Bojan Hlača, Ph. D.
Rijeka Port Authority
Riva 1
51000 Rijeka
Saša Aksentijević, univ. mag. oec.
Saipem Mediteran usluge d.o.o.
Alda Collonella 2
51000 Rijeka
Edvard Tijan, univ. mag. ing.
Faculty of Maritime studies
Studentska 2
5100 Rijeka
Croatia

Review article
UDK: 004.056(083.74)
656.615(497.5 Rijeka)
Received: 5th October 2008
Accepted: 23rd October 2008

INFLUENCE OF ISO 27001:2005 ON THE PORT OF RIJEKA SECURITY

The purpose of this paper is to explain clearly the role of the information system security management within the entire Port of Rijeka security process. The complexity of the Port of Rijeka system, in which Rijeka Port Authority contemplates the development strategy of the Rijeka traffic route and the services provided by the Port within the framework of the already existing development paradigm of the information-communication system, is elaborated. Within the management of the information-communication resources, one of the basic prerequisites for a success is the information security, or the protection of the information security management system. Therefore, the ISO 27001:2005 Certificate, which deals with the information security system management, is to be considered in the scope defined by the organization itself. While studying the advantages of the ISO 27001:2005 Certificate, the characteristics of Rijeka Port Authority are defined, the contents of the Certificate itself are explained and the possible comparative advantages that can be obtained within the broader framework of the port security process are stated.

Key words: *ISO 27001:2005 Certificate, information security management, Rijeka Port Authority.*

2. INTRODUCTION

Rijeka Port Authority was established in 1996 as a non-profit-making organization, that, after a thorough reorganization, has started with its activities within a strategic management of the port resources as an isolated process, which differs from the one of the economic usage of the port, and, consequently relayed to the concession partners, effectively and privately-owned companies. The primary role of Rijeka Port Authority has become the general management and strategic development planning.

After the Croatian War of Independence, lasting from 1991 to 1995, a great part of the port activities was transferred from the port of Rijeka to the ports of Kopar and Trieste. Efforts undertaken in the last decade, both in the areas of management and operations, have resulted in the revitalization of the capacity usage and turnover growth. In the past 8 years the total growth of bulk cargo was 216 percent, an explosive growth of the container cargo was almost 930 % (measured in TEU) and the growth of oil and oil products transport was 26 %. The number of passengers in the passenger traffic increased almost by 270 % [5].

The plans of Rijeka Port Authority are not limited strictly to their field of interest, but they are reflected on the city of Rijeka and its functioning as a whole, especially after the financing of the Rijeka Gateway project was approved to the amount of 155 million US$ by the World Bank and the further 26 million US$ derived from the budget of the Republic of Croatia. This plan shall revitalize a part of the Rijeka shore area and of the port facilities, create new and additional port capacities, avoid traffic issues that arose from effecting the merchandise delivery and transport by using the city roads and streets network and, within the principles of sustainability, shall create new seaside areas designed for the citizens of Rijeka, for public life and residential quarters. The basic part of the Rijeka Gateway project is the building of the state roads D 403 and D 404 that will connect the eastern and western port capacities with the exit to the highway, the construction of a new passenger terminal, fishing port (the first such port at the eastern coast of the Adriatic Sea) and the change in the purpose of the Delta and Porto Baross area, aiming at revitalizing and redesigning them as tourist and residential areas.

The location overview reveals that the Port of Rijeka economic activity is distributed to several locations. Furthermore, as alreay explained, the economic activities have been entrusted to concession-holders. For example, the general cargo concession-holder is the Port of Rijeka, the concession-holder for the transport of liquid cargo is Jadranski naftovod d.d. (The Adriatic Pipeline), while the container cargo concession is offered to the company Jadranska vrata d.d. (The Adriatic Gateway). A series of other concession-holders and partners are dealing with towing/tugging, quality and quantity control, ship supplying, ecology and other business areas of a particular interest.

