RESEARCH JOURNAL OF THE UNIVERSITY OF GDAŃSK

Transport Economics and Logistics Vol. 82 (2019)
https://doi.org/10.26881/etil.2019.82.07

Natalia Jagodzińska

BTCH Management System, Poland

IMPLEMENTING INFORMATION SECURITY MANAGEMENT SYSTEMS IN TRANSPORT INDUSTRY ORGANIZATIONS

Abstract

The aim of the publication is to present the concept of information security management systems and new requirements concerning such systems and indicate security areas and their application in the transport industry. Moreover, the effects of implementing the ISO 27001 requirements in the organizational culture in the transport sector enterprises will be outlined.

Keywords: ISO 27001, information security, information security management system

JEL: P4, L1, L9

Introduction

The transport industry is one of the fastest developing areas of economy. Transport companies are increasingly often seeking and implementing system tools to manage their organization. The ISO series systems were implemented partly by reason of the legal requirements stipulating that, for example, the HACCP system (2001) (food safety management) for the transport of food products should be introduced (The Act on Health Conditions…, 2001). Subsequently, suppliers were forced by corporations of large retail chains to have BRC (2015) and IFS (2017) systems in place. It was the market itself and the opportunity of being competitive that forced enterprises in the transport sector to implement the popular quality management system ISO 9001 (Quality Management Systems – Requirements…, 2016). Furthermore, system solutions are implemented more and more frequently, depending on the transport mode. To give an example, ISO 28001 (International Organization for Standardization, 2007) is increasingly often implemented in the road transport

to manage the supply chain – which, as claimed by Skojett-Larsen (1999) – is not an easy task in the adaptation to the organizational culture of an enterprise. Another example is the railway sector where the implemented safety systems are the standards EN 50126 (Railway Applications…, 2011) or IRIS (International Railway…, 2005) unifying the rules of security for all organizations participating in the railway transport (Białoń and Pawlik (2014) note that the standard (PN-IEC 60300-3-9) also applies in this area).

As far as management systems are concerned, great interest has been recently shown in the information security management system (ISO 27001). Before that time, interest in the system had been shown by financial, medical and governmental organizations often by reason of the importance of processed data. However, for several years, it has been possible to observe great interest in this system in various industries, including the transport sector. Small and medium-sized transport enterprises have started to see how valuable information is becoming aware that it should be protected. According to the data provided by certification bodies, such as SGS (*Liczba certyfikacji systemów…*, 2017) or TUV SUD (*ISO Survey 2016…*, 2016) a considerable increase in the number of certifications for these systems has been observed recently.

Research on the implementation of information security systems was carried out among transport industry companies. The studies have shown that it is a necessary system for this area of activity, and its implementation significantly affects changes in the organization. These changes mainly concern management methods and tools, competencies and awareness of people in the organization, identifying threats and incidents, and information management.

1. Information security management system concept

The international information security management standard has been defined in the form of the standard: PN-EN ISO/IEC 27001:2017-06 – Information Technology – Security Techniques – Information Security Management Systems – Requirements. An enterprise holding an ISO 27001 certificate (Information Technology…, 2018) is often perceived as a reliable business partner. It should be noted that the ISO 27001 standard "frees" the enterprise from formalized written procedures describing every activity to implement effective actions. These actions should be documented in any manner according to the so-called "Documented information" i.e., for example, instead of a detailed procedure, the enterprise may use an application managing a given area with defined tasks and specific access rights.

The concept of the system is to build a string of actions and sequences to ensure comprehensive management of data in the organization. Similarly to all ISO standards, this system is based on the PDCA Deming circle philosophy.

