RESEARCH JOURNAL OF THE UNIVERSITY OF GDAŃSK

Transport Economics and Logistics Vol. 78 (2018)
http://dx.doi.org/10.26881/etil.2018.78.09

Natalia Jagodzińska

BTCH Management Systems, Gdańsk, Poland

KEY CHANGES TO THE ISO 9001, ISO 14001, ISO 27001 MANAGEMENT STANDARDS IN THE APPROACH TO THE ORGANIZATIONAL CONTEXT INCLUDING RISK MANAGEMENT

Abstract

The aim of the publication is to show new areas required for use in the organization according to the quality management, environmental and information security management systems and to show how the new requirements of the organizational context analysis, inclusive of risk assessment, affect the activities of small and medium-sized enterprises.

Key words: ISO 9001, ISO 14001, ISO 27001, organizational context, risk assessment, ISO standards

Introduction

The standards for management systems described by the ISO standards are amended every 8–10 years on average, in line with the principle of continuous improvement. The last significant amendment was made in 2015. The ISO 9001 quality management, ISO 14001 environmental management, and ISO 27001 information security management systems were extended to include components of analysis of the impacts of the organization' external and internal environment on its operation. Additional requirements for analysing the organization's context, identifying threats and opportunities and risk assessment were adapted to the existing process approach of the ISO standards. These requirements are naturally to be met by large organizations and corporations, as it is companies of such type that base their management mechanisms on documented activities of such type. Nevertheless, micro and small enterprises already have problems with implementing this requirement into their organizational cultures. Although they carry out

threat assessments and environmental analysis as every organization operating on the market, nonetheless, these activities are often conducted on an *ad hoc* or even incidental basis. These are not systemic activities and they are not documented in structures of this type. Hence, the requirements of the 2015 ISO standards are difficult to adopt and document in small and medium-sized enterprises.

1. Evaluation of ISO management systems over last 20 years

The ISO 9001, ISO 14001 and ISO 27001 management standards are formal organizing system, a set of requirements related to the implementation of management systems in enterprises, including but not limited to, management with respect to quality, environment or information security. They unify the approach to systemic management applied by companies of various types. This allows organizations, without any specialized background support, to learn the basic directions of development of quality, environmental and information security systems and gives them the opportunity to develop their own systems. In the eighties of the last century, enterprises in Europe developed rapidly and it became necessary to define unified and universal requirements for the customer-enterprise, enterprise – supplier relations. This need lay at the basis of the development of the British BS 5750 standard adopted in 1979. The British standard was the basis for the development of international requirements contained in the ISO 9000 series of standards adopted in 1987. This standard was changed in 1996 (PN-ISO 9001:1996) which was followed by international editions in 2000 (PN-EN ISO 9001:2001) and 2008 (PN-EN ISO 9001:2009). The currently applicable latest standard is from 2015 (PN-EN ISO 9001:2015-10). The environmental management standard which is originally derived from the Rotterdam Charter prepared in 1991 underwent an analogous history of changes. This Charter was the basis for the development of the ISO 14001 standard for the environmental management system in 1998 (PN-EN ISO 14001:1998). Similarly to the quality standard, the environmental management standard was amended by the ISO in 2004 (PN-EN ISO 14001:2005) and the currently applicable standard was amended in 2015 (PN-EN ISO 14001:2015-09).

The same path was taken by the information security management standard dating back to the British standard BS 7799-1 of 1995, which was a set or a code of practices to be implemented for information security purposes. In Poland, this standard was reflected by the PN-ISO/IEC 1799:2003 and PN-I-07799-2:2005 standards. The key amendment to this standard in 2014 (PN-ISO/IEC 27001:2014-12) in the English version was indeed the basis for the amendments to the quality and environmental standards. It was exactly the information security standard that introduced the requirements for identifying the organizational context as well as opportunities and threats into the ISO 9001 and ISO 14001 standards, thus mobilizing the organization to conduct risk assessment and take actions in respect of business continuity planning. Nonetheless, the currently applicable standard published by the Polish Committee for Standardization originates from 2017 (PN-EN ISO/IEC 27001:2017-06) – however, this is not the date on which the international standard was issued (as the standard is from 2014), but it is the date of the translation into Polish.