Table 1: Activities in the Port of Rijeka area

Activity	Location	Remark
General cargo terminal	Port core – the Rijeka city center	Newly-built storage area is situated at the outskirts of Rijeka, in Škrljevo
Container and Ro-Ro terminal	Brajdica	
Bulk cargo terminal	Bakar	
Grains silo	Brajda	
General cargo and livestock	Port basin Rasa	Location Stalije - general cargo Location Bršica – livestock
Liquid cargo	Bay of Omišalj (on the island of Krk)	
Passenger traffic	Rijeka city center	

Source: created by the author

It can be concluded that, from the organizational point of view, the system of port traffic and its activities is a rather complex one, due to the different types of traffic, geographic location of various port capacities and to the fact that the economic activities are carried out by a number of concession-holders, heterogenous in nature.

2. INFORMATION AND TELECOMMUNICATIONS SYSTEM AND PROJECTS WITHIN RIJEKA PORT AUTHORITY AREA

The organization of the information and telecommunications system within such a complex system as the Port of Rijeka is, presents a challenge in front of the Board of Directors of Rijeka Port Authority, its Chairman and the ICT department manager. It is neccessary not only to enable a first-class network [2], physical and logical connections in all locations and support in terms of software, hardware, lifeware and orgware, but to maintain control over all the delivered ICT services as well, in such a way as to concentrate all feedback information about their utilization in one control point, whilst all functions fulfill their purpose in the distributed modality and uninterruption, in order to respect all principles of disaster recovery and business continuity.

In order to fully understand the complexity of the implemented systems, it is neccessary to outline briefly some specific qualities regarding the ICT technology implementation in the Port of Rijeka area as well as some challenges that are confronting both the responsible ones and the partners or subcontrac-

tors, implemented in a project development within the framework of expanding and restructuring the area under Rijeka Port Authority control and management.

1. The Port of Rijeka is performing the public transport activities, the subject of being third parties using traffic and storage/warehouse resources. The inclusion of third parties in business processes always carries elevated levels of risks and threats to the integral security of the business processes, including information security as its basic constituent
2. Rijeka Port Authority is organized in such a manner as to follow maritime norms of security and surveillance in all its integral parts, and in line with the ISPS[1] code of security of ships and port areas. An accelerated development of the International ISPS Code system is caused by hijackings, raids and assaults on vessels and it was finalized in 2002 with a significant lobbying by the United States of America
3. Handling dangerous cargo, its packaging, labelling, storage, separate handling and procedures in case of emergency or danger within the area of Rijeka Port Authority is in line with the IMDG[2] Code revised and refreshed every two years according to real-life developments in the area of the transport science and practice.
4. The tracking of the ship traffic in the port area is done by using the modern VTMS[3] system that uses GPS (Global Positioning System) equipments.
5. Surveillance of the service users is done via an identification cards (ID) and integrated business information system.
6. The Harbour Master`s Office performs tasks related to security and surveillance in segments dealing with security and uninterrupted traffic in the area of its responsitibility and is involved in the process of search and rescue at sea and inspection.
7. Rijeka Port Authority is theoretically and practically dedicated to the goals of excellence, development of information and telecommunications infrastructure and is keeping up the pace with similar projects in other European and worldwide ports.

Finally, Rijeka Port Authority participates in projects of procurement in a transparent and professional manner, often in international bids. Therefore, it is of utmost importance to improve the existing processes which involve information and integral security, raising them to a higher level and deriving benefits to all included in the business process. The ISO, SEC CODE department and the Inspection department of Rijeka Port Authority are ISO 9000 certified,

[1] International Ship and Port Facility Security Code

[2] International Maritime Dangerous Goods

[3] Vessel Traffic Management System

while the VTMS system is subject to a separate certification according to the same norm.

Due to the obvious importance of information and integral security in the framework of entirety of business processes, it is suggested, both as a logical and optimal measure in the continuty of Rijeka Port Authority activities, to consider the introduction of the information security management system, according to the internationally recognized norm ISO 27001:2005.

THE ISO 27001:2005 NORM (INFORMATION SECURITY MANAGEMENT SYSTEM)

ISO/IEC 27001 is the ISO[4] norm that, at the end of the year 2005, replaced the old British norm BS 779-2. It is a standard dealing with the information security management system that should be used together with the ISO/IEC 27002, known before as the ISO/IEC 17799 – a practical code defining goals of security controls suggesting their practical scope. This norm presents a practical model for establishing, implementing, using, following, maintaining and constantly improving the system of information security management. The design and application of the system should be under the influence of the business and operational goal systems, developing processes and size and structure of the organization. Those organizations, that in their everyday work use the ISO/IEC 27001 to evaluate their information security management system, are likely to be in line with the ISO/IEC 27001 norm.

