COMMUNICATIONS IN DEPENDABILITY AND QUALITY MANAGEMENT An International Journal

Volume 15, Number 2, June 2012 ISSN 1450-7196

Published by
The Research Center of Dependability and Quality Management
P.O. Box 132, 32102 Cacak, Serbia
www.dqmcenter.com

AIMS AND SCOPE

Communications in Dependability and Quality Management (CDQM) is an International Journal published by the Research Center of Dependability and Quality Management (DQM Research Center), Cacak, Serbia. This well-established, high-quality specialized scientific and technical journal is devoted to research, development, manufacturing and using modern and complicated systems.

This interdisciplinary journal considers papers with both theoretical and practical aspects on dependability management and life span, configuration management and quality management, safety and environmental protection, project management and production management. It is dedicated to researchers and practitioners who work in: design, production control, quality assurance, maintenance, simulation, computing, software, electronics, mechanics, aerospace, power systems, nuclear systems, communication systems, mechatronic systems and similar areas.

FUNCTIONAL AREAS

All submitted papers are reviewed by selected referees, all of whom are recognized experts in their fields. Acceptance of articles is the responsibility of the editorial board. The journal is published not less of twice a year.

Examples of subject areas of Dependability Management Life Span include:

- Life Cycle Cost Analysis
- Design to Cost
- System Performance
- Dependability
- Reliability
- Systems Effectiveness
- Robustness and Survivability
- Compatibility, Simplicity, Commonality and Friendliness
- Availability
- Maintainability and Testability
- Integrated Logistic Support (ILS)
- Failure Analysis
- Adaptability and Life Span

Examples of subject areas of Configuration Management and Quality Management include:

- Configuration Management
- Configuration Control
- Quality Management (including TQM)
- Quality of Design (Value Engineering-VE, Quality Function Deployment-QFD, etc.)
- Benchmarking
- Design of Experiments
- Taguchi Methods
- Quality Assurance (QA)
- Quality Control (QC)
- Economic Aspects of Quality

Examples of subject areas of Safety and Environmental Protection include:

- Diagnostics of Processes
- Hazard Analysis Techniques
- Work Physiology
- Safety Systems
- Risk Analysis and Contingency Planning
- Economic Aspects of Safety
- Industrial Health
- Toxicology
- Radiation
- Pollution Engineering
- Product Stewardship and Materials Recycling

Examples of subject areas of Project Management and Production Management include:

- Network Models' Structure
- Project Scheduling
- Cost Optimization
- PERT-Cost Models
- Resource Levelling
- Resource Supportability Models
- Stochastic Projects
- On-Line Control
- Computer Integrated Manufacturing (CIM)
- Production Planning and Control (including Production Scheduling)
- Controlling Hierarchical Production Systems
- Flexible Manufacturing Systems (FMS)
- Planning Under Uncertainty
- Concurrent Engineering

COMMUNICATIONS IN DEPENDABILITY AND QUALITY MANAGEMENT

An International Journal

Special Guest Issue

Human Resource Management

Volume 15, Number 2, June 2012 **ISSN 1450-7196**

CONTENTS

COMMUNICATIONS
IN
DEPENDABILITY AND
QUALITY
MANAGEMENT
An International Journal

CDQM, Volume 15, Number 2, 2012, pp. 29-40

UDC 005.334 ; 005.95/.96

Risk Management as the Basis for Human Resources Safety Management

Zdenko Adelsberger[1], Ivan Nadj[2] and Kresimir Buntak[3]

[1] *Bluefield d.o.o., Zagreb, Croatia*
E-Mail: zadelsbe@zg.t-com.hr
[2] *Zastita - Zagreb d.d., Zagreb, Croatia*
E-Mail: ivan.nadj@zg.t-com.hr
[3] *Polytechnic of Varazdin, Varazdin, Croatia*
E-Mail: kresimir.buntak@inet.hr

accepted May 2, 2012

Summary
Not only does human resources safety represent a human and business necessity, it is a legal requirement for all business entities. The method of approach to the implementation of activities related to human resources safety is based on the assessment of risk in accordance with the legislation and the international standards. However, the proactive human resources safety management requires more than just risk assessment, it requires comprehensive risk management. This paper presents a critical analysis of the risk assessment based on OHSAS 18001 and risk management based on ISO 31000. The paper also proposes an organizational approach to human resources safety management within the integrated safety management process of a company..

Key words: *Human resources, safety, risk management.*

1. INTRODUCTION

Within each organizational form, functions and activities are performed through one or more business processes, regardless of the business type. Having said this, one should also consider that technological processes are sub-processes of one or more business processes.