2. The idea of amendments to management standards in 2015

It should be noted that the fundamental premises for the quality management, information security and environmental management standards are the following:

- organizing the formal and legal status – compliance or greater likelihood of compliance with the legal requirements;
- better cooperation and relations with the society, the authorities and the inspection bodies;
- increasing the company's competitiveness – a better image of the company in the eyes of potential customers and investors;
- increasing the company's stability and security;
- rational calculation of insurance costs;
- motivating the employees;
- saving time and human effort;
- limiting the impact on the natural environment.

The above premises, implemented over a period of 5 years, in respect of the management standards were based on the following management model – the Deming Cycle.

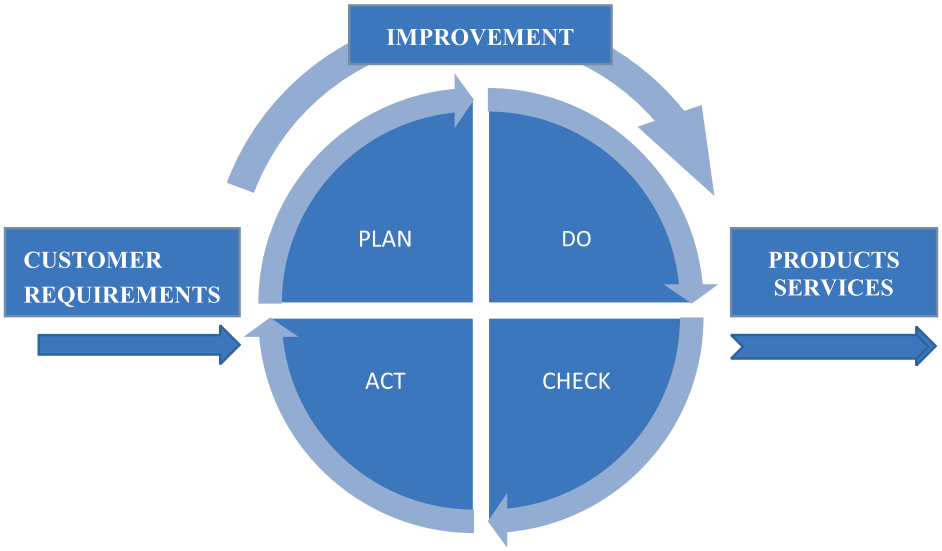

Figure 1. The management system idea: Plan-Do-Check-Act (PDCA) according to PN-EN ISO 9001:2009
Source: (PN-EN ISO 9001:2009 – Quality management systems – Requirements)

The key change in the system management model is placing leaders/managers in the management centre of the organization, and not only at the planning stage as was the case before. Another change is also the indication of additional components affecting the management system, such as the organizational context as well as opportunities and threats. The new management system model according to the arrangements of 2015 is presented in the following diagram.