Certifications, according to this norm, are being done by the accreditation bodies that often function at a national or international level. The process of certification is executed by the leading auditors. It usually consists of three connected phases [6]:

Checking the existence and completeness of the key documentation needed for the information security management system introduction. These usually comprise: the company security policy, the statement of applicability, the risk analysis and the risk treatment plan.

Deep probing and audit testing the existence and efficacy of the information security controls stated in the statement of applicability and risk analysis and risk treatment plan, including support documentation. The process of evaluation and information security management risk is a process in continuity and not only a one-time event. Theoretically, it is thought that the information security management system is never fully implemented; in fact, it is constantly in the process of evaluation and search for non-conformities and their rectification.

[4] International Organization for Standardization

Repeated evaluation or post-revision, checking whether the companies or organizations, initially certified in line with the standards, are still compliant. This is done periodically in order to confirm that the information security management system functions as it was envisaged, implemented and initially documented.

The standards are so structured that it is possible to implement them in every organization, profit- or non-profit-making, independently of its size. In the core of the standards is a basic demand for information security outlined in the C-I-A triad [1], according to which the access to information is allowed only to those who are authorized for its use, the information must be accurate and complete and the information access must be uninterrupted and allowed in continuity when necessary and in scope that has to be defined in advance.

The ISO/IEC 27001 and ISO/IEC 17799 standards define the following phases (steps) in the information security evaluation and risk management process:

1. Defining the approach to risk evaluation:
   - Identification of the evaluation methodology, appropriate for the system of corporate governance, legal and other external and internal demands
   - Development of the criteria for risk acceptance and identification of the acceptable risk level
2. Risk identification:
   - Identification of information assets within the scope of the assessment and identification of asset owners [3]
   - Identification of possible threats to the listed assets
   - Identification of vulnerabilities that could be exploited by the threats in order to cause damage
   - Identification of influence that loss of availability, confidentiality and integrity might cause to the listed assets
3. Risk analysis and assessment:
   - Evaluation of the influence on business processes that could be caused by security incidents
   - Evaluation of the possibility that the security incidents will occur in line with the identified vulnerabilities and threats and evaluation of the existing protection measures
   - Evaluation of risks acceptance and whether a risk requires treatment using the risk acceptance criteria
4. Identification and evaluation of risk treatment possibilities
   - Application of adequate protection measures
   - Risk acceptance
   - Risk evasion
   - Risk transference to third parties (insurance companies, vendors etc.)

5. Selection of protection measure goals and determining security measures for risk treatment
   For those risks for which the organization has decided to apply adequate protection measures, it has to be ensured that the risk is lowered to an acceptable level, considering:
   - Local and international legislative demands
   - Goals of the organization
   - Operative needs and constraints
   - Price of implementation in comparison to the severity and impact of the risk that has to be lowered
   - Need to balance investment in implementation versus potential damage from security incident occurrence.
6. Obtaining the Board approval for the protection measures implementation and risk acceptance

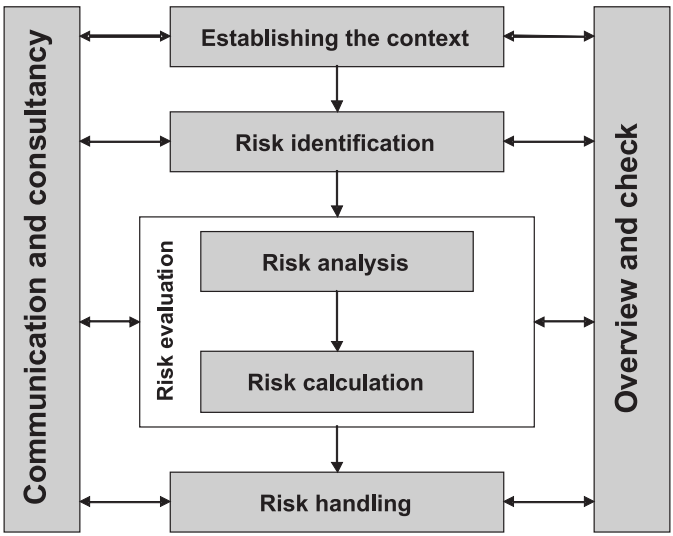


Figure 1: Process of risk evaluation and risk management

Source: Kosutic, D.: "Elements of assessment and information risk management", Kvadra Consulting LLc, 2007.