Management of these business processes is performed through formalized or non-formalized management systems. In the context of the theme of this paper, the difference between formalized and non-formalized management systems is that the formalized management systems are implemented in the manner of generally accepted rules and standards, which also ought to have a formal certificate of such established management system. The best known formal management

systems are based on ISO standards, such as ISO 9001 (Quality Management System), ISO 14001 (Environmental Management System), OHSAS 18001 (Occupational Health and Safety Advisory Services), ISO 22000 (Food Safety Management System), ISO/IEC 27001 (Information Security Management System), ISO 31000 (Risk Management System) etc. There is a number of other ISO standards which deal with management systems in various other (specialized) fields. What all these formal management systems based on ISO standards have in common is that they define each management system as a process.

The basic standard for all management systems from the ISO standard family, ISO 9001, defines the process as a documented group of activities which take the entry requests and turn them into meeting these requests with the help of resources and rules. Figure 1 portrays the business process scheme.

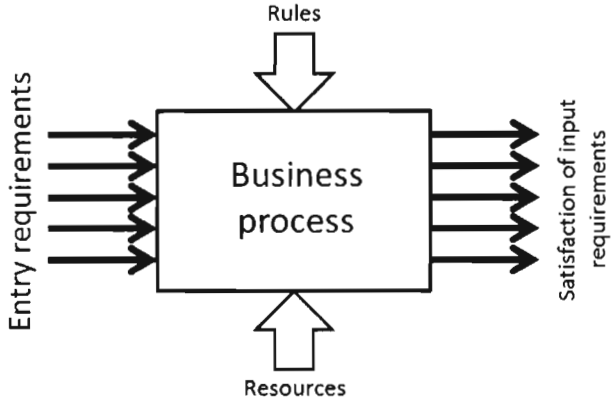

Figure 1. Business process scheme
Source: own source

In accordance with the aforesaid, each management system is in fact one process. ISO 9001, for example, defines a group of requirements which must be met in order to complete the formal quality management system, and ISO/IEC 27001 is a standard which defines a group of requirements that must be met in order to complete the formal information security management process, etc. The accent is on "must". This means that all defined requirements in a standard must be met if one desires to obtain the independent certificate from an accredited certification institution. Having said this, one should have in mind that all the stated standards only define which requirements must be met in order to obtain the certificate, but none of the standards specifies the manner in which these requirements must be met, meaning that each organization meets these requirements in its own way, in accordance with its abilities and needs.

The analysis of any of the above mentioned standards may point out that within resources each of them places a special accent on human resources, i.e. by its definition each standard considers human resources to be one of the key resources for establishing and the functioning of any business process.

If a more detailed analysis of the business process portrayed in Figure 1. is done, it can easily be shown that entrances and exits of the business process are processes themselves, as portrayed in Figure 2.

If the attention is directed solely on the resource management process, it may be show that it consists of a number of other sub-processes, such as assets management, inventory management, reserves management, energy management, etc., but in this context, human resources management

is especially accented. This brings us to an irrefutable fact that the human resources management sub-process is of inevitable, most often fundamental significance to the functioning of any business process. The comparison of all these business processes within an organization may indicate that human resources are a must in each business process, whereas this is not the case with other types of resources.

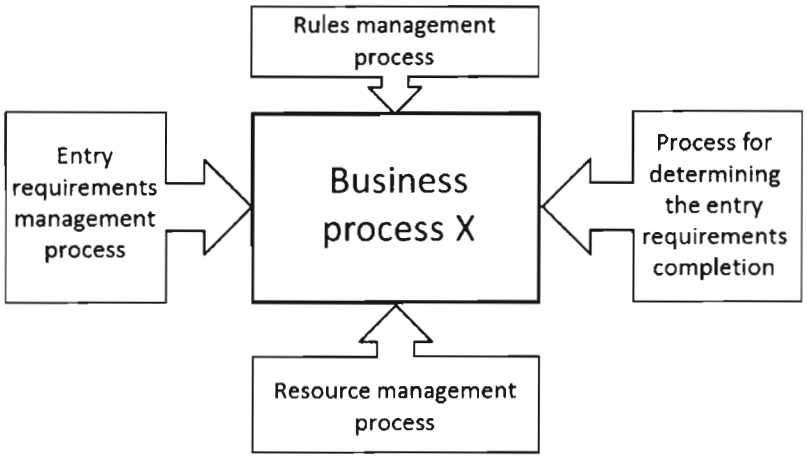

Figure 2. Process scheme in interaction with other processes
Source: own source

Since each organization operates, i.e. its processes take place, in conditions of lesser or greater entropy, this results in business process objectives, and with it the business policies of an organization to be realized in an unsafe environment. If the business policies, i.e. if the business policy objectives present a premise which needs to be secured, than the insecurity management of the environment in which the business processes are taking place, as well as their relative sub-processes, are one of the key requirements for survival and advancement of business. Today, the only manner to manage safety and thus decrease business entropy is to manage risk on all levels, from strategic, through business and operational, to process risk.