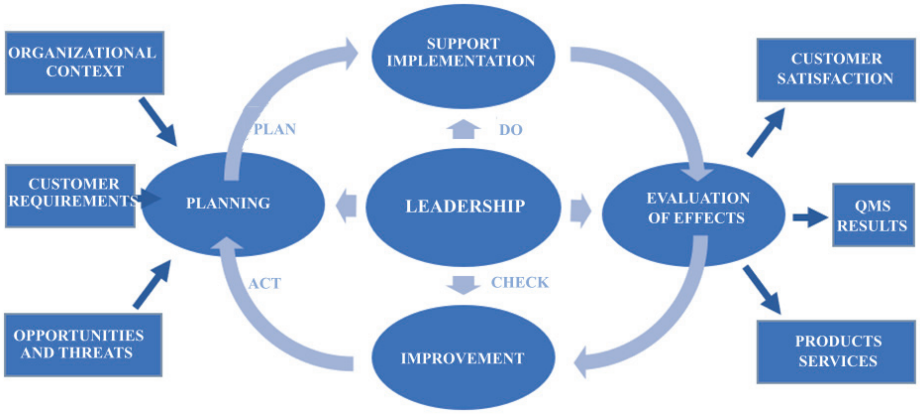

Figure 2. The management system idea according to the new PN-EN ISO 9001:2015-10 standard
Source: (PN-EN ISO 9001:2015-10 – Quality management systems – Requirements)

A fundamental condition to successfully fulfil the requirements of the management system standards is commitment of the top management and the belief that involved leadership is an important factor in the organizational development whereby the organization can well perform the tasks assigned to it. Without this conviction the system can become an unnecessary burden that does not bring the expected results.

3. New requirements for management standards in 2015

Obviously there were more changes to the standards of 2015 that described above. The changes included the method of documenting the functioning of management systems, relations with suppliers and particularly supervision over them, overseeing non-compliant products and requirements regarding auditing. These changes do not significantly affect the functioning of the systems but they are rather more specific for them in terms of details. However, the new requirements in respect of the organizational context and identification of opportunities and threats introduce major changes to the approach to management. Hence, what is currently implemented by large organizations is often a problem for smaller enterprises. Analysis of external and internal strategic factors affecting the organization is not a one-off task following the requirements for the system, but it is a task regularly performed by the management. The organization supervises and checks, on a currents basis, where significant changes occur and ensures that significant changes have resulted from the management system functioning. The tool for such assessment for small organizations it the SWOT analysis. This allows easy assessment of external and internal factors as well as strengths and weaknesses of the organization. In respect of the discussed systems this will concern the quality of products/services, environmental impact and the possibilities of ensuring information security. The stakeholders of the company are all entities that may have requirements and expectations, and thus affect the company.

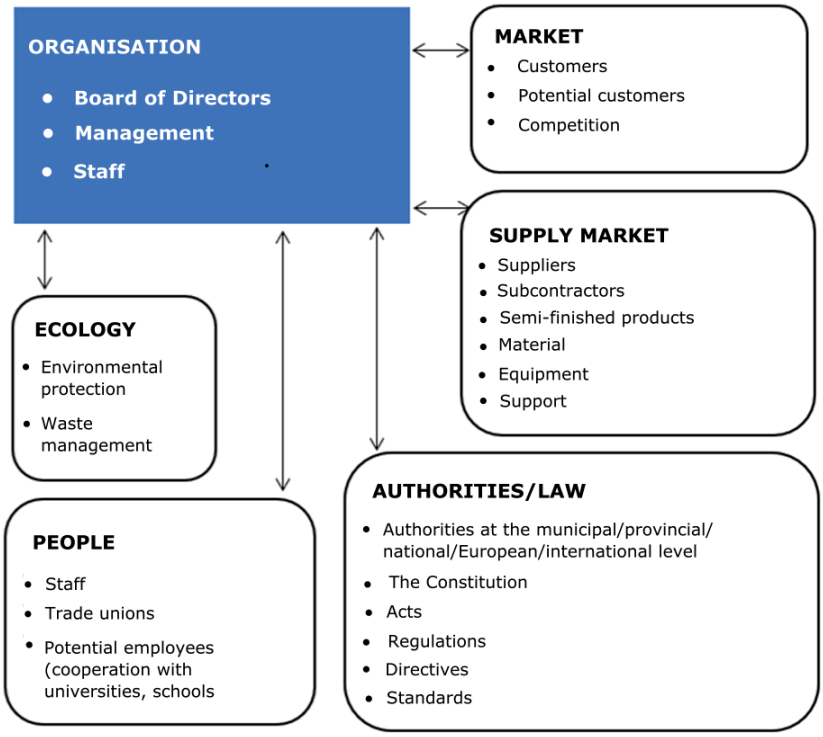

Figure 3. Components of the environment – stakeholders interested in the organization's operations (based on PN-EN ISO 9001:2015-10)
Source: (own elaboration)