The standard itself is based on the PDCA model[5] applied to all structures of the information security management process.

[5] "Plan-Do-Check-Act", ISO 27001:2005 basic methodology

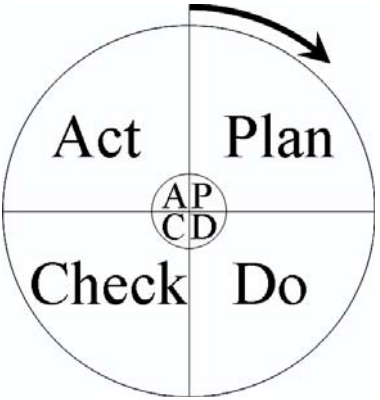


Figure 2: PDCA cycle (Plan-Do-Check-Act cycle)

Source: created by the author

The standard involves:

1. Planning the ISMS introduction[6] – in this phase it is necessary to establish information security policy, define goals, processes and procedures needed to manage the risk and improve information security, and contribute to the goals of the organization
2. Implementation (usage of the ISMS) – policies, controls, processes and procedures dealing with the information security management system are being introduced and operatively used
3. Checking (follow up and the ISMS revision) – during the checking phase, the functioning of the information security management system is being measured and compared to the existing policies, goals and practical experience; the final results are handed over to the Board in charge
4. Application (maintenance and improvement of the ISMS) – after the checking, corrective and preventive actions are being undertaken based on the results of the internal revision in order to establish a constant improvement of the information security management system

The standards require that part of the procedures must be in a documented form, while for the operative procedures, it is necessary that they exist but do not have to be documented. Documents in a written form, envisaged within the standards, are the following ones:

– information security policy and goals
– information security management system scope

[6] ISMS – Information Security Management System

- procedures and controls supporting information security management system
- description of the risk assessment methodology
- report on risk assessment
- plan of risk treatment
- documented procedures used by the organization to ensure effective planning, execution and process control in the information security and description of the control efficiency
- documented procedures describing the record keeping
- statement of control applicability
- documented responsibility of the instances in charge of audit planning and revision, reporting and audit result safekeeping
- documented procedures on the execution of corrective and preventive actions

Controls or protection measures are ways to manage information risks. In its basis, they incorporate processes, policies, standards, practices, guidelines, instructions, organizational structures and other elements that can be administrative, managerial, legal or technical in nature. The basic purpose of protection measures (controls) is to lower the risk identified through the risk assessment that is imposed to the functioning of the information security management system.

The ISO standard 27001:2005 in its separate part, annex A, recommends a total of 133 controls that regulate the areas of specific competence through its sub controls which are [9]:

