ENTERPRISE RISK MANAGEMENT AND THE INFORMATION SECURITY

Zoran ČEKEREVAC[1], Dubravko ŽIVKOVIĆ[2]

SUMMARY:

Risk management should be the subject of attention in all business systems, especially in manufacturing companies. The article emphasizes the risks associated with the size of enterprises, production orientation, dislocated parts, sales and procurement processes. Special attention is given to the application of ISO standards in the field of protection against risks and increasing of safety. Failure in this area can have major consequences in terms of material losses and human life threats. In this paper, there are given some recommendations for introduction of ISO 31000 and ISO 27000 families of standards in practice.

KEYWORDS: *risk, security, information security, management, manufacturing organization, ISO 31000, ISO 27000*

INTRODUCTION

The problem of security in general, and therefore the security in manufacturing organizations, has changed radically in recent decades. This change is particularly evident from the beginning of the new millennium. Globalization requires from enterprises the expansion of the supply chain, dislocation of certain production activities (outsourcing) outside the country and even a continent, and placement of finished products on the market far broader than the local market. This results in the company's activities in the wider geographical area, and companies' defense of the potential danger becomes more complex. Furthermore, survival in the market depends on the ongoing efforts to reduce production costs, with short cycles in the development of new products, and the application of scientific knowledge and appropriate organizational measures. In these conditions, the life interest of enterprises is to go out with a new product on the market before the competition. The battle on this front is cruel and merciless, with use of all weapons, from corruption to industrial espionage. In addition, the turbulence caused by the global economic crisis, does not bypass any manufacturing organization, and therefore sacking of large numbers of employees leads to strikes, social unrests and the like.

In these terms of doing business, security risks are greatly increased, and the actions taken to reduce them are often significantly behind what really needs to be done. One of reasons for this situation is the inadequate treatment of risks. The aim of this paper is to present the treatment of risks and the information security in manufacturing organizations as well as the measures to be taken to minimize them. The work is not focused to a manufacturing plant, where production activities take place, but to the production system in general, from the information, through the procurement of materials and its transformation into finished products, up to the sale of the finished products.

RISK MANAGEMENT

Risk is defined by the international standard ISO 31000:2009 Risk management - Principles and Guidelines which provides principles and generic guidelines on risk management. It can be used by any public, private or community enterprise, association, group or individual. Therefore, ISO 31000:2009 is not specific to any industry or sector. Also, it can be applied to any type of risk, whatever its nature, whether having positive or negative consequences. It is intended that ISO 31000:2009 be utilized to harmonize risk management processes in existing and future

[1] Zoran Čekerevac, Dr, Assoc. Professor, Union University Belgrade, Faculty of business industrial management, Kosančićev venac 2/V, 11000 Belgrade, Serbia, tel. +381 11 2630654, e-mail: zoran.cekerevac@hotmail.com.
[2] Dubravko Živković, Mgr.Sc, Business College Čačak, Učiteljska 1, 32000 Čačak, Serbia, tel. +381 11 3771-552, e-mail dubravko@eunet.rs.

standards. It provides a common approach in support of standards dealing with specific risks and/or sectors, and does not replace those standards. ISO/IEC 31000:2009 is not intended for the purpose of certification. [1]

Standard ISO 31000:2009 is followed by two publications:
- ISO 31010:2009 - Risk assessment techniques,
- ISO Guide 73:2009 - Risk management glossary.

ISO/IEC 31010:2009 is a dual logo ISO/IEC supporting standard for ISO 31000 and provides guidance on selection and application of systematic techniques for risk assessment. The purpose of this standard is to be applicable in the broader context, in large and small business systems, in production, but also in other areas (economy, health, information technology, insurance, finance, etc.). [2]

There are many definitions of risk. In this paper is mentioned the one given in the ISO Guide 73:2009 [3]. In this dictionary risk is defined as the effect of uncertainty on objectives (business system). Uncertainty includes events that may but also may not happen, and also uncertainty caused by lack of information or inaccuracy or ambiguity in communication. The uncertainty includes both positive and negative effects on the aims. This definition indicates that the risk implicitly has a stochastic nature, that it has its probability of occurrence and its degree of impacts to the objectives.