All of the above stated show that the human resources risk management is one of extremely significant management systems which significantly contributes to general business stability, and as such should be formalized.

2. RISK MANAGEMENT PROCESS

The standard ISO 31000:2009 defines the risk management process and is a part of a group of guidelines, i.e. non-mandatory application standards. This means that none of the organizations undertake to apply the ISO 31000 standard or any of its derivatives in the certification procedures for any of the management systems. However, since the risk management process generically described in ISO 31000 is the result of long-term experience derived from the national standard AS/NZ 4360, accepted worldwide, it is highly unlikely that someone should decide to independently build a risk management process which is not in accordance with ISO 31000. The application of ISO 31000 is absolutely recommended and practically mandatory everywhere where risk management is desired, especially when dealing with the implementation of one or more management systems based on ISO standards.

ISO 31000 is intended for organizations of all types and sizes which face a number of risks that may have adverse effects on the realization of their objectives defined by their business policies.

These objectives may include a wide spectrum of organizational activities, from strategic initiatives to its operations, processes and projects, and are reflected in the strategic, business, financial results and influences, as well as good reputation. It has already been shown that activities of an organization also include risks. Risk management assists in decision making, as it takes into consideration the uncertainty and influence that the uncertainty has on objective realization and the assessment of necessity to undertake certain actions. The correct application of ISO 31000 requires the use of ISO Guide 73, the terms of reference related to risk management issues. In accordance with ISO Guide 73, the risk is defined as the effect of uncertainty on objectives. Effect is considered to be a deviation from the expected – positive and/or negative. Risk is often characterized by the connection to potential events or consequences, or the combination of the two. The simplified physical principle of risk manifestation is shown in Figure 3 and the significance of individual dimensions in Table 1.

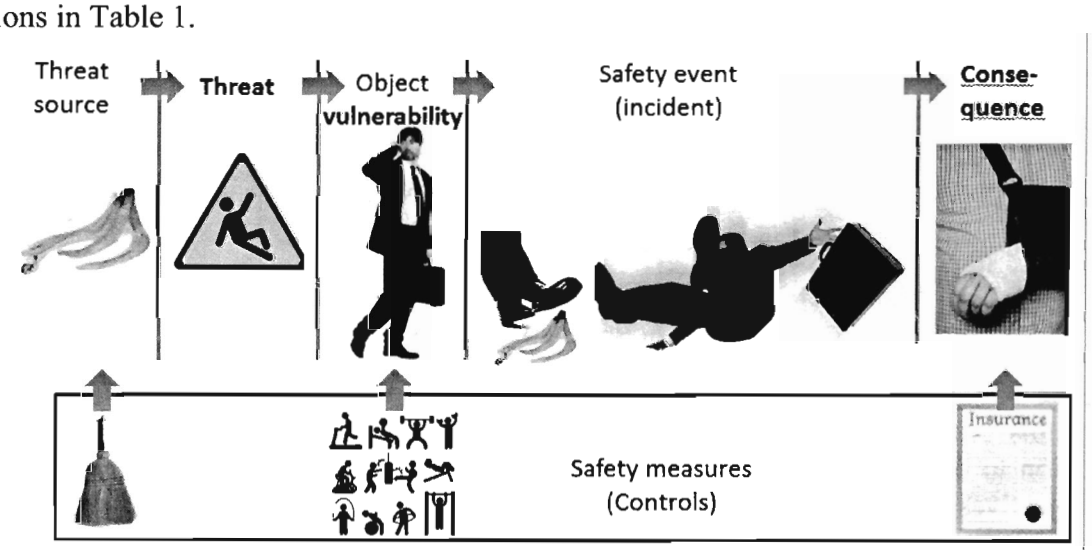

Figure 3. Simplified physical risk manifestation principle scheme
Source: own source

Table 1. Significance of individual values in Figure 3

Threat	Possible source of unwanted incident which may cause damage to the system or the organization
Vulnerability	Vulnerability of an asset or a group of assets which may be used by one or more threats.
Consequence	The result or effect of an event Note 1: There might be one or more consequences of an event. Note 2: The consequences may range from positive to negative. Note 3: The consequences may be expressed qualitatively or quantitatively. Note 4: The consequences are considered in relation to the realization of objectives.
Safety measure (Control)	risk management means including policies, procedures, guidelines, practices or organizational structures which may be of administrative, technical, managing or legislative nature. Note: Control is also used as the synonym for protection or counter measures.
Safety event (Incident)	the safety event or the incident is a recognizable case of system state which directs to the possible infringement of safety policies or a protection failure or until that moment unknown circumstances which may be important to safety.