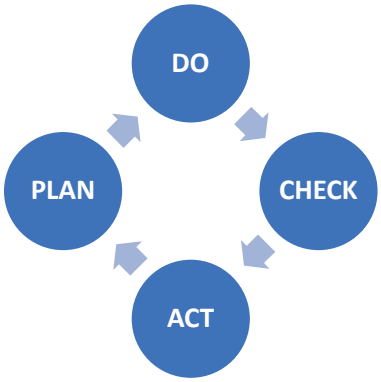

Figure 1. PDCA-Deming circle philosophy
Source: (own elaboration based on: Information Technology…, 2018)

The Deming cycle based on the PLAN-DO-CHECK-ACT principle in an information security management system should be understood as:

1. PLAN – identify and plan actions to attain a goal, which means that you should:
   – define the information security policy;
   – define the scope of the system;
   – identify and assess the risk;
   – establish a risk management plan;
   – define the methods to measure the effectiveness of the applied controls.
2. DO – carry out the planned actions as a trial, which means that you should:
   – implement a risk management plan (apply security controls);
   – implement a training and awareness program;
   – manage the resources;
   – implement procedures and controls.
3. CHECK – check whether the implemented plan was effective, if it brings results and how this process can be improved, which means that you should:
   – check if the procedures are followed:
     • review the effectiveness of the information security management system;
     • review the level of residual and acceptable risk;
     • conduct internal audits;
     • have the information security management system inspected by the management;
     • record the actions and events affecting the information security management system effectiveness.
4. ACT – improve the process that has worked or correct the errors in an unsuccessful process which means that you should:
   – implement and improve the information security management system;
   – implement the identified improvements;
   – register inconsistencies;
   – take corrective actions.

Hence, we can say that the objective of the information security management system is to ensure the selection of adequate and proportionate controls to protect information assets and ensure trust in the stakeholders.

Attention should be also paid to what information is, where it occurs and what ensures its security. The new ISO 9000 standard (Quality Management Systems – Fundamentals…, 2016) defines a document as information and its medium, and the ISO 27001 standard uses the concept of documented information. Such documented information are:

– all IT systems containing a series of data in various applications located on the firm's servers or in cloud solutions;
– all paper documents used in offices and used by customers, suppliers, employees and the outsourcing personnel, e.g. the accounting office;
– information and knowledge "in people's heads" – knowledge about events, figures, contacts, experience, education – this is the documented information that is most difficult to manage.

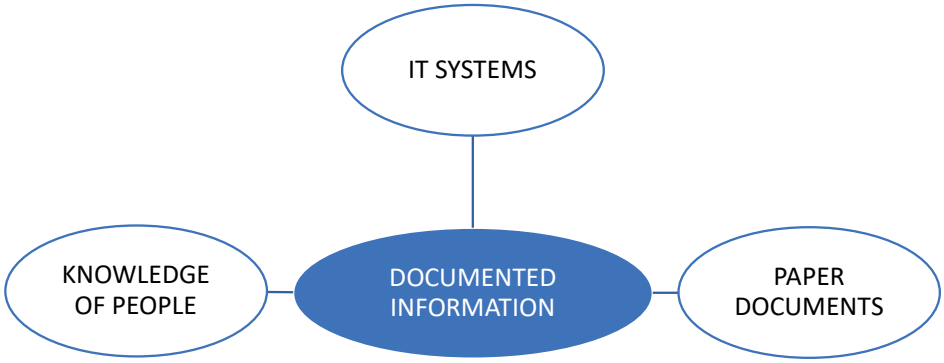

Figure 2. Object components – documented information
Source: (own elaboration)

The notion of the asset must be mentioned in the context of documented information. Information means "assets that unlike other important business assets are necessary for business organization and, in consequence, require an adequate protection (...)" according to PN-ISO/IEC 27000: 2014 (3.2.2) and more precisely "information is significant data" according to PN-EN ISO 9000:2015 (3.7.1). Recapitulating – assets are everything that is of any value for the organization. Hence, the security of documented information – of the assets – has three main attributes: confidentiality, accessibility and integrity. Taking into account the objective, which is to ensure uninterrupted business success and going concern and to minimize the effects, information security consists in applying and managing the adequate security controls, which in turn consists in contemplating a wide range of threats as defined in ISO/IEC 27000:2014 (Information Technology…, 2014).

