Information & Security

Published since 1998

S. Dotsenko, O. Illiashenko,
S. Kamenskyi & V. Kharchenko
vol. 43, no. 3 (2019): 305-317
https://doi.org/10.11610/isij.4323
ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Research Article

Integrated Model of Knowledge Management for Security of Information Technologies: Standards ISO/IEC 15408 and ISO/IEC 18045

Sergiy Dotsenko [a], ***Oleg Illiashenko*** [b] (✉),
Sergii Kamenskyi [a], ***Vyacheslav Kharchenko*** [b]

[a] *Ukrainian State University of Railway Transport, Kharkiv, Ukraine*
http://kart.edu.ua/en

[b] *National Aerospace University "KhAI", Kharkiv, Ukraine*
https://khai.edu

ABSTRACT:

The paper presents analysis of existing knowledge management models and justification for introducing an integrated model of knowledge management for both industry and academia. It is proposed to build such a model using well-known standards of IT security – common criteria and methodology for IT security evaluation. The model of knowledge management is elaborated by analysing the content of the relevant elements of standards and establishing the knowledge content that determines the forms of relations between them. The authors propose the application of an architecture of four-factor models towards the formation of knowledge management models in the organization of the information security management system in accordance with the standards of the series ISO/ IEC 27000.

ARTICLE INFO:

RECEIVED: 20 AUG 2019
REVISED: 04 SEP 2019
ONLINE: 22 SEP 2019

KEYWORDS:

knowledge management, information security, information technologies, IT security, security standards

✉ Corresponding Author: Tel.: +380954676066; E-mail: o.illiashenko@khai.edu

Introduction

It is essential to form an integrated security system to bring into life the Industry 4.0 concept in full. The focus of this paper is on security of information technologies. In the field of information technologies security there are two approaches to the formation of security systems.

On the one hand, there are studies that are being carried out to develop business models for information security,[1] as well as an integrated model of security awareness to evaluate its risks.[2] Studies of compliance of information security policies are also carried out, specifically, the integration of the theory of planned behaviour and the protection motivation theory.[3]

On the other hand,[1] the relevant international and national standards for security of informational technologies are analysed and implemented. In particular, provision of enterprise security systems is based on the standards of the ISO/IEC 15408 series, parts 1-3,[4;5;6] which define the methods and tools for providing and criteria for evaluating the security of information technologies. Together with the standards of ISO/IEC 18045 series, which defines methods and tools for security of information technologies, the security evaluation methodology [7] is used.

During the application process of the abovementioned standards the problem of knowledge management, which is formed in these standards, appears. By that, the process of gaining new knowledge through the establishment of appropriate links between the structural elements of these standards is meant.

However, the development of knowledge management models for these standards, which would have been the basis for the formation of appropriate information security management systems, has not yet been carried out. At the same time, standard ISO/IEC 15408-1 [4] states that there are relevant links among the elements of these standards, but the form of these links is not clearly defined and the method of their establishing is not proposed. Consequently, the task of defining the method of forming such connections arises, for example, in the form of an appropriate *knowledge management model*. Its development will enable the creation of a library (or a set) of standard forms of knowledge management models for appropriate information technology security systems. This is especially relevant when implementing an information security management system in accordance with a series of standards ISO/IEC 27000.[8]

The goal of this paper is in the justification of the choice of the method of knowledge management model formation for ISO/IEC 15408 series standards and ISO/IEC 18045:2008 standard. The structure of the paper is the following. Section II analyses the existed models of knowledge management and discusses possibilities of their application for development of integrated model. Section III describes the suggested integrated model of knowledge and algorithms of its development and application for the standards ISO/IEC 15408 and ISO/IEC 18045. Section IV concludes the paper and discusses the results and future research.

