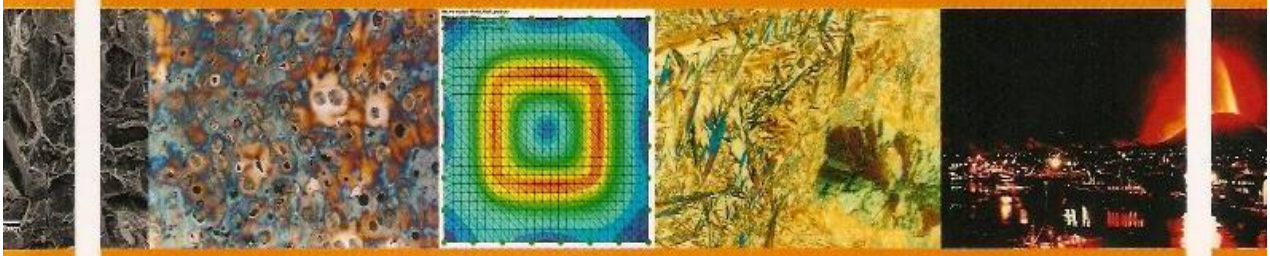
ISSN (1897-3310)

Polish Academy of Sciences
The Katowice Branch
Commission of Foundry Engineering

AFE

ARCHIVES of FOUNDRY ENGINEERING



Published quarterly
as the organ of the Commission of Foundry Engineering

Vol. 10, Special Issue 3 / 2010

Published since 1978 formerly as
Solidification of Metals and Alloys
and
Archiwum Odlewnictwa

ARCHIVES of FOUNDRY ENGINEERING

Published quarterly as the organ of the Foundry Commission of the Polish Academy of Sciences

EDITORIAL ADDRESS
Commission of Foundry, Polish Academy of Sciences
Department of Foundry, Faculty of Mechanical Engineering, Silesian University of Technology
Ul. Towarowa 7, 44-100 Gliwice, Poland
tel. +48 32 338 55 17, fax +48 32 338 55 18, e-mail: kkm@polsl.pl
Abstracts of paper are available at: http://www.odlewnictwo.polsl.pl/Archive.htm

POLISH ACADEMY OF SCIENCES
Commission of Foundry Engineering

ARCHIVES of FOUNDRY ENGINEERING

QUARTERLY

VOLUME 10, SPECIAL ISSUE 3/2010

KATOWICE - GLIWICE 2010

ARCHIVES of FOUNDRY ENGINEERING

ISSN (1897-3310)
Volume 10
Special Issue 3/2010

149 – 152

Published quarterly as the organ of the Foundry Commission of the Polish Academy of Sciences

Risk in Management Systems according to ISO standard

P. Królas [a,*], L. Królas [b]

[a] Politechnika Poznańska – Zakład Zarządzania i Systemów Informatycznych

[b] Ośrodek Kwalifikacji Jakości Wyrobów SIMPTEST w Poznaniu

* Corresponding author. E-mail address: pawel.krolas@gmail.com

Received 30.04.2010; accepted in revised form 30.05.2010

Abstract

The purpose of this article was to present selected management standards in context of risk management. It presents main ISO management standards (ISO 9001, ISO 14001, OHSAS 18001, ISO 27001, BS 25999, ISO 31000) that apply to polish enterprises. In the first part of this article there are analyzed management standards regarding quality, environment, occupational health and safety, information security, as well as business continuity management and risk management. The second part of the article discusses the process of dealing with risk based on chosen management standard.

Keywords: risk, risk management, ISO

1. Introduction

Management systems according to ISO standard apply to polish organizations since the beginning of the 90's. The first publicized and implemented standard was ISO 9001 – Quality management systems. In following years as a result of enterprises' need new standards appeared, such as ISO 14001 – Environmental management systems, British specification OHSAS 18001 – Occupational health and safety management systems (later polish norm PN-N-18001), ISO 27001 – Information security management, as well as trade norms such as ISO 22000 – Food safety management systems and others. Depending on norm's specification individual standards referred in different degree to risk or risk management. The subject of risk appears practically in all norms, risk strictly or in largo sense, regarding applied actions e.g. corrective and preventive actions and management revision.

