.

It is noticeable that in order to meet the requirements related to the competence of employees, it is necessary to establish and implement the process of providing the necessary competencies of employees for the proper and timely implementation of all activities in the field of data and information security. This process should be part (subprocess) of the process of human resources management of the organization, i.e., the process of ensuring the competencies of employees, with specifics arising from the importance and specificity of the process of data and information security management. This process is shown in Figure 1.

4. The process of providing the necessary competencies of employees in terms of data and information security is based on the need to meet the needs of the organization in this area as a result of the situation and changes in the environment, primarily in terms of types and degrees of data and information. Data on the state and changes in the environment and the needs of the organization are the basic input elements of this process.

Based on its needs and the situation in the environment, the organization determines the necessary competencies of employees in relation to data and information security. The next step is to provide the necessary competencies. By monitoring and measuring the existing competencies, the organization determines the needs and undertakes the necessary activities in order to improve the competencies of its employees. This process is continuous, given that changes in the environment (internal and external) are continuous, which directly affects the changes in the needs of the organization in the field of data and information security that it has and uses them in its business.

It is noticeable that the structure of this process follows the Deming PDCA cycle.

Establishing and implementation of this process requires *the engagement of appropriate resources* - human and material, which depends on the structure of the organization, its activities, types and characteristics of data and information at its disposal, dangers and risks to data and information security and other factors. However, one should keep in mind the *potential benefits* arising from the results of this process, which, except in material terms, can be very important for maintaining *stakeholders confidence* in the organization's capabilities, as well as its image and overall position in the environment.

Awareness

A very important factor for the effective and efficient functioning of the management system and its subsystems is *the awareness of employees about the facts and phenomena that affect or may affect the achievement of expected results in a particular area, as well as their participation and contribution*. The requirement to develop and maintain the awareness of employees in certain areas is a mandatory prerequisite of all standards for management systems related to that area.

In the field of data and information security, the issue of developing and maintaining employee awareness requires a systematic approach, given the importance of data and information for the functioning of the organization. International Standard *SRPS ISO/IEC 27001*, clause 7.3, defines the requirements that an organization must meet in terms of awareness of its employees on data and information security issues.

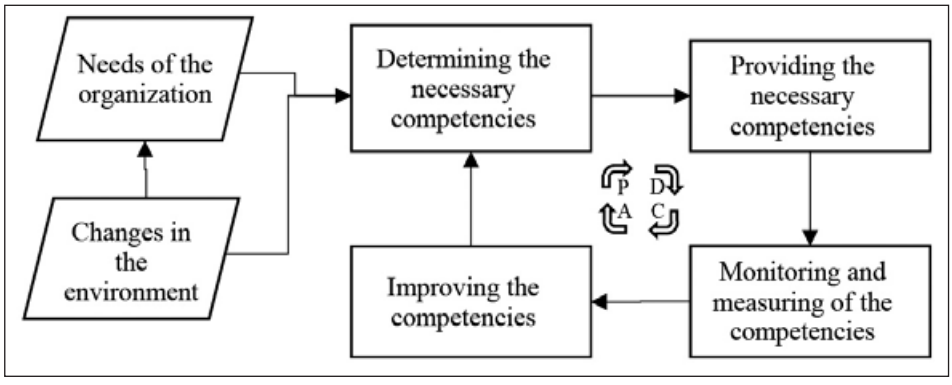

Figure 1: *The process of providing the necessary competencies*

1. The first requirement of clause 7.3 of the standard is that ***all employees who perform tasks managed by the organization are aware of the quality policy***.

Here, as in the case of requests related to employee competencies, the request applies to *all employees in the organization* as well as *other persons* (individuals or members of other organizations) who, on any basis, perform tasks for which the organization is responsible. The essence of the request is that all employees:

- *are acquainted with the existence, content and essence* of data and information security policy,
- *understand and accept* the importance of that policy,
- *recognize their place and role* in the implementation of that policy and actively participate in it.

To meet this requirement, it is necessary that the data and information security policy is defined clearly, unambiguously and understandably for all employees, regardless of their status in the organization. It is also necessary for the management of the organization at all levels, by a detailed interpretation of this policy, to ensure that all employees take *the same, positive* attitude towards it and accept it as a solid and stable framework for their actions in the organization. In addition, the ongoing obligation of management is to monitor the level of awareness of employees about data and information security policies and take appropriate measures to improve them. In this regard, management should establish a process for monitoring and measuring the degree of understanding, acceptance and implementation of data and information security policies and, based on the results of those monitoring, take appropriate action.

2. Employees must ***be aware of their contribution to the effectiveness and efficiency of the data and information security management system***.