Analysis of Models of Knowledge Management

An analysis of some well-known models in knowledge management was performed in: [9]

- Lawson's model for identifying one of the knowledge management tools;[10]
- The model by Lee and Choi for evaluating organizational culture and measuring other factors.[11]

Several studies have also been carried out to measure the knowledge management process as an indirect factor.[12]

The study identifies two perspectives on the knowledge management process: social and technical. For the social perspective and the organizational culture, the structure and people are distinguished. For the technical perspective, the information technologies are distinguished. On the basis of expert assessments, interrelations between structure, culture, people and information technologies are established through knowledge management and organizational creativity.

Business Model

The business model for *information security* is presented in [13] (see Fig. 1). It contains four components:

- organization (design and strategy);
- people;
- technology;
- process.

For these components, the forms of connections are established as in the previous work. However, the task of forming a security *system* in the organization is not raised in it.

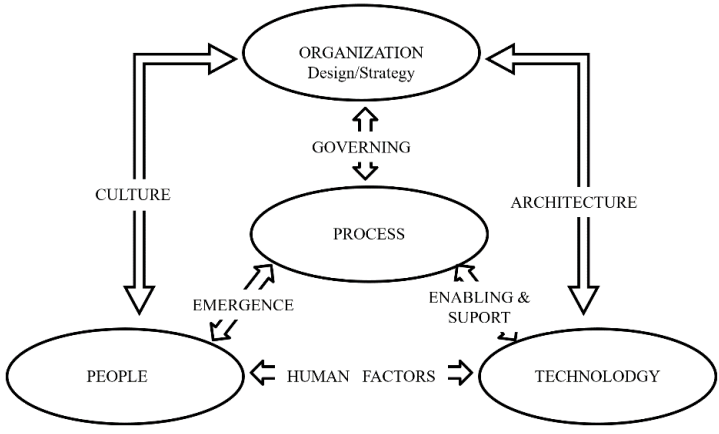

Figure 1: The Business Model for Information Security.

And so, it could be truly said that there is a certain contradiction obviously introduced be the developers of the studied regulations. On the one hand, standards have been developed that will determine the requirements for security systems, but they do not have the theoretical justification. And on the other hand, there are theoretical works that establish appropriate recommendations for integrated knowledge management models for information technology security systems, but these recommendations do not have sufficient practical implementation.

It should also be noted that the concept of a culture of security is included as an important component of the business model for information security (see Table 1).[13]

This table represents the content of the four elements of the business model for *information security*, which was investigated by ISACA[13] before the implementation of the security culture concept in this model and after its implementation.

Table 1. Shifting from Functional to Intentional Security Culture.

FROM	*TO*
Technology	
• Uncertainty about the level of security the technology provides • Seeing security-related technology as disruptive and cumbersome to use	• Technology used is based on an assessment of the risk. • Seeing new security technology as a means to enhance the sales process
Process	
• Security brought in when there is a suspected breach • Security is maintained by an expert knowledge	• Security involvement in the earliest planning phases of campaigns • Security shares its knowledge and expertise, developing broader security awareness across the enterprise.
People	
• Security as an entity that enforces compliance • Security as a functional expert	• Security "as a partner" that creates awareness and commitment • Security "as a partner" that transfers security knowledge and expertise to its sales customers
Enterprise	
• Limited visibility or awareness of security issues • Security structure focused on technical expertise	• Receiving regular updates about potential risk • Security structure supports processes of its customers

Conceptual Model

Raudeliūnienė et al. proposed an improved conceptual model of knowledge management process (see Fig. 2).[14]