Due to big verity of norms and enterprises' needs definitions and ranges of risk are ambiguous.

This article presents main management systems according to ISO occurring in polish organizations as well as new tendencies appearing in ISO standards' area.

2. Definition of risk

"New dictionary of polish language" (PWN, Warsaw, 2003) defines risk as "the possibility of failure, loss; and: action that can bring such results [1]".

4-volume "Universal encyclopedia" (PWN, Warsaw, 1987) defines risk as a notion from the law: "(...) in civil law a danger of loss's rising burdening the person directly in harm, unless an agreement or regulation obligates another person to compensate the loss (...); especially responsibility for losses inflicted by the power of nature bases on the risk rule (...). In penal law an action in range of acceptable risk can be a statutory circumstance excluding offender's responsibility [2, 3]".

ISO standards define risk depending on the subject of norm (occupational health and safety, information security etc.). In the

PN-N-18001 norm risk regards "work performed": a probability of occurring of unwelcomed situations concerning the performed job, resulting in losses, especially in adverse health problems caused by occupational dangers in workplace or work performance [4]. PN-N-18002:2000 - Occupational Safety and Hygiene Management Systems – General requirements for occupational risk assessment defines risk as combination of frequency or probability of occurrence causing danger and its consequences [5]. Standard concerning Information Security Management PN-ISO/IEC 27001:2007 – Requirements applying to ISO/IEC Guide 73:2002, where risk is defined as probability of occurrence and its consequences [6]. British standard BS 25999 – "Business Continuity Management. Code of Practice" defines risk as combination of probability of noticed danger/chance and size of its effect on purposes [7]. ISO/FDIS 31000 – Final Draft treats risk as an effect of purposes uncertainty [8].

3. Risk, risk management in ISO systems

The most popular pre-quality system is ISO 9001 standard – Quality management system. The last novelization of ISO 9001 standard in year 2008 did not bring many changes with regard to the shape of norm and approach to risk.

First benchmark of the norm to subject of risk is "Introduction – 01 general regulations" where subpoint a) determines "organizational conditioning, its changes and related risk" which is one of the elements that influence designing and implementing of management system in organization [9]. Second element is "Introduction – 04 compatibility with other systems" which determines lack of "specific requirements for other management systems (...) financial management and risk management" with regard to ISO 9001 norm.

PN-EN ISO 14001:2005 like PN-EN ISO 9001 does not include requirements for risk management. But there is a reference to environmental aspects both in terminology and in standard itself. This norm predicts creating of a procedure concerning environmental aspects (defining environmental aspects in organization and way of their monitoring). In point 4.4.7 this norm defines requirements for a procedure concerning preparedness for accidents that may influence environment. All elements that are directly or indirectly connected to risk (environmental aspects, accidents preparedness) concern environmental elements.

PN-N-18001:2004 concerns Occupational safety and hygiene management system. Similarly to environmental norm (ISO 14001) this standard brings up subject of risk in its terminology (risk definitions, risk assessment, occupational risk). Procedures included in Occupational safety and hygiene management system also concern risk and accident preparedness in context of occupational safety and hygiene (BHP) the same as in ISO 14001 norm in reference to environment. PN-N-18002 defines requirements for occupational risk assessment. Occupational risk assessment methodology contains 3-degree and 5-degree scale. Detailed information about probability and defining harmfulness of consequences are described in point 7.4 "Risk assessment" of this standard [5].

Another standard that is becoming more and more popular in Poland is standard concerning Information security management system by ISO 27001:2005. In contrast to previously described norms it bases on risk management, especially for assets identified in organization. Point 4.2.1 – Establishment of Information security management system defines stages of the system organization which is mostly based on:risk assessment (in context of the kind of business)

- risk assessment (in context of the kind of business)
- risk estimation
- risk analysis and grading
- defying and choosing the way of coping with risk

Detailed information concerning risk assessment in context of Information security management system (ISMS) are described in norm ISO 27005. [12].