Risk management includes the processes related to identifying, analyzing and treating risk [1]. It is one of the most effective mechanisms to protect people and property in productive enterprises.

Risks can be classified into three groups:
- *Known risks* – risks whose existence and whose effects are known (e.g. driving a car whose registration has expired, for which the penalty is defined in the appropriate amount).
- *Unknown / known risks* – risks whose existence is known, but whose effects are not (e.g. driving of unregistered vehicles close to the traffic policeman who checks the driving documents).
- *Unknown/unknown risks* – risks for whose existence and effects data are currently not available (e.g. when one forgets to extend the car registration and drives after the expiration of the registration).

Of course, it is not possible to predict and plan actions for all the potential risks of manufacturing companies, but for that reason, those which are the most likely and most critical should be identified, and brought to acceptable levels at reasonable cost.

Risk management of production systems is achieved through the following steps:
- *Identification* – the risk has been identified but not yet evaluated according the effects of the domain of action, scope and urgency.
- *Assessment* – the risk is measured and its priority is determined based on its importance and urgency.
- *Answer* – for all risks are foreseen appropriate actions ranging from acceptance of risk to the development of appropriate procedures to avoid or reduce risk.
- *Documenting* – the previous steps have to be documented to show the process of the decision making to transfer the acquired knowledge into the future projects.

Risk management process has a permanent character, because some risks are permanent, others have a limited duration, some transforms from concealed to the recognizable state, etc. It should be noted that the risk is higher in the initial stages of production activities, and that lowers towards the end of the activity.

There are three standard ways of treating the risk, and which of them will be implemented depends on the cost to risk ratio of each particular risk:
- *Avoidance* – the elimination of the causes of a risk before the risk occurs.
- *Mitigation* – development of procedures to reduce risks, e.g. changes in strategy or transfer risk, i.e. purchase of insurance (to transfer the potential losses to the insurance company).
- *Acceptance* – recording of the risk and willingness to accept all the consequences from such an approach.

Given the previously mentioned categories of known/unknown risks, they can be treated as follows:
- *Known risk* – If the effect of the risk is high, develop a new strategy for its disarming. If the effect of risk is low, consider mitigation or acceptance.
- *Unknown / known risk* – First, estimate the effect of risk, and then, depending on the

assessment of hazards, implement strategies that are applied for known risks.
- *Unknown / unknown risk* – Since the occurrence and effects of these risks cannot be predicted, it is necessary to consider the possibility of increasing the project budget for a certain percentage, so it can solve unforeseen situations.

Risk management in general, and in particular in manufacturing companies, is of very dynamic matter. As a consequence, every company should define its own approach to risk management, with the constructive application of standard procedures. It should be noted that there are no appropriate economic models to assess the benefits of the marginal risk reduction, as opposed to investing in its avoidance or reduction. One of the problems of risk management in manufacturing companies is also the lack of acceptable system measures, which would enable managers and analysts to adequately assess risks and identify resources to ensure their reduction or elimination. Therefore, the risk management is very complex, especially in complex manufacturing organizations. That job is permanent, and the number of officers who will deal with it is a matter of assessment of each manufacturing organization.

INFORMATION SECURITY

One of the most important tasks is to protect information. There are different ways to perform this task, but a company can get a lot of useful information from ISO27001 standard. This standard is an information technology security management processes standard which specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving documented ISMS within the context of the organization's overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof. [9]

At the time of its creation, it was said that the ISO27001 was developed to provide a model for establishing, implementing and improving an information security management system. ISO27001 uses a risk-based approach. It is independent from the applied technology. It has six parts, and includes a definition of security policy. ISO27001 defines the scope of the ISMS and conduction of a risk assessment procedure. In addition, management of identified risks must also be a factor as well as selection of control objectives and the controls that need to be implemented. At the end, statement of applicability also must be prepared. In today's conditions of industry exchanges and doing businesses, not every company has proven to be at par with the others. By fulfilling ISO 27000 demands, it is to believe that a company does business on the highest level and that is certainly a cut above the others.