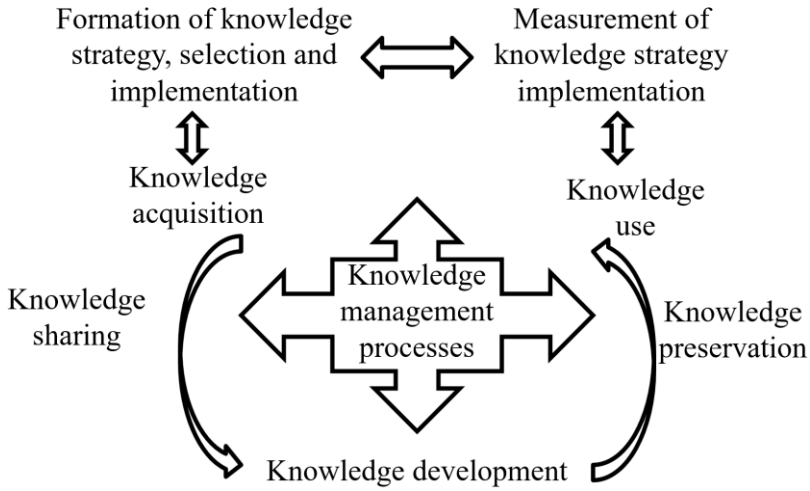

Figure 2: Improved Conceptual Model of Knowledge Management Process.

The specific recommendations for the formation of the composition and content of elements of knowledge management models are not included in the considered models of knowledge management. This problem can be solved developing an appropriate model of knowledge management as an expert system. However, its creation is connected to the necessity of pre-designing the database, output machine and other elements of the expert system. Such systems, as a rule, are unique in design and require significant material, human and financial resources.

Therefore, the problem arises to find other methods of forming a knowledge management model. Requirements for such a model are as follows:

- knowledge management should be simple;
- the knowledge management model should have an open architecture;
- the model must be universal, without dependency of the content of knowledge.

DMT Based Model

According to Steinberg, the didactic multidimensional technology, based on visual didactic multidimensional instruments,[15] is actively developing in the search of solutions of this problem.

The concept of visual didactic multidimensional tools (DMT) consists in transforming the verbal, textual or other form of information representation into a

visual, figurative-conceptual form, which is characterized by three parameters: *semantic (meaningful)*, *logical* and *special graphic*.

The multidimensionality of the theme displayed by the tool is provided by three components (Fig. 3,[15] where K1-K8 – Coordinates – directing measurements of the subject being studied):

- logical-semantic modelling;
- cognitive presentation of knowledge;
- radial-circular organization.

The content of the specified coordinates is determined for a specific subject area at the stage of development. Therefore, there is no universal definition of the content of these coordinates. When implementing DMT information is converted using the following principles:

- the principle of system-multidimensionality in the selection and consolidation of content;
- the principle of splitting and merging and the related principle of additionality in the formation and using of DMT;
- the principle of trinity in the formation of semantic groups that enhance psychological stability.

This concept does not have an unambiguous theoretical justification for each of these bases of multidimensionality of the subject being studied. In these models eight coordinate models of knowledge management are used as a rule.

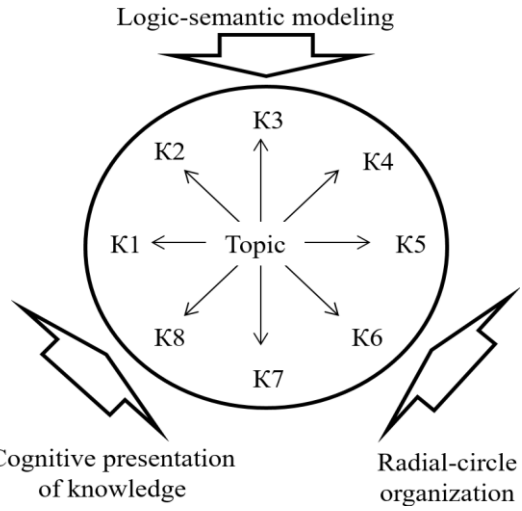

Figure 3: Trinity Basis of DMT.[15]

Model of Strategical Thinking

Krogerus and Tschäppeler presented fifty models of strategic thinking.[16] It should be noted that among them there are ten models that have a four-vector architecture, which is similar to the Cartesian coordinate system architecture. Fig. 4 shows an example of such an architecture. Model analysis shows that the four-vector graphical representation of knowledge can be the basis for a knowledge management model for a particular subject area, since there are relations between pairs of factors that are characterized by a certain content of knowledge about these relationships, specifically: Me – Thought; Me – Actions; They – Thought; They – Actions. On this basis, a knowledge base about the subject area, which is characterized by these factors, is formed.