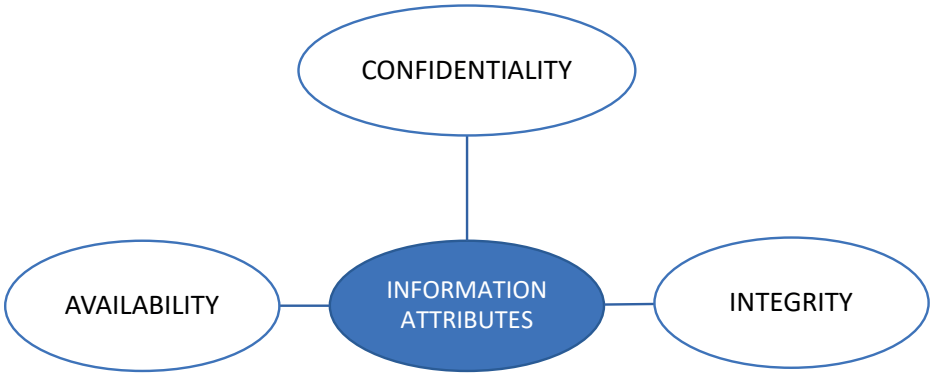

Figure 3. Information attributes
Source: (own elaboration)

To explain, the attributes of information are:

– confidentiality of information – the quality consisting in the fact that information is neither shared with or disclosed to unauthorized persons, entities or processes;
– integrity of information – the quality to ensure the completeness and accuracy of information;
– availability of information – the quality of being available and useful to an authorized entity on demand.

Let us come back to the concept of an information security management system. Once it has been established what information is and what its attributes are, it should be defined what can be done with such data. The task of an organization implementing an information security management system is to define operations or sets of operations performed on the data, including but not limited to collecting, recording, organizing, ordering, storing, adapting or modifying, downloading, browsing, using, disclosing by sending, distributing or otherwise sharing, matching or combining, restricting, deleting or destroying. A premise for an information security management system is that the following rules should be established for the foregoing activities defining: who, what, how, where, when – in respect of ensuring the security of information. And the guidelines on how to effectively protect the system are stipulated in the ISO 27001 standard requirements.

3. Requirements for the information security management system

The requirements for an information security management system are described in detail in PN-EN ISO/IEC 27001:2017-06. Information Technology – Security Techniques – Information Security Management Systems – Requirements. It can be said that this standard consists of two parts, the first part devoted to system solutions and the second part showing the security areas to be applied.

The first part comprises ten chapters which describe the requirements for an information security management system in a systemic manner (like most ISO standards). The requirements are contained, *inter alia*, in clauses related to the scope,

normative references, terms and definitions, the context of organization, leadership, planning, support, operational activities, evaluation of performance and improvement. The standard requires that the following actions should be taken: define the scope of the ISMS, define the ISMS policy, develop mechanisms for systematic risk assessment, identify risks, assess risks, identify and assess risk management variants, select objectives and controls, prepare a declaration of application, prepare a plan how to deal with risk, implement controls, define how to measure performance and implement tools for improving the controls, and then repeat these actions regularly as part of risk reassessment.

The above guidelines are supported by the second part of the standard – Annex A, which contains 117 detailed requirements for the application of controls within the information security management system. These requirements apply to:

A.5 Security policy – information security policy document. Review and assessment. The information security policy should be published and provided to all employees of the company. The objective of the policy should be defined and it should be specified how the information will be secured in terms of confidentiality, integrity, accessibility, accountability and lawfulness.

A.6 Organization of information security – information security infrastructure. Information security management forum. Information security coordination. Allocation of information security responsibilities. Authorisation process for information processing facilities. Specialist information security advice. Cooperation between organizations. Independent review of information. Authorisation process for information processing facilities. Cooperation between organizations. Identification of risk related to external parties. Security requirements in agreements with external parties. Security requirements in third party agreements.