Source: own source

It is necessary to stress that the situation in Figure 3 makes sense only in the event that the source of the threat generates the threat which the object is vulnerable to and that they act mutually, i.e. if the threat uses the vulnerability and leads to the consequence.

ISO 31000 completely identifies the risk management principles, defines the risk management framework, and finally the risk management process. The mutual relationship of these elements is shown in Figure 4.

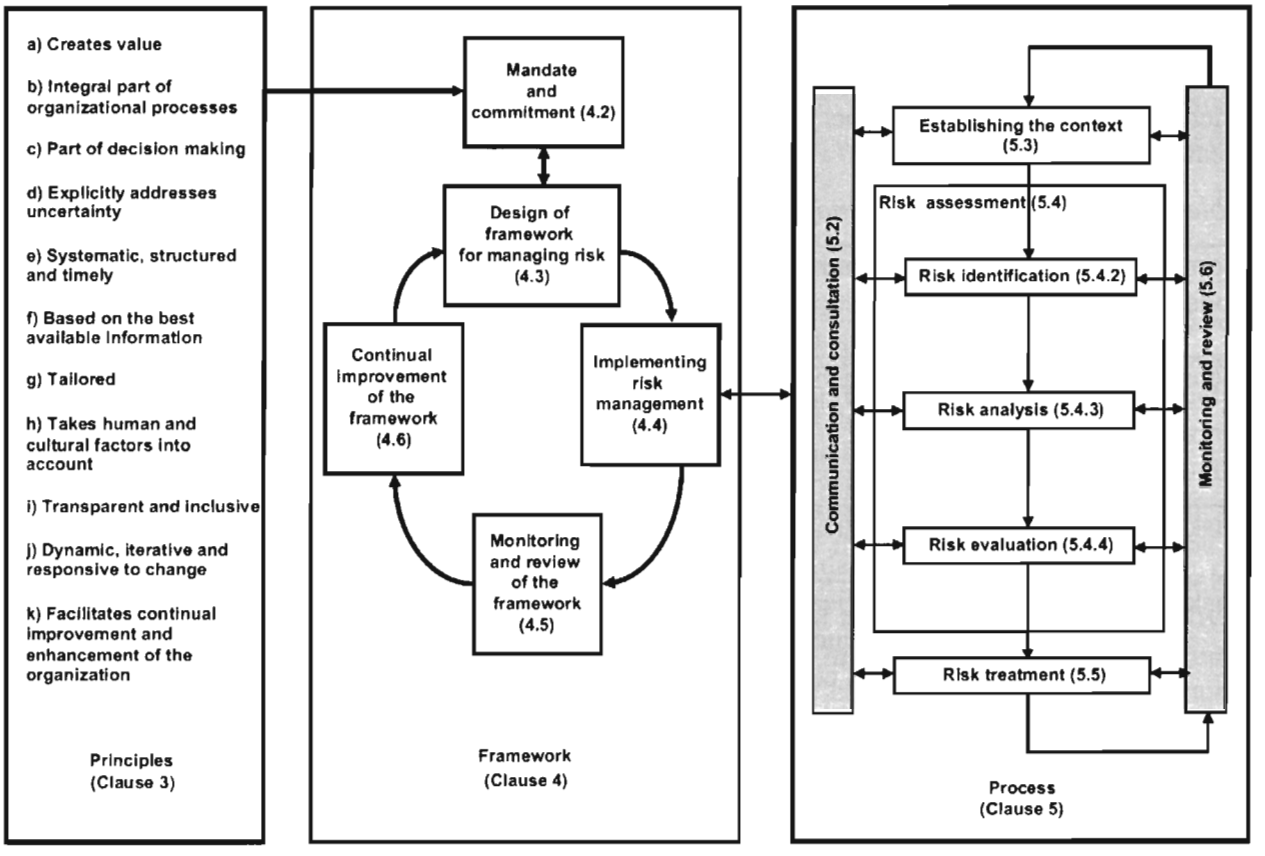

Figure 4. Scheme of ISO 31000:2009 elements
Source: ISO 31000:2009

Of all the stated risk management principles that are shown in Figure 4, the fact that risk management creates value draws special attention, i.e. in the final annual business balance risk management makes its contribution to creating extra value. The risk management framework shows that upon the decision of the top management to start with the systematic risk management, based on this decision authorizations are defined and support is formally given to the implementation project, and later also to carrying out the risk management process. The entire risk management process takes place according to the PDCA circle (4.3, 4.4, 4.5, 4.6). The risk management process shown in Figure 3 is relatively complex, and the most critical part of the entire process is the risk management phase. The significance of individual risk management process elements is shown in Table 2.