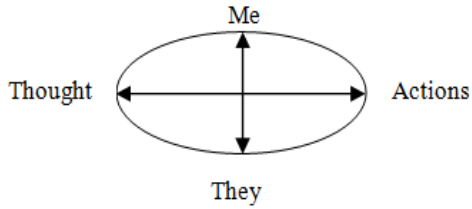

Figure 4: Version of the Model of Strategic Thinking.

From the analysis of the methods of forming knowledge management models based on the concepts of a business model,[13] a conceptual model,[14] didactic multidimensional tools,[15] and models of strategic thinking [16] it follows that these concepts correspond to specific subject areas and do not have a clear theoretical justification. At the same time, a special attention should be paid to the last two models. In these models the relations are established in an explicit form between the elements of adjacent factors.

To quantify the content of these relationships as a metric, it is recommended to use the metric in the form of the ratio of the number of non-zero elements for Cartesian products of each factor pair of adjacent model vectors (see Figures 3 and 4) to the total number of elements for all pairs of adjacent vectors.

Revealing the content of these relationships provides the establishment of the content of knowledge that characterizes these relationships, but no recommendations on the formation of the appropriate knowledge base.[15,16] This impedes the practical application of these models. Therefore, the task of developing proposals for the practical implementation of these models for the standards of ISO / IEC 15408, ISO / IEC 18045 is actual.

The problem of theoretical justification of four-factor knowledge model architectures is of independent importance. The solution to this problem lies beyond the scope of this study.

The Model of Knowledge Management for Standards ISO/IEC 15408 and ISO/IEC 18045

Development of the Model

We propose the usage of four-factor knowledge structuring models to establish relationships between the elements of the standards of the ISO/IEC 15408 series and the ISO/IEC 18045 standard. Preliminary analysis showed that it is possible to establish special links between elements of these standards as shown in Fig. 5.

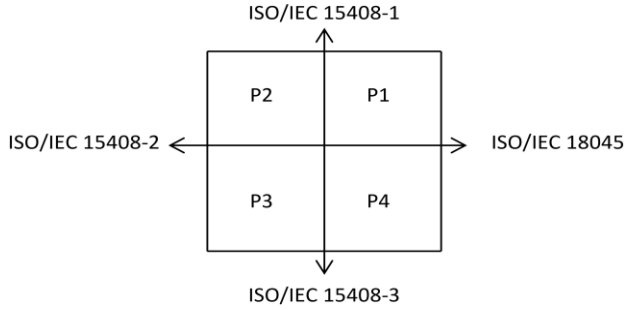

Figure 5: Knowledge Management Model.

For the knowledge management model for the generated matrices, the special metric is proposed to be calculated in the next way.

The total power of the Cartesian product for adjacent pairs of vectors of factors is determined:

$$| E^{(18045)} \times E^{(15408-1)} |; | E^{(15804-1)} \times E^{(15408-2)} |;$$

$$| E^{(15804-2)} \times E^{(15408-3)} |; | E^{(15804-3)} \times E^{(18045)} | .$$

After that, the Cartesian product capacities for the adjacent pairs of factor vectors with non-zero elements are calculated:

$$| \Delta(E^{(18045)} \times E^{(15408-1)}) |; | \Delta(E^{(15804-1)} \times E^{(15408-2)}) |;$$

$$| \Delta(E^{(15804-2)} \times E^{(15408-3)}) |; | \Delta(E^{(15804-3)} \times E^{(18045)}) | .$$

Based on the results of these calculations, the percentage of Cartesian output with non-zero elements relative to the total Cartesian output is calculated.

$$M_E = \frac{|\bigcup_{i,j} \Delta E^{(i),(j)}|}{\bigcup_{i,j} (E^{(i)} \times E^{(j)})}.$$

Fig. 6 shows a screenshot of the automation tool developed as a Microsoft Excel spreadsheet. Figure 7 shows a screenshot of the Microsoft Office Excel spreadsheet (quadrant P4 in Fig. 5).