In enclosure to described norm there is "Appendage A" regarding purposes of using security as well as security itself. Point 14 of this appendage is "Business continuity management" whose purpose is to define breaks prevention and business activities and protection of critical business processes in enterprise. This point is an "introduction" to British standard regarding Business continuity management – BS 25999.

BS 25999 norm was implemented in 2006 (English version). It consists of good practices regarding business continuity management (part 1) and specification regarding business continuity management (part 2). With reference to previously described standards it can be stated that it brings "new quality" to management systems. Risk in earlier systems concerned mostly specific standard (environment, occupational safety and information security although in smaller degree). This standard treats about ensuring business continuity in whole enterprise which is identified with business. Risks and way of coping with risk which constitute as this standard requirement are suppose to minimize "disturbances" in organization so that losses for business are limited. New concepts that define this standard's terminology: appetite for risk, maximal tolerable period of disturbance and other terms set new challenges for standardization. Although it is a British standard (the same as most of ISO norms implemented in enterprises e.g. ISO 9001, ISO 27001) it can be expected to be converted into ISO standard.

Risk management by ISO 31000 is a new standard publicized in 2009. It aims at minimizing potential losses in organization by implementing risk in various ranges of enterprise's operation (organization's politics, strategy, processes and other elements). Main assumption of this standard regards complex approach to risk and not only to specific elements of enterprise. It is necessary

to analyze the process of risk management to correctly understand the problem of risk.

4. Risk management process

Risk management process covers series of logically following elements. Despite the fact that the risk management process presented in Picture 1 concerns Information security management, it differs only in a small degree from other risk assessment e.g. occupational risk assessment by PN-N-18002 norm.

First element of risk management process concerns setting a context. It is necessary to establish range of analysis, criteria and range of risk assessment. Second stage is to identify risk concerning potential occurrence. Next stage it to estimate risk and potential loss for business which may be caused by breach of safety with reference to confidentiality, integrity and assets' availability. The last element is to apply actions regarding risk management: acceptance, avoidance, transfer and reduction.

Model of risk management differs in reference to various standards. There are though some constant elements that are a base of methodology which is presented in Picture 1.

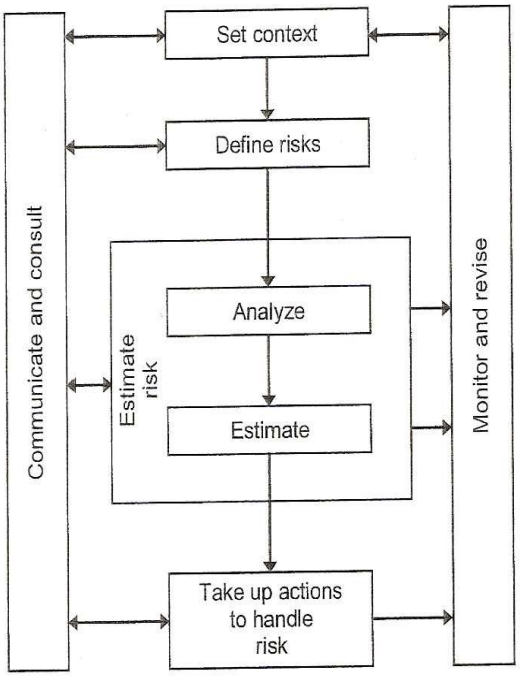


Fig. 1. Managing pisk process.
Source: ISO/IEC 27005 norm

5. Summary

Management standards by ISO systems exist in Poland from the 90's. An approach to pro-quality system changes along with changes in organizations. First novelization of norms ISO 9000 series took place in 1994 when interpretation and application problems were removed with maintain of norm's shape. Another change in 2000 contributed to implementing of process approach, which was a big challenge for enterprises, consulting companies and certifying companies [10]. Novelization proposed in 2008 did not implement any significant changes to this standard.