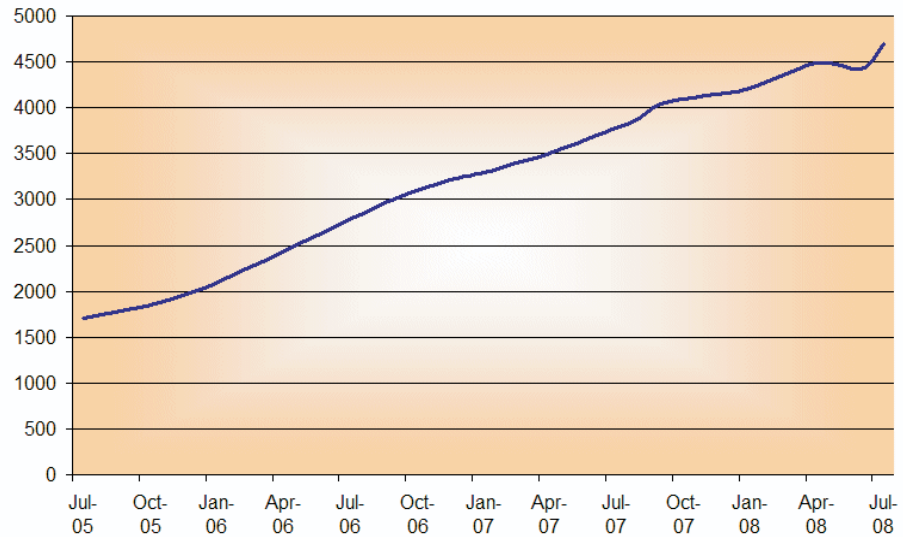
1. Controls of security policy
2. Controls of organization of information security
3. Controls or resources management
4. Staff security controls
5. Controls of physical security and environment security
6. Controls of communications management and operative procedures
7. Access controls
8. Controls of procurement, development and information system development
9. Controls of information security management incidents
10. Controls of business continuity management
11. Controls of law and regulation compliance

4. ANALYSIS OF THE APPLICABILITY AND POTENTIAL BENEFITS OF THE ISO 27001:2005 CERTIFICATE IN RIJEKA PORT AUTHORITY

The basic benefits that Rijeka Port Authority could yield from the ISMS certificate according to 27001:2005 can be derived from the JTC1/SC27 board guidelines, in charge of the ISO 27001 and related to the standard family:

1. Security demands and goals can be articulated in a clear way, using common language and internationally recognized terminology and procedures that can be clearly understood both by partners and collaborators in international bids
2. Security risks can be addressed in line with goals of cost effectiveness
3. Setting up the system to be ISO 27001:2005 compliant enables an easier adjustment to local legislation
4. The norm can be considered to be a framework within which security controls can be implemented that will ensure the achievement of specific goals set by the Management Board of Rijeka Port Authority
5. Introduction of the norm in one part of the system enables an easier introduction in some other processes or systems, if the need occurs
6. Introduction of the norm makes the underlying processes and subjects involved in the process of information policy security creation and information processes management more transparent and clear
7. The certification system can be also used to determine effectiveness of the existing activities of the information security management and of the information security processing
8. The ISMS certification shows to internal and external auditors that the information security policies have been completely adapted in a clear manner, demonstrates the level of the achieved compliance on a practical level and can be used in order to prove relevant information to concession-holders, clients, partners, banks and insurance companies of the clear intention of Rijeka Port Authority to achieve the goals of excellence in management
9. The relevance of the ISO 27001:2005 certificate is clearly visible in the exponential growth of the organizations that have in the past three years certified their respective ISMS's according to that norm.

Chart 1: Number of organizations in the world certified according to the ISO 27001:2005



Source: http://www.iso27001security.com/html/27001.html

5. CONCLUSION

Due to its location, variety of installed port capacities, organization and importance in the maritime world, the basin of the Port of Rijeka has been recognized by the Republic of Croatia as a strategic resource. Rijeka Port Authority represents a body that uses strategic and managerial activities in order to fulfill the potential of the port activities in the Kvarner area. This can be seen in the change of the organizational paradigm from the mid 90's of the past century and the consequential growth of the port capacities, their quality, quantitative indicators that follow the positive momentum of movement and the number of the carried out projects.

Rijeka Port Authority does not perform its activity in an isolated manner as regard other subjects involved and the course of its activity flows both towards the concession-holders of the port activities, clients, international organizations that regulate the area of the port activities and harbor security and traffic, potential creditors and project investors and to those directly involved in their execution and later exploitation of new capacities and services.

The diversity of the applied technological support in the sector of information and telecommunications of Rijeka Port Authority calls for reasonable activities in regard to information security, to ensure that the principles of excellence towards all parties involved can be reflected on elevated levels of the key processes security, information and channels of their exchange. Therefore, an evaluation of key processes is indicated along with the assessment of all underlying risks and the introduction of a coherent information security management system, not only according to the rules of common sense and good governance, but also by using the professional standards certification system. The optimal system of certification in this case would be the internationally recognized norm ISO 27001:2005.