The importance of the risk evaluation phase is reflected in a selected method used to implement the evaluation. In practice, the qualitative method is acceptable for the purposes of the management system and the human resources risk assessment. This method of risk assessment has several faults, but the most significant are the subjectivity of the assessment which is conditioned by the

insufficient exactness of the values which are used to calculate (estimate) the risk. Depending on the selection of elements used to assess the risk, a number of formulas for calculation, i.e. risk validation may be defined. If limited to the above stated, that the risk assessment is conducted based on three stated factors, the most common mathematical form of risk validation is expressed as follows:

Risk = Threat * Vulnerability * Consequence (1)

or

Risk = Probability * Consequence. (2)

Where the probability represents the measure of incident manifestation, implicitly containing the threat and vulnerability within.

Table 2. Significance of risk management process elements

Communication and consulting	Communication and consulting with internal and external investors – interesting parties, as it is fitting, in every level of the risk management process and consideration of the process as a whole.
Determining context	Establishing external, internal and the context of risk management wherein the rest of the process will take place. It is necessary to establish criteria according to which the risk will be evaluated and the analysis structure shall be defined.
Risk identification	Identification of where, when, why and how events might prevent, diminish, defer or increase the accomplishment of objectives.
Risk analysis	Identification and evaluation of existing controls. Determining consequences and probabilities followed by the risk level. This analysis should consider the field of potential consequences and how they might manifest.
Risk evaluation	The comparison of evaluated risk levels with previously determined criteria and consideration for the balance between the potential benefits and unfavorable results. This provides for decision making regarding the volume and nature of necessary analyses and priorities.
Risk processing	The making and the application of specific cost effective strategies and action plans for increasing potential benefits and decreasing potential costs.
Monitoring and Re-evaluation	It is necessary to monitor the efficiency of all risk management process steps. This is important for continuous improvement. It is necessary to monitor risks and efficiency of analysis measures in order to ensure that the change in conditions does not result in the change of priorities.

Source: own source

The risk validation according to expressions (1) or (2) is realized by defining scales which descriptively define the levels of individual parameters, such as the threat assessment scale, vulnerability assessment scale, consequence assessment scale and in case of expression (2) the scale of probability assessment. Each descriptive value is assigned a numeric value which is then used in the said expressions. The values in individual scales range between 1-3, or 1-5, or 1-7, etc. It is better to use larger scales for greater precision, but that presents a problem of how to define each level so that a value might be unanimously selected. For example, it is easier to make descriptions which will define the significance of a threat within boundaries of 1-3, than it is within boundaries of 1-7.

This approach to risk assessment, i.e. risk management in an organization is flexible enough and acceptable for almost all types of risk, including the human resources risks.

Speaking of safety in general, one can say that the safety is complementary to risk, i.e. greater the risk of objective realization, lower the realization safety. The correlation between the safety and the risk may be expressed as follows:

$$\text{Safety} = 1 - \text{Risk} \quad (3)$$

Note: the risk must be expressed in a relative value, from 0-1.

This may lead to the conclusion that the approach to human resources management issue is equivalent to the human resources management approach and the correlation is determined by expression (3).

3. HUMAN RESOURCES SAFETY (RISKS)

The analysis of ISO standards meant for establishing and certifying management systems shows that only the Annex A to ISO 27001:2005 speaks more of this issue. All other ISO standards accent the importance of human resources but do not continue to elaborate further. However, the analysis of requirements related to human resources within ISO 27001:2005 shows that it can all be applied to any management system and not only the information security management system. It is therefore logical to take the characteristics of human resources safety management as shown in ISO 27001 as a universal approach in an organization, regardless of the management system type. To compare, OHSAS 18001 speaks of a relatively narrow aspect of human resources safety, only in relation to the possible adversity of a job and the preservation of the life and health of employees. National work protection laws have the same area of interest. On the practical side of the human resources safety analysis this is insufficient as the mentioned cased say nothing of the human resources safety related to the regular (planned) carrying out of business processes. It is one more reason to apply the holistic approach to the human resources safety management, taking into consideration OHSAS 18001, national work protection laws and approaches shown in ISO 27001:2005.