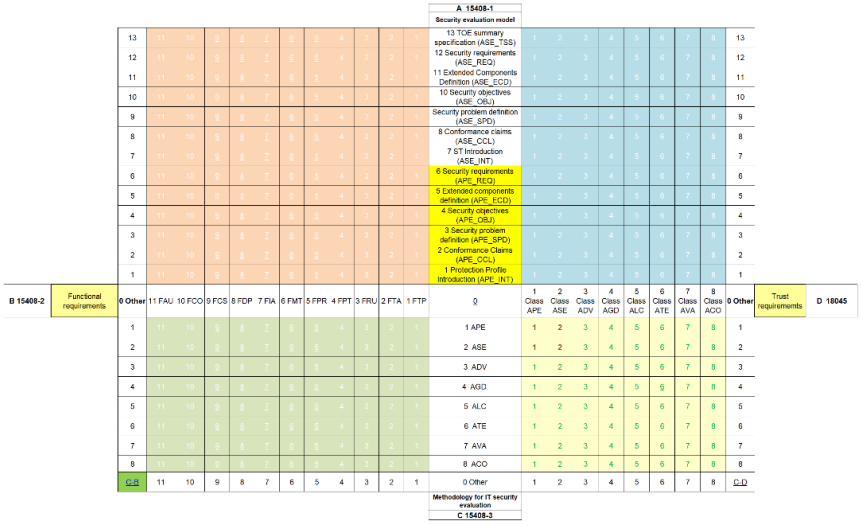

Figure 6: Screenshot of the Automation Tool Spreadsheet.

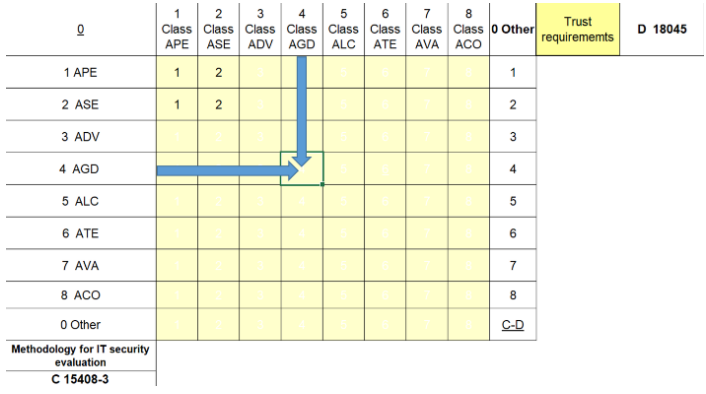

Figure 7: Screenshot of the Fragment of Automation Tool Spreadsheet (Quadrant P4 in Fig. 5).

The contents of all abbreviations given in Figures 6 and 7 are defined in the relevant standards, which are indicated for the respective axes, namely:

- ISO/IEC 15408-1:2009 Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model (the acronyms are indicated in the Fig. 6);
- ISO/IEC 15408-2:2008 Information technology — Security techniques — Evaluation criteria for IT security — Part 2. Security functional components (*Classes of functional requirements*: FAU – Security audit, FCO – Communication, FCS – Cryptographic support, FDP – User data protection, FIA – Identification and authentication, FMT – Security management, FPR – Privacy, FPT – Protection of the TSF, FRU – Resource utilization, FTA – TOE (Target of Evaluation) access, FTP – Trusted path/channels));
- ISO/IEC 15408-3:2008 Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components (*Classes of trust requirements*: APE – Protection Profile evaluation, ASE – Security Target evaluation, ADV – Development, AGD – Guidance documents, ALC – Life-cycle support, ATE – Tests, AVA – Vulnerability assessment, ACO – Composition);
- ISO/IEC 18045:2008 Information technology — Security techniques — Methodology for IT security evaluation (*Classes of Methodology for IT security evaluation*: APE – Protection Profile evaluation, ASE – Security Target evaluation, ADV – Development, AGD – Guidance documents, ALC – Life-cycle support, ATE – Tests, AVA – Vulnerability assessment, ACO – Composition).