A.7 Human resources security – security when defining roles and responsibilities in management of human resources. Conditions of employment. Non-disclosure agreements. User training. Response to security incidents and improper functioning of the system.

A.8 Asset management – inventory of assets. Inventory categories of information assets. Classification guidelines. Information labelling and handling.

A.9 Access control – business requirements for access control. User access management. User responsibilities. Control of access to the system and applications.

A.10 Cryptographic controls – cryptographic security.

A.11 Physical and environmental security – secure areas. Physical security perimeter. Physical entry controls. Securing offices, rooms and facilities. Working in secure areas. Public access, delivery and loading areas. Equipment security. Equipment siting and protection. Supporting utilities. Cabling security. Equipment maintenance. Security of equipment off premises. Secure disposal or re-use of equipment. General controls. Clear desk and clear screen policy. Removal of property.

A.12 Secure operations – operational procedures and responsibilities. Documented operating procedures. Operating change management. Security incident management procedures. Segregation of duties. Separation of development, test and operational facilities. Protection against malicious code. Controls against malicious code. Recording and monitoring of events. Control of operational software. Information systems audit considerations.

A.13 Security of communications – network security management. Transmission of information.

A.14 Systems acquisition, development and maintenance – security requirements of information systems. Security requirements analysis and specification. Security of application services in public networks. Protection of application services. Security in development and support processes. Test data. Test data protection. Input data validation. Control of internal processing message authentication.

A.15. Information security in relations with suppliers – policy of information security in relations with suppliers. Management of services provided by suppliers.

A.16 Information security incident management – responsibilities and procedures. Reporting incidents. Reporting security weaknesses. Assessment of events. Response to incidents. Lessons learned. Collection of evidence.

A.17 Business continuity management – aspects of business continuity management. Business continuity management process. Business continuity and risk assessment. Developing and implementing business continuity plans. Business continuity planning framework. Testing, maintaining and reassessing business continuity plans.

A.18 Compliance – compliance with legal requirements. Intellectual property rights. Securing documents. Data protection and privacy of personal information. Prevention of misuse of information processing facilities. Regulation of cryptographic controls. Collection of evidence. Review of security policy and technical compliance. Compliance with security policies. Technical compliance checking. Information system audit controls and tools. Information system audit controls. Protection of information system audit tools.

Nevertheless, it should be remembered that excluding any requirements included under any clause of the standard is not possible if the organization declares compliance with this international standard. Any exclusion of controls considered as required should be justified and evidence should be provided that the associated risks have been accepted by authorized individuals. If exclusions have been made, the compliance with the standard is declared when such exclusions do not affect the organization's ability to ensure information security and the responsibility for doing so.

4. Effects of implementing an information security management systems in transport sector organizations

At the time of implementation, training and audit works, research was conducted with respect to adapting the requirements of the information security management standard in transport industry enterprises. The following results confirm that the implementation of such a system is not easy, nonetheless, it significantly increases the security of information in the organization.

The information security management system having been implemented in transport companies, the awareness of employees and managers with respect to the identification of legal requirements, application of legal and normative requirements in the organization and awareness as to the consequences of disclosure or loss of data, etc. increased significantly.

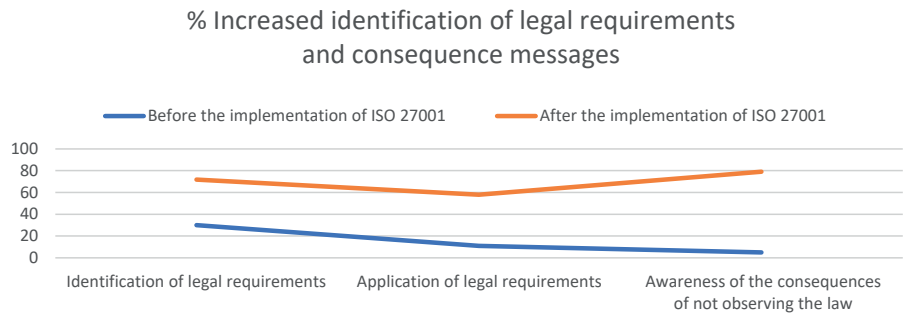

Figure 4. Awareness of legal requirements in organizations before and after implementation of ISO 27001
Source: (own elaboration)