It needs to be said that the mentioned Annex A to ISO 27001:2005 includes a text, the contents of which are directed towards the information safety issues. However, if this text is somewhat generalized it provides the content which is applicable to all management systems. Further in this paper we will show modified texts of the Annex A, which may be applied to all cases.

According to Annex A of ISO 27001:2005 there are three safety objectives which must be achieved. These safety objectives are defined for the period before employment, after employment and after the employment has ended. Table 3 shows safety objectives and their modification for general application.

According to Table 3, it is visible that the settings in Annex A to ISO 27001:2005 related to human resources safety are in fact universal and significant for all management systems and not only for ISMS. Only the text of the human resources safety monitoring modified for general application shall therefore be shown further on.

According to the Annex A, three safety measures (controls) are provided for the realization of each of the three safety objectives, as shown in Table 4.

Table 3. Safety objectives for human resources safety

Application period	Safety objectives	
	According to ISO 27001:2005 (A.8)	Universal application
Before employment	Provide the employees, contracted associates and third parties with the understanding of their responsibilities, check their suitability for the task that is meant for them and decrease the risk of theft, fraud or abuse	Provide the employees, contracted associates and third parties with the understanding of their responsibilities, check their suitability for the task that is meant for them and decrease the risk of theft, fraud or abuse
During employment	Provide the employees, contracted associates and third parties with the understanding of threats to **information** security, their responsibilities and obligations and how to equip them for support to the **safety** policy of their organization during their normal work and lower the risk of human error.	Provide the employees, contracted associates and third parties with the understanding of threats to **business** security, their responsibilities and obligations and how to equip them for support to the **business** policies of their organization during their normal work and lower the risk of human error.
Termination or change of employment	Ensure that the employees, contracted associates and third party beneficiaries may properly leave the organization or change their job.	Ensure that the employees, contracted associates and third party beneficiaries may properly leave the organization or change their job.

Source: own source

In the event that upon the identification of a significant human resources risk (according to the safety policy of unacceptable level) a decision is brought to lower the said risk, it is necessary to select one of the offered objectives for lowering risks. After having selected the objective which is aimed to be achieved by lowering the said risk, it is necessary to select one or more safety measures (controls) which serve to achieve such objective. It is also necessary to make a Cost Benefit Analysis in order to verify the justification behind the implementation of such measure in relation to the potential damages caused by the consequences, as well as the possible legal obligation of such implementation. To illustrate, Table 5 shows an example of some activities related to human resources and some of the potential risks and threats for the said activities.

Within the organization and the implementation of risk management for the purposes of human resources, a question is posed on how to formally implement this in an organization. There is, of course, no regulation, nor does ISO 31000 say anything about it. This falls into the domain of internal organization, firstly depending on its size and dedication of the management to the risk management issues. Human resources risk management organization is, in any case, a part of general risk management within the organization and should be observed as such. In case of small companies this problem is mainly approached with less organization and resources of the risk management system. However, for medium and larger (large) organizations, the issue of risk management and, in that context, the position of human resources risk management is a strategic issue. The issue of risk management within an organization must be properly treated and supported by the organizational structure in all management and decision making levels, as well as implementation of business activities. For illustration purposes, Figure 5 shows one of the possible organization forms and implementation of risk management system. In a concrete case, the organization adjusts to the needs and wishes of the management, but the example is illustrative enough to be able to demonstrate all the complexities of the risk management organization within a company.

Table 4. Safety measures (controls) for human resources safety objectives

	Safety objectives		
	Before employment	**During employment**	**Termination or change**
Safety measures (controls)	**Functions and responsibilities** It is necessary to determine and document business functions and responsibilities of employees, contracted associates and third parties in accordance with the business policies of the organization.	**Management responsibilities** Management should demand that the activities of its employees, contracted associates and third party beneficiaries be in accordance with the existing policies and procedures of the organization.	**Termination responsibilities** The responsibilities for termination or change of employment must be clearly determined and assigned.
	Selection of candidates It is necessary to check out all candidates for the job, contracted associated and third party beneficiaries in accordance with the valid laws, regulations and ethics, in accordance with the requirements of the tasks that will be performed and possible risks.	**Business policies, education and training awareness level** All employees within the organization, and if there are any, contracted associates and third party beneficiaries should participate in appropriate training for the purposes of raising the awareness level and regular information regarding the policies and procedures of the organization, which regards their business function.	**Return of assets** After their employment, contract or agreement has ended, all employees, contracted associates and third party beneficiaries must return all assets that the organization provided them with.
	Employment duration and conditions As a part of their contractual obligation, employees, contracted associates and third party beneficiaries should agree on and sign the document with the duration and terms of the employment contract, which must state their responsibilities and the responsibilities of the organization regarding the task performance.	**Disciplinary process** There should be a formal disciplinary process for employees who endangered the business activities planned by policies and procedures.	**Access rights termination** The right of access of all employees, contracted associates and third party beneficiaries to information and business equipment should be terminated with the end of employment, contract or agreement or should be adjusted to the changes.