The formation of a model of knowledge management is carried out by analysing the content of the relevant elements of standards and establishing the content of knowledge that determines the forms of relations between them. The knowledge formed in such way is entered into the corresponding cell by one of the above methods. The proposed model of knowledge management is integrated because it includes various sources of knowledge about the subject area (content standards). Establishing additional relations between these sources provides the formation of *new knowledge* about the chosen subject area, which is also the result of knowledge management.

Application of the Model

The sequence of constructing and using the integrated model is as follows.

In the first stage, the formation of composition and content of the elements of the relations is performed by analysing the content of the relevant elements of the standards and establishing the content of knowledge that determines the forms of relations between them with a non-zero value for each of the matrices P1 – P4.

Structural elements are allocated for each of the standards (see Fig. 5). For the standard like an ISO/IEC 15408-1, such items have been selected as the composition and contents of the *security specification*, as well as the *security profile specification*. For ISO/IEC 15408-2, the classes have been selected as elements that describe *functional security elements*. For ISO/IEC 15408-3, classes that describe the *security assur-*

ance are selected as *elements*. For ISO/IEC 18045, *subsystems for evaluation the security* of information technology have been selected as elements. This method of integration is based on the functional representation of the enterprise. It involves the integration of enterprise management systems and production process management systems, that means, the integration of the two control systems of parts of the enterprise into a whole one.

The correlation of the elements of the respective pairs is performed in the following sequence:

- ISO/IEC 15408-1 – ISO/IEC 15408-2;
- ISO/IEC 15408-2 – ISO/IEC 15408-3;
- ISO/IEC 15408-3 – ISO/IEC 18045;
- ISO/IEC 15408-1 – ISO/IEC 18045.

In case where the presence of relations is established for the corresponding pair of elements, an appropriate *content of knowledge* about these relations is formed. A document containing the content of this knowledge should be associated with the corresponding cell through a hyperlink. To access the contents of this document it is enough to go over the hyperlink of the corresponding cell. Thus, the formed matrices are reference. For each of the P1-P4 matrices, the corresponding M_{E1e} - M_{E4e} metrics, which are subsequently used as benchmarks, are calculated.

After the formation of knowledge for all relations is done, application of the formed model of knowledge management is possible.

In the second stage, the *information security system formation* at the enterprise is carried out by forming a description of the object of assessment and forming a security profile for specific information technologies that are planned for use. This requires knowledge of the requirements that are formed in the elements of the planes P2 and P3 (see Fig. 5). For each of the matrices P2 and P3, the corresponding metrics M_{E2} and M_{E3} are calculated.

In the third stage, the knowledge, which is formed in the documents, the messages to which are contained in the cells of planes P1 and P4, is used to carry out the assessment of *information technology security* according to ISO / IEC 18045.

At the same time, the composition and content of the actual measures that are being implemented are checked. The knowledge thus formed is entered into the corresponding cell by one of the above methods. The contents of the cells are then compared with non-zero values. The degree of compliance of the implemented measures with the requirements set out in the standard is established. Full compliance is rated "one." The discrepancy is rated zero. Intermediary estimates are possible. After that, real metrics M_{E1} and M_{E4} are calculated for the P1 and P4 matrices. The comparison with the benchmark of the relevant metrics establishes the degree of compliance of the actual security measures for the particular assessment entity with the ideal requirements.

For current information technology, the total value of M_E metrics is calculated, which is further used to assess the current level of information technology security.

Conclusions

The paper substantiates the choice of the method of knowledge management model formation for ISO/IEC 15408 and ISO/IEC 18045: 2008 standards. It is proposed to choose four-factor model of knowledge management. It meets the requirement of open architecture, is accessible to the user, as well as universal in relation to the subject area.

The developed model can be applied both for the analysis of existing knowledge for the chosen subject domain and for the synthesis of new knowledge. In the latter case, it is sufficient to form the composition and content of the elements of coordinate meshes.