ISO 27001 can help with [8]:
- minimizing the risk of privacy and security breaches,
- demonstrating due diligence for compliance with privacy laws,
- defining the security process,
- creating security objectives and requirements,
- cost-effectively managing security risks,
- ensuring the organization's security objectives are met by providing a roadmap for managing requirements,
- complying with government, industry and other regulations,
- providing a uniform platform to show customers and partners how information is secured,
- determining the extent of compliance with corporate directives and government policies.

One of the best benefits that are received from implementing the ISO27001 is avoiding specific security objectives such as threats vulnerabilities such as theft, terrorism, misuse of information and a viral attack. This is extremely important to any organization where any of the said factors can be applicable. For example, if a business has a computer network that is hacked or has had a virus uploaded to it, it could lose all the information in the network which is very detrimental to the operations of the business. [10]

One can put the question about importance and necessity of company's certification with ISO 27001, but there are many benefits when it comes to being certified with this industry standard. First of all, business continuity or the continued operations of business is insured through legal compliance and avoiding future security failure issues as well as concerns. In addition, the company can expect that their customers will be satisfied with the fact that their information will never be threatened by hackers or vagrants. When the company is certified, this will give its business or organization increased credibility by showing that the company is indeed within the industries' related standards.

At last, it is quite difficult to acquire more clients in nowadays economy. A good recommendation for potential clients is if an organization, that they are looking into, has an ISO certification. By having ISO 27001 certificate, the company assures clients that it works compliant with the standards and that intends to do its business for a long time. To get ISO 27001 certificate, a company must firstly pass through the process of registration. At the beginning it may seem difficult to proceed with the registration process, but there is not much to do if a company fulfils all the requirements and has the things that are needed for it's doing business.

If a company seeks independent certification and audit for the ISO27001, there are three phases that should be passed. At the beginning, company has to expect a visit from the auditor. The auditor has to confirm that the organization is prepared for further assessment. This step includes checking for compliance, and the report making. In this report will be registered each noncompliance or even potential for noncompliance. The second phase involves a visit of the auditor to confirm that the management system is fully compliant the requirements of ISO27001. The auditor has to document that the entire system is complying with the standard. He will thoroughly check everything so he can report about any of the noncompliance and any potential for non-compliance. In the third phase, a periodic visits from the auditor will take a place, allowing to the auditor to be sure that the company continues to do business within the industry's standards and that there is no any noncompliance.

A lot of large corporations are now trying to get ISO certificate. If company has foreign clients, and can show ISO certificate, the other party can be assured of the company's credibility. If an organization shows a sign of noncompliance, certification will not be granted. This is good recommendation to the current and potential clients.

ISO 27001 is created for the purpose of certification. When company established its ISMS that suits to the organization's needs and meets the ISO 27001 requirements, it can ask external auditor to audit its system. If auditor finds no noncompliance, the company can get an official certificate that the company's ISMS meets the ISO 27001 requirements.

A company can use ISO 27001 as a help to establish the information security management system (ISMS).

ISO 27001 uses the process approach and the Plan-Do-Check-Act (PDCA) model on the following way:

- *PLAN* – Section 4 expects the company to plan the establishment of the organization's ISMS,
- *DO* – Section 5 expects the company to implement, operate, and maintain the ISMS,
- *CHECK* – Sections 6 and 7 expect the company to monitor, measure, audit, and review its ISMS,
- *ACT* – Section 8 expects the company to take corrective and preventive actions and continually improve its ISMS.

Since ISO IEC has used a PDCA model to organize the ISO IEC 27001 standard, it is conveniently designed to facilitate system development. If company follows the five general steps (sections 4 to 8) that make up the standard, company will automatically develop comprehensive ISMS. According to ISO IEC 27001, the company must meet every requirement (specified in clauses 4, 5, 6, 7, and 8) if it wish to claim that its ISMS complies with the standard. [11]

MANAGING FOR ENTERPRISE SECURITY

Making security is one of the main business tasks. As the organizations' understanding about security growing, they look for new techniques and technologies to manage security. Enterprise security management (ESM) is a fast growing discipline that aims to help organizations in their quest for a better approach to security. Today's trends focus on shifting to the point of view where managing security is a core competency instead of an extension of information technology. This means a new approach where security is used to achieve the company's goals and that it is used that company become more resilient.