Control over documents and assets having been implemented, the level of documenting transport operations, particularly in respect of documenting the provided information increased significantly and the same applies to the level of documenting actions aimed at controlling the data security system which to a large extent has translated into the employee awareness in respect of the importance and significance of the provided information.

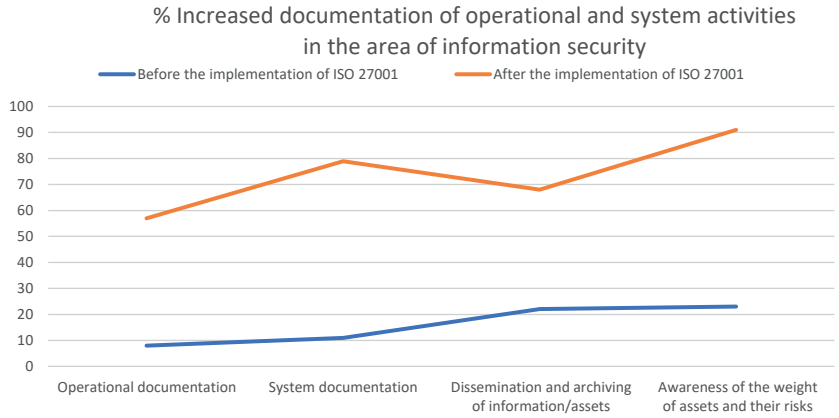

Figure 5. Awareness concerning documenting operational and system activities in the area of information security before and after implementation of ISO 27001
Source: (own elaboration)

Having familiarized themselves with the requirements of the standard, transport entrepreneurs started to pay significant attention to the surrounding risks and established risk identification and documentation methods.

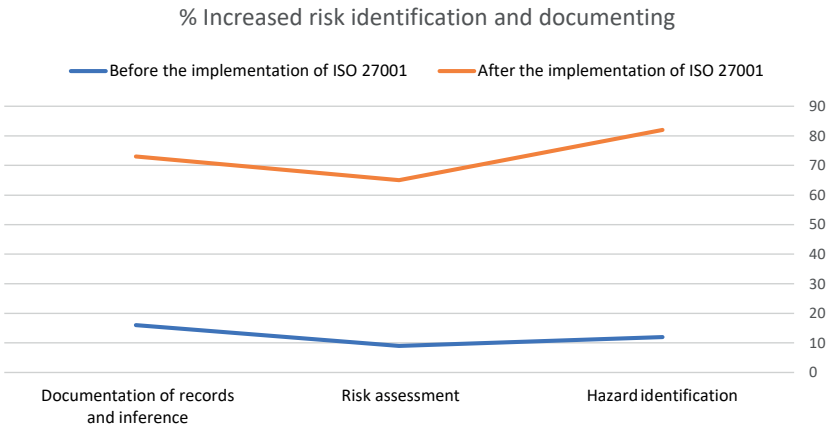

Figure 6. Awareness of risk identification and documentation before and after implementation of ISO 27001
Source: (own elaboration)

Having conducted risk analysis and risk assessment, managers of transport enterprises considerably formalized the rights and responsibilities in respect of information security. Moreover, several time-related and financial outlays were made to build appropriate awareness of employees in respect of information security management system operations.