The mutual relations between the stakeholders and the organization should be defined for all identified stakeholders in each system. Significant threats and opportunities should be identified for specific elements. The enterprise should assess the risk for each link, by analysing the impact of threats and their possible occurrence. The identified documented risks should be estimated by the organization and then, depending on the criteria, corrective and preventive actions, security measures or established business continuity plans should be introduced. In small enterprises these activities are carried out by teams appointed for this task. The team consists of the owner, his/her assistant or secretary, the contact person for customers, the contact person for suppliers, an accountant and often external advisors such as OHS, IT or environmental experts. The most common result of the brainstorming of this team is a SWOT analysis.

4. Application of new ISO 2015 requirements in small and medium-sized enterprises

Quality, environmental, information security management systems basically have one common idea – to regularly identify threats, assess risks and undertake

preventive and improvement actions. In practice, the introduction of these systems significantly helps small enterprises in their daily operations. The following results were obtained from surveys conducted among micro and small enterprises.

In the area of identification of legal requirements and assessment of their compliance, the requirements stipulated in the standards were the reason why most entrepreneurs have already successfully implemented the already familiar legal requirements in their organizations.

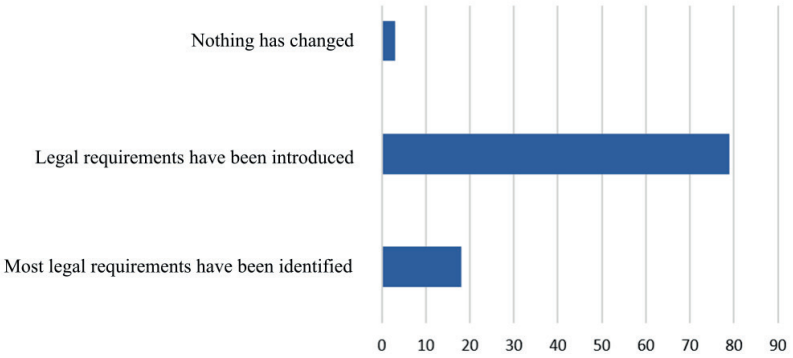

Figure 4. Percentage results of the survey in answer to the question: What has changed in your organization with the obligation to identify the legal requirements?
Source: (own elaboration)

In respect of identification and documenting of threats, small entrepreneurs indicated problems with carrying out these activities because the issue had not been known or used by them so far. The following results were obtained in answer to the question asked about problems in this area.

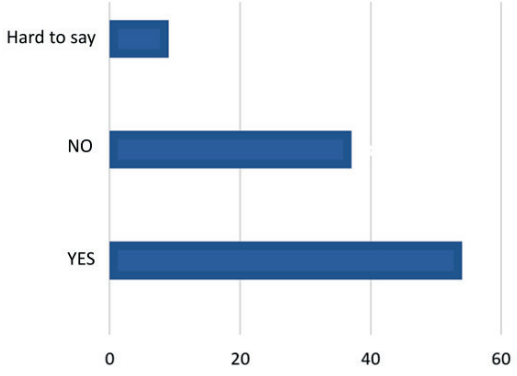

Figure 5. Percentage results of the questionnaire survey in answer to the question: Have you had any problems in identifying threats and documenting them?
Source: (own elaboration)

Importantly, it can be seen that small entrepreneurs are visibly satisfied from the implementation of the risk monitoring tools. It follows from the conducted interviews that the monitoring has given them a sense of control and overseeing, which often escaped them before – which is admitted by them now.