In conclusion, modern organizations expect solutions adapted to our times. Important problems from organization's point of view are: increase of information quantity, the need to optimize processes, business continuity management, risk assessment. Continuing development forces constant improvement of services offered by organizations in free market economy as well as of management standards.

Literature

[1] (---);Nowy słownik języka polskiego, PWN Warszawa 2003.

[2] (---);Encyklopedia powszechna, PWN Warszawa 1987.

[3] K. Liderman, Analiza Ryzyka i ochrona informacji w systemach komputerowych, Wydawnictwo Naukowe PWN, Warszawa 2008 .

[4] PN–N–18001:2004 – System Zarządzania Bezpieczeństwem i Higieną Pracy –Wymagania.

[5] PN–N–18002:2000 – Systemy zarządzania bezpieczeństwem i higieną pracy – Ogólne wytyczne do oceny ryzyka zawodowego.

[6] ISO/IEC Guide 73:2002 – Risk management – Vocabulary – Guidelines for use in standards.

[7] BS 25999:2006 – System Zarządzania Ciągłością Działania.

[8] ISO / FDIS 31000 – Final Draft – Zarządzanie Ryzykiem.

[9] PN-EN ISO 9001:2009 – System Zarządzania Jakością – Wymagania.

[10] PN-ISO/IEC 27001:2007 – System Zarządzania Bezpieczeństwem Informacji – Wymagania.

[11] W. Sokołowicz, A. Srzednicki, ISO – Systemy zarządzania jakością oraz inne systemy oparte na normach", Wydawnictwo C.H. Beck, Warszawa 2006.

[12] PN–ISO/IEC 27005:2010 - Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji.

Archives of Foundry Engineering continues the publishing activity started by Foundry Commission of Polish Academy of Sciences (PAN) in Katowice in 1978. The initiator of this action was the first Chairman Professor Dr Eng. Waclaw Sakwa - Corresponding Member of PAN, Holder of the Honorary Doctorate of Czestochowa University of Technology and Silesian University of Technology, President of CIATF. This periodical, previously entitled **"Solidification of Metals and Alloys"**, enabled publication of results achieved in the field of the Basic Problems Research Cooperation. The thematic scope was related to periodical title and concerned widely understand problems of metals and alloys crystallization in a casting mould. Within 1978-2000 the 44 issues have been published. Since 2001 the Foundry Commission has had patronage of the annually published **"Archives of Foundry"** and since 2007 quarterly published **"Archiwum Odlewnictwa"**. Periodical thematic scope includes scientific issues of foundry industry:

Theoretical Aspects of Casting Processes,

Innovative Foundry Technologies and Materials,

Cast Alloys Design,

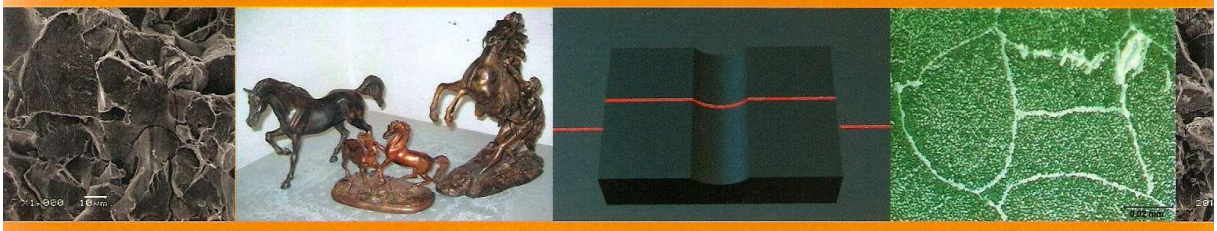
Computer Aided Foundry Processes ,

Mechanization, Automation and Robotics in Foundry,

Transport Systems in Foundry,

Castings Quality Management,

Environment Protection.



ISSN (1897-3310)