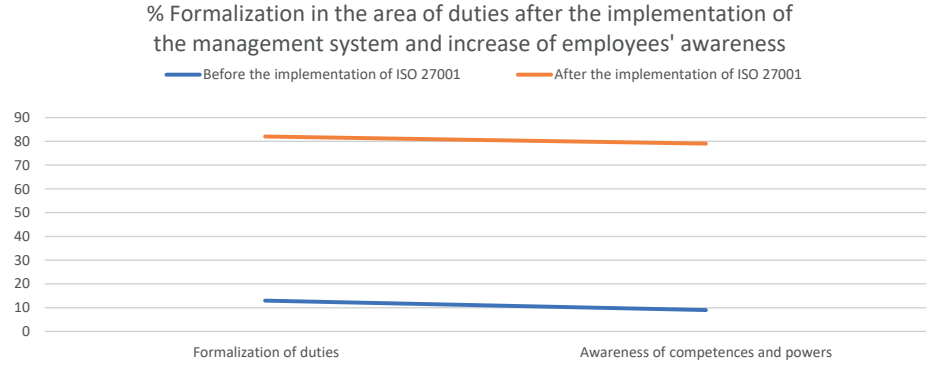

Figure 7. Relation in the area of competence and awareness before and after implementation of ISO 27001
Source: (own elaboration)

When the data control policies had been implemented in transport firms, the identification and recording of data losses or potential data losses increased significantly.

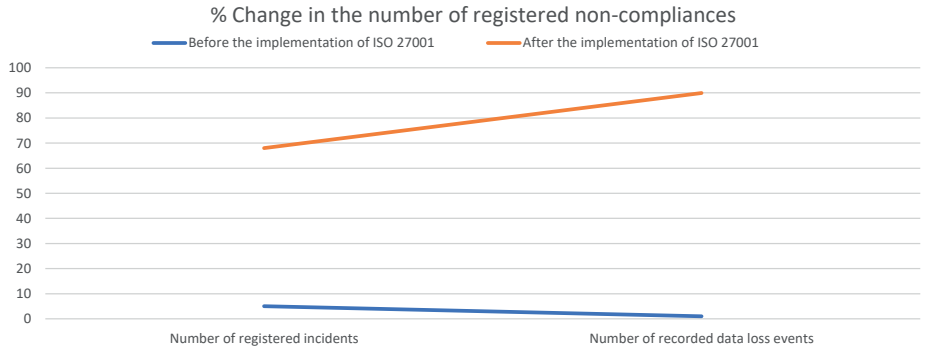

Figure 8. Recording of incidents and data loss events before and after implementation of ISO 27001
Source: (own elaboration)

Before the system was implemented there had been no resource planning activities to secure data in transport companies. It was only when the information security standard requirements had been complied with that planning and predicting financial and other resources to ensure data security started.

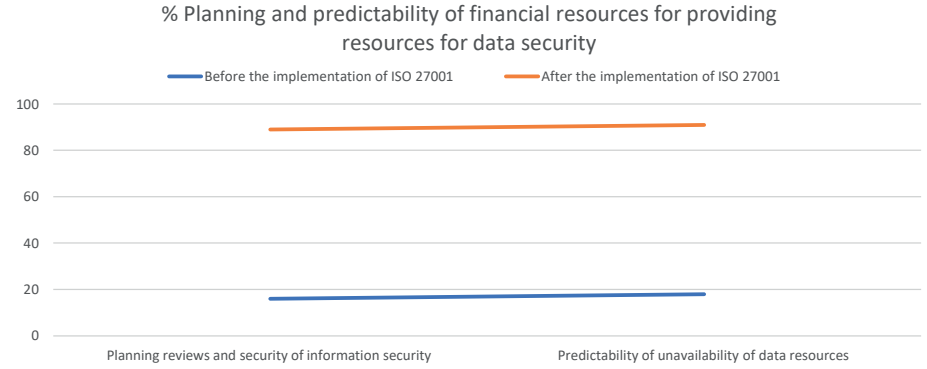

Figure 9. Planning and predicting financial resources for the provision of resources and information security system operation before and after the implementation of ISO 27001
Source: (own elaboration)

Conclusions

Observing the surveyed organizations it can be said that implementing an information security management system changes organizations to a very large extent. The awareness of the importance of data and the willingness to protect it are growing significantly.