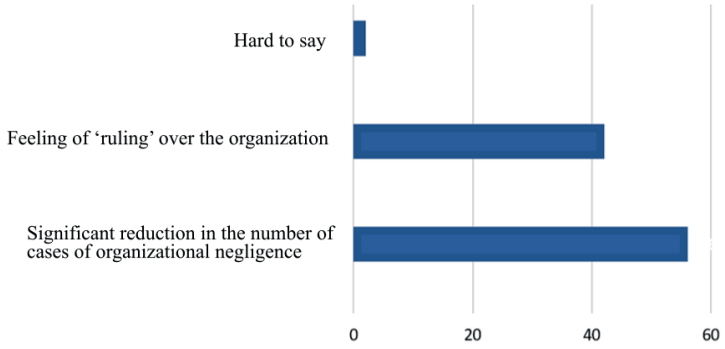

Figure 6. Percentage results of the questionnaire survey in answer to the question: What has been gained by monitoring the risks?
Source: (own elaboration)

The surveyed entrepreneurs also drew attention to the fact that after the implementation of management systems their enterprise is perceived differently on the market. They have obtained the attributes of a 'reliable company', a 'stable enterprise', a 'safe business partner'.

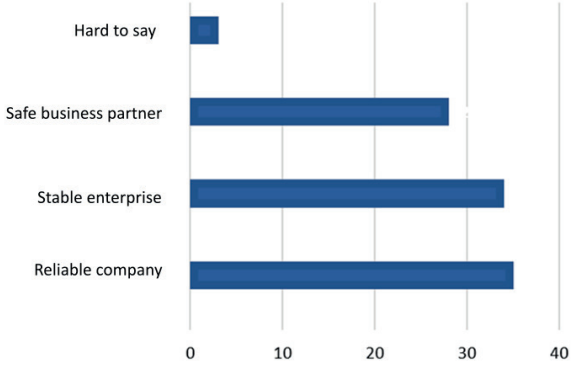

Figure 7. Percentage results of the questionnaire survey in answer to the question: How is the organization perceived by the environment after implementation of management systems?
Source: (own elaboration)

A change in the requirements of the standards is also a change in the way of documenting the system activities. The surveyed enterprises have indicated that 'documented information' in accordance with the new requirements stipulated

in the standard also includes all information currently contained in the IT systems. Such documentation of work has made it possible to discontinue entries in the paper form – which was often an artificial form of documenting activities in the system. This flexibility stipulated in the requirements of the standard and implemented in the enterprise has allowed developing management systems that efficiently monitor and oversee all activities. This has been confirmed by small entrepreneurs in the survey and in the interviews.

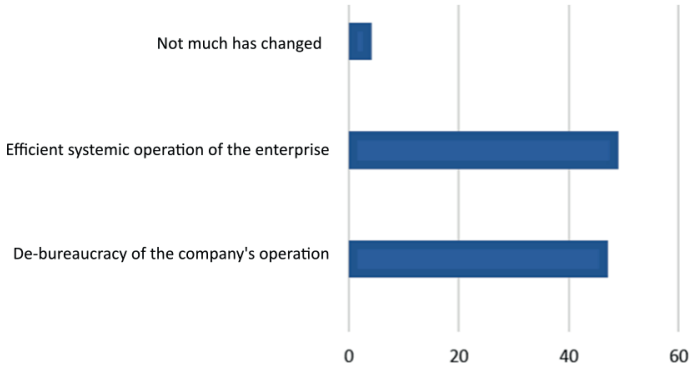

Figure 8. Percentage results of the questionnaire survey in answer to the question: What has changed in your organization after implementation of the new requirements of the 2015 standards?
Source: (own elaboration)

It is also worth noting that the new standards emphasize the HR relations and caring for the employee. The questionnaire survey results clearly show that due to the changes in the 2015 standards, there has been a significantly growing sense of value and safety of employees.