The contribution of the employee in the realization of the goals of the data and information security management system can be different in types and intensity. It can be positive or negative, small or large, ***but it cannot be neutral***! Employees must be aware of the fact that *each of their activities*, regardless of its characteristics, in some way *affects the level of data and information security*. In doing so, they must *be aware of the type and intensity of their influence* and, on that basis, *aware of the necessary way of their action* in order for their contribution to be within the expected limits. In doing so, they must be aware of the type and intensity of their influence and, on that basis, aware of the necessary way of their action in order for their contribution to be within the expected limits. In other words, employees must be in a proper way *informed of the possible consequences of their activities,* as well as the way in which *they must act so that those consequences are not be negative but, where possible, positive*. This approach enables ***proactive action*** of all employees in accordance with their status in the organization and ***continuous improvement*** of the level of data and information security in the organization and the performance of its information security management system.

What should the organization do?

Starting from the fact that a man is the most important element of any management system, its strongest but often the weakest element, the management of the organization must *recognize the strengths and weaknesses* of its employees regarding information security. Management should, in an appropriate manner, *inform employees* of this and take measures to *use existing forces and increase them*, as well as *eliminate or reduce to an acceptable level* the characteristics of their employees that may adversely affect the level of data and information security. It should be borne in mind that the identified strengths and weaknesses do not arise solely from the characteristics of the employee (education, experience, culture, habits...) but also from factors arising from the characteristics of the organization: type of activity, context of the organization, organizational structure, personnel structure, organizational culture, etc.

The constant task and continuous activity of the organization's management should be to *develop, monitor and evaluate* the level of awareness of employees about *their* (potential and actual) contribution to data and information security. At the same time, it is necessary to ensure that employees *realistically see their (actual and potential) influence and contribution* in this area, because any unrealistic as-

sessment of their own influence and contribution (increase or decrease) can lead to undesirable consequences. One of the most effective ways to achieve the expected results in this area is the *active involvement of all employees* in addressing issues in the field of data and information security, in accordance with their status in the organization through:

- *timely and complete two-way informing* ***(both management by employees, as well as employees by management)*** about the occurred and possible *("near miss")* cases of endangering the security of data and information, with emphasis on events that occurred as a result of poor professional practice and due to non-application of defined preventive measures,
- *informing about new sources and methods of endangering* the security of data and information, as well as ways of protection from them,
- *collecting opinions and suggestions from employees* regarding data and information security,
- *application of appropriate forms of motivating and stimulating* employees for an active approach to solving problems related to data and information security,
- *developing and implementing an approach to reporting* on data and information security events aimed at increasing *the efficiency of the system, rather than identifying shortcomings and taking repressive measures*.

This procedure is shown in Figure 2. It is noticeable that the essence of the process is *the continuous flow of information and efficient communication between the management of the organization* and employees on data security and information issues.

In that way, the employee will become a conscious, active and useful subject of the data and information security management system.

The process of monitoring and measuring employee awareness of their impact on data and information security, as well as in the case of monitoring and measuring their competencies, must be based on the development and application of appropriate ***indicators*** of compliance with employee awareness requirements (policy implementation, achievement of goals, etc.), as well as ***the criteria*** for drawing conclusions in this regard. These indicators and criteria must also be harmonized with the real situation, needs and capabilities of the organization, in order to enable obtaining the results applicable in the processes of improving the data and information security management system. Given the connection between the impact of competence and employee awareness on data and information security, it is recommended that, when developing indicators and criteria, these two parameters be considered simultaneously, taking into account their mutual influences.

3. A particularly important requirement, which is directly related to the previous one, is that employees must ***be aware of the consequences of non-compliance with the requirements of the data and information security management system***.

Requirements for the effectiveness and efficiency of the data and information security management system are defined by the organization's management with appropriate documents that are binding for all members of the organization and, in certain cases, for members of other organizations and individuals who perform certain tasks related to the organization. These requirements, primarily, include the requirements of binding documents (laws, bylaws, regulations...). Also, if management decides, the requirements of appropriate, non-binding, external documents (standards, guidelines, rules of

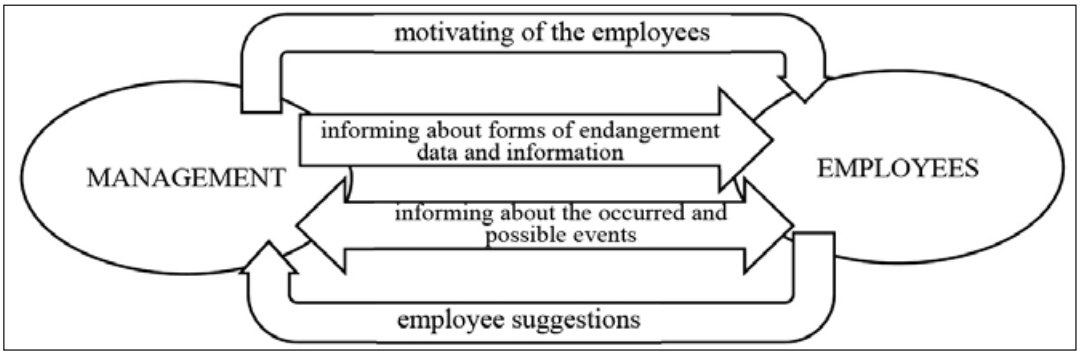

Figure 2: *Active involvement of employees in the data and information security management process*

practice, etc.) may be included. *Any deviation from the observance and application* of these documents and full or partial deviation from the satisfaction of their requirements - *non-compliance* - can have different, often unforeseeable, consequences for the security of data and information that organization disposes. This can also jeopardize the survival of the organization.