Transport enterprises implementing such a system often pinpoint the difficulties in its implementation. The most frequently indicated obstacles include: difficulties in interpreting the requirements of the ISO/IEC 27001:2017 standard, problems in developing a risk assessment model and difficulties in risk management, a vast number of procedures and instructions regulating the data management procedures, the formal system requirements, the expenditures for security which often are not low, high commitment of all the personnel and the specialist knowledge which is lacking in transport enterprises, wherefore it has to be procured and purchased.

Nevertheless, it should be noted that the surveyed enterprises show great appreciation for the implemented system and often emphasize that "it is worth the cost incurred in terms of money and time".

The literature on the subject, the standards supporting ISO 27001 and the practice of transport organizations that have implemented the information security management system show that the implemented system develops the company and strengthens security. Efficient safeguarding of information in the organization by implementing adequate controls prevents information loss. Possible financial and image losses are also reduced by preventing and minimizing the frequency of leakage of confidential information to the outside. Effectively implemented systems prevent breaches of law due to unauthorized use of information and ensure compliance with the legal requirements.

Recapitulating, the aim of implementing and certifying the ISO 27001 system in the transport industry is to give credibility to the organization and improve its image as a secure, reliable and modern business partner, which increases the competitive advantage.

References

Białoń, A., Pawlik, M. (2014), Bezpieczeństwo i ryzyko na przykładzie urządzeń sterowania ruchem kolejowym. *Problemy Kolejnictwa*, 163, p. 27.

BRC Global Standard Food Safety, issue 7, January 2015.

Codex Alimentarius Commission (1997), Food and Agriculture Organization of the United Nations, World Health Organization, Geneva, 23–27 June 1997.

IFS Food Standard for Auditing Quality and Food Safety of Food Products. Version 6.1 (2017), IFS Food, (n.p.).

International Organization for Standardization (2007), Security Management Systems for the Supply Chain – Best Practices for Implementing Supply Chain Security, Assessments and Plans – Requirements and Guidance, ISO 28001:2007.

International Railway Industry Standard of 2005.

ISO Survey 2016 – wzrost certyfikacji systemów zarządzania (2016), https://www.tuv-sud.pl/pl-pl/media-i-prasa/archiwum-aktualnosci/iso-survey-2016-wzrost-certyfikacji-systemow-zarzadzania [Accessed 17 June 2019].

Liczba certyfikacji systemów zarządzania rośnie – wyniki badania ISO Survey 2016 (2017), https://www.sgs.pl/pl-pl/news/2017/10/wyniki-badania-iso-survey-2016 [Accessed 10 June 2019].

PN-EN 50126:2002/AC:2011. Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (2011), Polski Komitet Normalizacyjny, Warszawa.

PN-EN ISO 9000:2015-10. Quality Management Systems – Fundamentals and Vocabulary (2016), Polski Komitet Normalizacyjny, Warszawa.

PN-EN ISO 9001: 2015. Quality Management Systems – Requirements (2016), Polski Komitet Normalizacyjny, Warszawa.
PN-EN ISO/IEC 27001:2017-06. Information Technology – Security Techniques – Information Security Management Systems – Requirements (2018), Polski Komitet Normalizacyjny, Warszawa.
PN-ISO/IEC 27000:2014. Information Technology – Security Techniques – Information Security Management Systems – Review and Terminology (2014), Polski Komitet Normalizacyjny, Warszawa.
Skojett-Larsen, T. (1999), Supply Chain Management: A New Challenge for Researchers and Managers in Logistics. *The International Journal of Logistics Management*, 10(2), pp. 40–42.
The Act on Health Conditions of Food and Nutrition of 11 May 2001, Journal of Laws of 2003, No. 208, item 2020, as amended.

Corresponding author

Natalia Jagodzińska can be contacted at: nj.jagodzinska@wp.pl