Source: own source

Table 5. Examples of some human resources activities related to risk analysis

People Activities	Potential Risk	Potential Reasons (Threat Sources)
Employment	• Discriminatory practices • Hiring an inappropriate or uncertain candidate • "Unjust" employment	• Incomplete check of potential candidates • Not taking local and national laws related to human rights into consideration • No trial period • Making unrealistic promises to candidates • Not signing an Employment Contract and the Statement on Respecting Business Policies
Labor protection and work safety	• Ecology • Physical injuries and death	• Uncertain working conditions and not implementing regular safety checks? • Not implementing appropriate staff training • Not using appropriate clothing and safety equipment? • Non-existence of adequate policies and procedures
Employee Supervision	• Insulting and molesting (mobbing) • Reputation within the community • Revealing personal information	• No clearly written authorizations and descriptions of jobs • Parameters of job descriptions are not respected • There is no employee manual • There is no organized constant training regarding the business policies and actions • Not insuring the assets of the organization • No adequate policies and procedures against mobbing?
Leaving of employees	Assets Reputation within the community Compensation	• Existence of organizational assets and equipment which the employee is using at home (theft) • Not providing for deactivation of all access codes and passwords

Source: own source

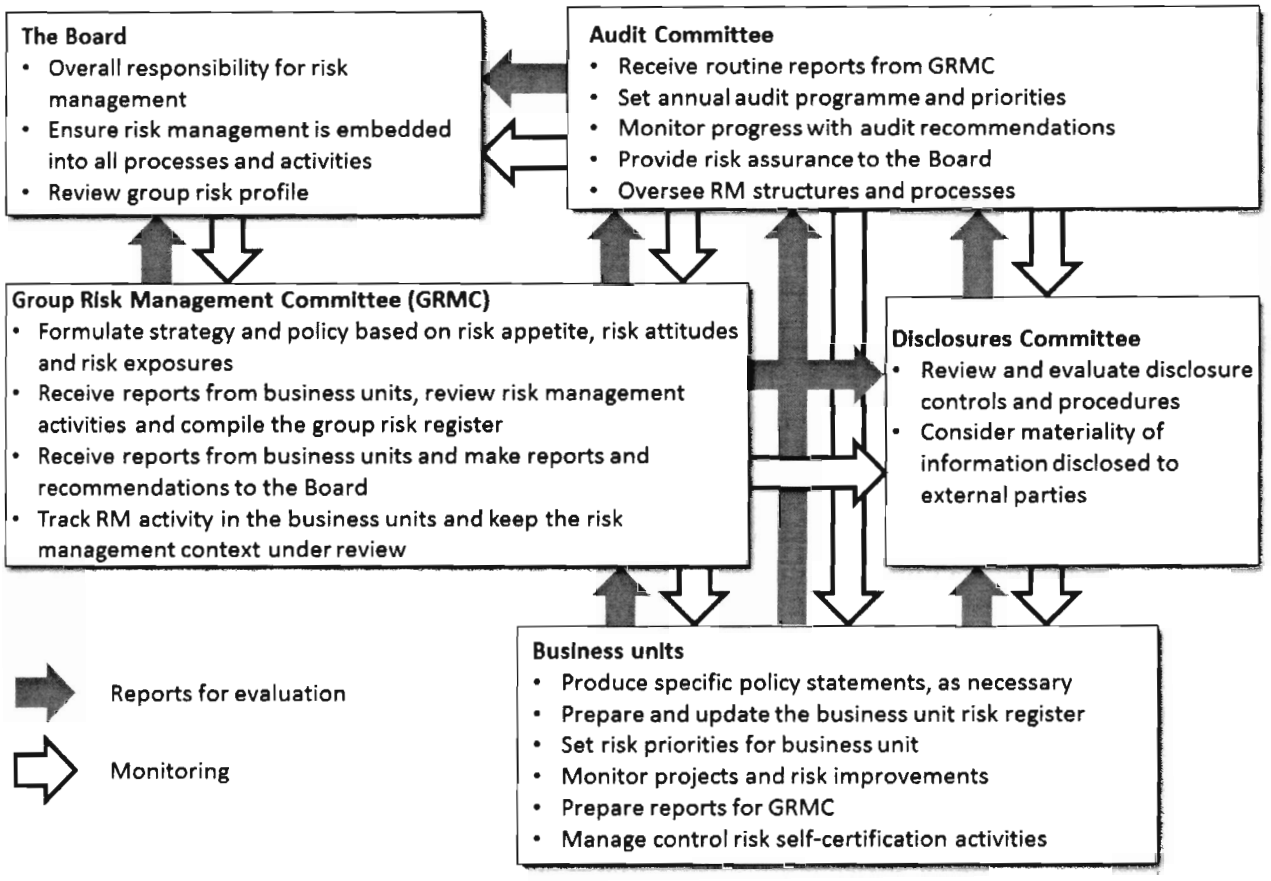

Figure 5. Scheme of the risk management organization example within the business structure Source: A structured approach to enterprise Risk Management (ERM) and the requirements of ISO 31000

The head of the Risk Management Board is the safety manager who usually holds the title of CSO (Chief Security Officer). CSO is the highest executive corporate function which answers to the top management in the matters of safety. The CSO is directly responsible for identification, development, implementation and maintenance of safety processes through risk diminishing procedures, response to incidents, lowering exposure to all forms of risks and establishing safety policies and procedures.

4. CONCLUSION

The above said may lead to the conclusion that human resources management within an organization is one of the key processes which directly influence all other business processes. Since each business process takes place in uncertain conditions, i.e. there is a number of risks which may endanger the achievement of process objectives, among other things due to inadequate human resources management. In order to lower the level of risk dependant on human resources, it is necessary to manage them, i.e. keep them at an acceptable, low enough level. This achieves proactive human resources management, as one of the prerequisites for successful business of the organization.