The organization must, based on the analysis of the information security risks of the process and the requirements related to the key elements of the process, identify possible non-compliances, their causes and consequences. The organization must then evaluate the consequences of non-compliance and determine their possible impact on the effectiveness and efficiency of the data and information security management system. The results of these analyzes must be, to the extent necessary, available to all employees so that they can, within their powers and responsibilities, apply them in the implementation of their activities.

CONCLUSION

The security of data and information is one of the key factors for the sustainable success of the organization, given the importance of data and information for the business of the organization, as well as the possibility of incalculable harmful consequences through unauthorized and malicious use. The development and functioning of an effective and efficient data and information security management system is one of the most important preconditions for reducing *the information security risk* and the possibility of *adverse events* related to data and information security.

According to the International Standards of the *SRPS ISO/IEC 27000* series, the issue of the functioning of the data and information security management system is considered from several aspects. The most important aspect is defining the ***requirements*** that this system should meet in order to be able to provide effective data and information security management in the organization. Requirements for ***competence*** and ***awareness*** of employees in the field of data and information security are, although this, at first glance, is not noticeable at first glance, two very important requirements for the effective and efficient functioning of this system.

The importance of employee ***competencies*** and their ***awareness*** in terms of achieving, maintaining and improving the effectiveness and efficiency of data and information security management systems stems from their status in the organization, ie. from the functions they perform and the responsibilities and powers that arise from it.

What is most important regarding the implementation of the requirements of the International Standard *SRPS ISO/IEC 27001,* related to the competencies and awareness of employees, is the following:

- The organization must *pay special attention* to ensuring the necessary competencies of employees, as well as developing and maintaining their awareness regarding data and information security issues.
- The organization must *establish processes to monitor and measure* compliance with both requirements.
- For monitoring and measuring the satisfaction of the considered requirements, the organization must *define indicators and criteria* on the basis of which it will monitor and measure the degree of satisfaction of the requirements and, based on the obtained results, make appropriate decisions.
- The consequences of not meeting the requirements considered can be very detrimental to the organization, including its success, image and survival in the market.
- To meet the considered requirements, the organization must plan to engage appropriate resources (human and material), as well as all other investments in achieving and maintaining the effectiveness and efficiency of data and information security management systems, which will result in multiple, tangible and intangible benefits for the organization.

Due to all the above, the top management of each organization must, as its priority tasks, define:

- Publication and consistent application of data and information security policy and, accordingly, policy of development and maintenance of necessary competencies of employees in relation to data and information security issues.
- Development and maintenance of awareness of employees at all levels in the organization about the importance of data and informa-

tion security for the organization's business, as well as their importance for achieving and maintaining the required level of data and information security.

With this approach, the organization gains another solid support that enables its sustainable success and continuous business in a modern, very demanding business environment.

REFERENCES

[1] International Standard SRPS ISO 9000:2015 Quality Management Systems - Fundamentals and Vocabulary, Institute for Standardization of Serbia, Belgrade, 2015.
[2] International Standard SRPS ISO/IEC 27000:2018 Information Technology - Security Techniques - Information Security Management Systems - Overview and Vocabulary, Institute for Standardization of Serbia, Belgrade, 2018.
[3] International Standard SRPS ISO/IEC 27001:2014 Information Technology - Security Techniques - Information Security Management Systems - Requirements, Institute for Standardization of Serbia, Belgrade, 2014.
[4] SRPS ISO/IEC Guide 73:2004 Risk Management - Vocabulary - Guidelines for Use in Standards, Institute for Standardization of Serbia, Belgrade, 2004.

Submitted: June 15, 2020
Accepted: October 12, 2020

ABOUT THE AUTHORS

Vitomir T. Miladinovic, PhD, Assistant Professor (scientific area Road Transport), Professor of Vocational Studies (area of Engineering Management). He was engaged as a freelance researcher (field of Motor vehicles) and head of the standardization service at the Military Technical Institute, Belgrade, lecturer - external associate at the Military Academy, Belgrade, (subject Motor vehicles), consultant for management systems at the company Bonex Engineering Belgrade and professor of vocational study at the College of vocational Studies Belgrade Polytechnic, Belgrade. He published several scientific and professional papers.

FOR CITATION

Vitomir T. Miladinovic, Development of Awareness and Competences of Employees in the Processes of Information Security Management System - guidelines for practical application, *JITA – Journal of Information Technology and Applications Banja Luka*, PanEuropien University APEIRON, Banja Luka, Republika Srpska, Bosna i Hercegovina, JITA 10(2020) 2:87-95, (UDC: 004.6.056:[005.334:351.78), (DOI: 10.7251/JIT2002087M), Volume 10, Number 2, Banja Luka, December 2020 (69-128), ISSN 2232-9625 (print), ISSN 2233-0194 (online), UDC 004