The architecture of *four-factor models* is proposed to apply also for the formation of knowledge management models in the organization of the information security management system in accordance with the standards of the series ISO / IEC 27000.

The developed conception and models have been adopted and implemented at the PC "RPC Radiy" in Kropyvnytskyi, Ukraine and PrJSC FED in Kharkiv, Ukraine.

The task of forming a reference model is planned for further research. The future steps can be dedicated to development application of the described model considering integrated safety and security management system.[17]

Acknowledgements

This work was supported by the ECHO project which has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement no. 830943.

The authors appreciate the scientific society of the ECHO consortium and in particular the staff of Department of Computer Systems, Networks and Cybersecurity of the National Aerospace University "Kharkiv Aviation Institute" for invaluable inspiration, hardworking and creative analysis during the preparation of this paper.

References

1 "An Introduction to the Business Model for information Security," ISACA, USA, 2009, https://www.isaca.org/Knowledge-Center/Research/Documents/Introduction-to-the-Business-Model-for-Information-Security_res_Eng_0109.pdf.

2 Roberto Mejias, "An Integrative Model of Information Security Awareness for Assessing Information Systems Security Risk," Proceedings of the Annual Hawaii International Conference on System Sciences (2012): 3258-3267, https://doi.org/10.1109/HICSS.2012.104.

3 Princely Ifinedo, "Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory", *Computers & Security* 31, no. 1 (February 2012): 83-95.

4 ISO/IEC 15408-1:2009 Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model, 2009.

[5] ISO/IEC 15408-2:2008 Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components, 2008.

[6] ISO/IEC 15408-3:2008 Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components, 2008.

[7] ISO/IEC 18045:2008 Information technology — Security techniques — Methodology for IT security evaluation, 2008.

[8] ISO/IEC 27000:2014 (E) Technologies de l'Information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Vue d'ensemble et vocabulaire, 2014.

[9] Maha Alkaffaf, Monira Muflih, and Mahmoud Al-Dalahmeh, "An Integrated Model of Knowledge Management Enablers and Organizational Creativity: The Mediating Role of Knowledge Management Processes in Social Security Corporation in Jordan," *Journal of Theoretical and Applied Information Technology* 96, no. 3 (15 February 2018): 677-700.

[10] Lawson, S. "Examining the relationship between organizational culture and knowledge management," Doctoral dissertation, Nova Southeastern University, 2003.

[11] Lee H. Choi, "Knowledge management enablers, process, and organizational performance: an integrative view and empirical examination," *Journal of Management Information Systems* 20, no. 1 (2003): 179–228.

[12] Rifat O. Shannak, "Measuring Knowledge Management Performance," *European Journal of Scientific Research* 35 no. 2 (2009: 242-253.

[13] ISACA, "An Introduction to the Business Model for information Security," https://m.isaca.org/Knowledge-Center/Research/Documents/Introduction-to-the-Business-Model-for-Information-Security_res_Eng_0109.pdf.

[14] Jurgita Raudeliūnienė, Vida Davidavičienė, and Artūras Jakubavičius, "Knowledge Management Process Model," *Entrepreneurship and Sustainability* 5, no. 3 (2018): 542-554, https://doi.org/10.9770/jesi.2018.5.3(10).

[15] Valery E. Steinberg, *Theory and practice of multi-dimensional teaching technology* (Moscow, National education, 2015).

[16] Mikael Krogerus and Roman Tschäppeler, *50 Erfolgsmodelle - Kleines Handbuch für strategische Entscheidungen - Neuausgabe* (Zürich, Kein &Aber, 2008), 200.

[17] Vyacheslav Kharchenko, Sergiy Dotsenko, Oleg Illiashenko, and Sergiy Kamenskyi, "Integrated Cyber Safety and Security Management System: Industry 4.0 Issue," *Proc. of the 10th IEEE Dependable Systems, Services and Technologies Conference, DESSERT 2019*, Leeds, United Kingdom (2019): 197-201.

About the Authors

See p. 304 in this volume.