The practice of security is viewed now as all activities that keep the company's productive elements free from harm or disruption. Protected technology, people and assets can better perform their intended functions and the organization can much easier accomplish its mission. Company cannot separate security from its other goals.
In developing the ESM approach, the team is concentrating its efforts on several key processes [6]:

- *Identification of core capabilities* – The immediate focus of the ESM research is to develop a capabilities framework that represents the essential capabilities necessary for addressing security as a business problem.
- *Development of appropriate tools, techniques, and methods* – Throughout its work, the ESM team continues to develop additional supporting tools, techniques, and methods that facilitate an enterprise approach to security management. One of these methods can be the Critical Success Factors Method that helps organizations to establish a foundation for ESM by identifying the organization's strategic drivers and using them to guide security strategies.
- *Leverage best practices* **–** The best practices are beyond the scope of security and relate to many different organizational capabilities. Some of the practices used span the topics of security, IT operations and service delivery, and compliance and regulations. They represent administrative / managerial, technical, and operational practices. [6].

The physical protection of information, equipment and facilities is also very important. Security threats in a manufacturing environment can mean stopping business, assembly lines, shutdowns, fear and even a plant-wide employee evacuation.[7] In case of emergency, having a centralized security management for people, assets and information that can automatically trigger voice alarms, open doors, record video, provide reports, send email to authorities for immediate response, account for all personnel in and out of dangerous areas, and complying with the company's safety regulations is vital for work environment.

CONCLUSIONS

Today's manufacturing companies are exposed to many risks in their work, including risks of information, property and persons' security. Risk management in manufacturing organizations is vital to their work and success. In large production systems, there are countless critical points where problems may appear. If a company allows these problems to escalate, it can result in the issue of stable operation of the company, there may appear a great material costs and, even worse, loss of human life. The company has to fight, with the consistent application of methods and techniques of risk management that the unwanted situations do not occur. Employees, who deal with risk assessment and safety aspects of the manufacturing enterprise, should be trained to look for potential points of risk. Risk management team should be composed on the way that it connects people with knowledge and experience to predict what might happen. The most dangerous risks are included in a specially prepared supervision plan. The risks which potential adverse effects are lower are not a subject to special control procedures, and they are managed by managers at lower levels. When a risky situation appears, there has to be pre-defined procedure that should be applied. In the event of a problem that has not been considered, and whose influence cannot be estimated, the problem can be solved more easily by using special budget funds planned for such situations.

Failure in risk protection could have negative consequences not only for the company which initiated the implementation, but also on local development in the case of small companies, up to the global consequences in the case of international corporations. It can and should be avoided if a company pays enough attention to the risks to which the company is exposed.

LITERATURE

[1] "A guide to the Project Management Body of Knowledge (PMBOK)", 1996, Project Management Institute.
[2] APICS Principles of Operations Management: Principles of Ops Planning Participant Guide, 2011, APICS.
[3] http://www.iso.org/iso/catalogue_detail?csnumber=43170
[4] http://www.iss.rs/standard/?natstandard_document_id=34180.
[5] http://www.sei.cmu.edu/library/abstracts/news-at-sei/feature220051.cfm.
[6] http://www.lenel.com/manufacturing.
[7] http://www.qmi.com/registration/iso27001/Default.asp?language=english.
[8] http://www.iss.rs/standard/?natstandard_document_id=37873.
[9] http://www.iso27001pdf.org/.
[10] http://www.praxiom.com/iso-27001-intro.htm.
[11] "Principles and Guidelines on Implementation", 2009, ISO 31000:2009.
[12] "Risk Management Vocabulary", 2009, ISO Guide 73:2009.