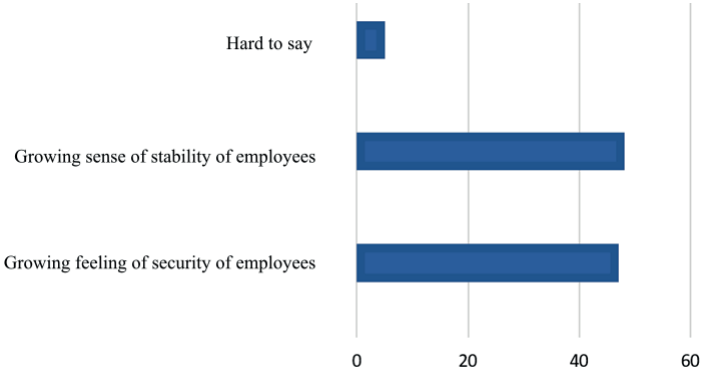

Figure 9. Percentage results of the questionnaire survey in answer to the question: What has changed in your organization after implementation of the new requirements of the 2015 standards?
Source: (own elaboration)

5. Effects of implementing the new ISO 9001, ISO 14001, ISO 27001 requirements in small and medium-sized enterprises

In practice, the introduction of these management systems significantly helps small enterprises to:

- identify the legal requirements, understand them and apply them in the enterprise;
- identify significant (business, security, environmental, quality) threats;
- introduce system solutions for monitoring threats and procedures for responding to threats;
- achieve a stable position on the market and have the organization perceived as safe by third parties;
- organize regular ongoing work;
- give the feeling of value and security to employees.

Most of the small entrepreneurs surveyed indicate that despite problems with understanding and documenting the activities aimed at identifying the environment and the threats, they are satisfied with the path that they have covered. They have realized that superficial analyses conducted 'in mind' are not as objective as risk assessments conducted in a reliable way. Having implemented and certified their management systems, most small entrepreneurs are satisfied with the path which they covered and with the business effects that they have achieved, although, as they emphasize, 'it was not easy'.

Conclusions

In 2015 the requirements of the ISO standards concerning quality, safety and environmental management significantly changed. The process approach was extended to include components of organizational context identification, including external factors and internal factors affecting the functioning of the organization. The component of identification of opportunities and threats, risk estimation and business continuity plans have been introduced to the standards on a permanent basis. The above-mentioned components had been in place in larger organizations for a long time and they had been heavily documented. However, the introduction of these requirements was quite a challenge for the micro and small enterprises sector. It seemed a difficult but not impossible thing to implement. Representatives of small and medium entrepreneurs admit that they had intuitively some of these actions in place, however, they were not systematized. As a result, entrepreneurs from the SME sector have very positively accepted the requirements of the new standards and they have become convinced as to the effectiveness of system management.

References

BS 7799-1 – Code of practice for Information Security Management – a standard code of practice, a catalogue of issues to be implemented for information security purposes

PN-EN ISO 14001:1998 – Environmental management systems – Requirements and guidance for use
PN-EN ISO 14001:2005 – Environmental management systems – Requirements and guidance for use
PN-EN ISO 14001:2015-09 – Environmental management systems – Requirements and guidance for use
PN-EN ISO 9001:2001 – Quality management systems – Requirements
PN-EN ISO 9001:2009 – Quality management systems – Requirements
PN-EN ISO 9001:2015-10 – Quality management systems – Requirements
PN-EN ISO/IEC27001:2017-06 – Information technology – Security techniques – Information security management systems – Requirements
PN-I-07799-2: 2005 – Information security management systems – Part II. Specification and guidelines for use
PN-ISO 9001:1996 – Quality systems – Model for quality assurance in design, development, production, installation and servicing
PN-ISO/IEC 1799:2003 – Information technology. Practical principles of information security management
PN-ISO/IEC 27001:2014-12 – Information technology – Security techniques – Information security management systems – Requirements/English version

Corresponding author

Natalia Jagodzińska can be contacted at: natalia.jagodzinska@outlook.com