There is no standard which is directly focused on human resources risk management, but as shown, based on some existing, broadly applied standards (ISO 31000, ISO 27001) it is possible to approach human resources risk management completely and with high quality, without basing the approach solely on the creativity of the organization.

Functional introduction of risk management in an organization makes sense as a part of the whole approach to management of all types of risks. Depending on the size of the organization and the awareness of the management, this basically requires a partial reorganization of the company. When it comes to smaller companies, this is reflected in assigning additional functions to some employees who are additionally educated for risk management jobs, and in larger organizations this is resolved by formally introducing new organizational units.

REFERENCES

[1] John Stevens (Ed): Managing Risk: The Human Resources Contribution, LexisNexis UK, 2005, ISBN 0406971455.

[2] Timothy P. Layton: Information security Design, Implementation, Measurement, and Compliance, Auerbach Publications, 2007, ISBN 0-8493-7087-6 .

[3] Mathis, Robert L., Jackson, John H.: Human Resource Management, South-Western Educational Publishing, 1999, ISBN 0538890045.

[4] Lacey, David: Managing The Human Factor In Information Security: How To Win Over Staff And Influence Business Managers, John Wiley and Sons, 2009, ISBN 9780470721995.

[5] Beach, Lee Roy: The Human Element: Understanding And Managing Employee Behavior, M.E. Sharpe, 2007, ISBN 9780765620354.

[6] Duffey Romney Beecher, Saull John Walton: Managing Risk: The Human Element, Wiley, 2008, ISBN 9780470699768.

[7] Jane Gawron Valerie, Gawron Valerie J.: Human Performance, Workload, And Situational Awareness Measures Handbook, Second Edition (Handbook), CRC, ISBN 9781420064490.

[8] A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000, AIRMIC, Alarm, IRM, 2010.

Standards

[9] ISO 9001:2008, Quality management systems - Requirements.

[10] ISO 14001:2004, Environmental management systems - Requirements with guidance for use.

ISO 22000:2005, Food safety management systems - Requirements for any organization in the food chain.

[11] ISO/IEC 27001:2005, Information technology - Security techniques - Information security management systems - Requirements .

[12] ISO 31000:2009, Risk management - Principles and guidelines.

[13] ISO Guide 73:2009, Risk management - Vocabulary.

[14] OHSAS 18001:2007, Occupational Health and Safety Management System.

[15] AS/NZS 4360:2004, Risk management.

ISSN 1450-7196

COMMUNICATIONS IN DEPENDABILITY AND QUALITY MANAGEMENT

An International Journal