The ISO 27001:2005 provides an extreme flexibility to the organization when it comes to determining the exact certification scope. The organization is not obligated to certificate the whole information security management system according to this norm. On the contrary, it can be done only with the part that is considered to be crucial, or the part that should be adequately and additionally protected.

Certification calls for the participation of all decision levels and operative levels included, but has to be initiated from the management pyramid top, in this case the Management Board. Only a firm commitment from the top decision levels and their dedication to the supervision of obligations committed towards information and integral security can set and maintain a coherent and robust information security management system. The certification benefit usually exceeds the invested resources. These resources can be clearly quantified by using the GAP and S.W.O.T. analysis methodology that are a subject of the separate analysis and consideration and are an elementary part of the preliminary cooperation with the consultant team involved in the certification preparation process of Rijeka Port Authority.

The anticipated length of the certification can be set from 9 months to one year under optimal conditions, depending on the scope and subject of the certification, on the existing condition of the information security management system and on the general complexity of the organization.

Before the proper certification process, a clear segregation of the duties is recommended. This means that the security management function should be held separately from other business functions, especially from the information and communication department that sometimes, due to their nature, deal with the operative tasks of information and integral security function. The reason for duty segregation is the fact that the entity operatively executing certain security measures, or the entity included in the security measure management should not be the auditor that has to evaluate their efficiency in non-biased manner.

BIBLIOGRAPHY

[1] Stamp, M., Information security principles and practice, Wiley-Interscience, 2006.
[2] Sviličić, B., A. Kraš, Zaštita privatnosti računalnog sustava, Pomorstvo, 19(2005), str. 275-284.
[3] Tipton, H.F., M. Crause, Information Security Management Handbook, 5th ed., Volume 3, Auerbach Publications, 2006.
[4] Kosutic, D., Elements of assessment and information risk management, Kvadra Consulting LLc, 2007.
[5] Yearbook 2007, Rijeka, Rijeka Port Authority, 2007.
[6] Aksentijevic, S., Integral corporate security function and information system security management – Saipem Mediterranean Services LLc, Master thesis, Rijeka, S. Aksentijevic, 2008.
[7] http://www.iso27001security.com/html/27001.html, 03.09.2008.
[8] http://www.portauthority.hr/rijeka/lucka_uprava_rijeka.shtml, 03.09.2008.
[9] http://17799.standardsdirect.org/, (ISO 27001 and ISO 27002 (ISO 17799), Standards Direct International Standards And Documentation), 03.06.2008.

Sažetak

UTJECAJ ISO 27001:2005 NA SIGURNOST RIJEČKE LUKE

Cilj ovoga rada je jasno izložiti ulogu upravljanja sigurnošću informacijskog sustava u cjelokupnoj sigurnosti luke Rijeka. Objasnit će se složenost sustava Lučke uprave Rijeka, način na koji Lučka uprava promišlja razvojnu strategiju riječkog prometnog pravca te usluge koje pruža u okviru postojeće razvojne paradigme informacijsko-komunikacijskog sustava. U sklopu upravljanja informacijsko-komunikacijskim resursima, jedna od temeljnih odrednica uspješnosti svih interesnih skupina uključenih u poslovnu aktivnost jest zaštita sustava upravljanja informacijskom sigurnošću. Predlaže se razmatranje certifikacije prema normi ISO 27001:2005 koja se odnosi na upravljanje sigurnošću informacijskog sustava u opsegu definiranom od strane same organizacije. Pri tome se povezuju specifičnosti poslovanja Lučke uprave, navodi postupak i sadržaj certifikacije te nabrajaju moguće komparativne prednosti koje mogu biti dobijene procesom certifikacije unutar ukupnog sustava sigurnosti u lukama.

Ključne riječi: *ISO 27001:2005 certifikacija, upravljanje informacijskom sigurnošću, Lučka uprava Rijeka*

Dr. sc. Bojan Hlača
Lučka uprava Rijeka
Riva 1
51000 Rijeka

Saša Aksentijević, univ. mag. oec.
Saipem Mediteran usluge d.o.o.
Alda Collonella 2
51000 Rijeka

Edvard Tijan, univ. mag. ing.
Pomorski fakultet u Rijeci
Studentska 2
5100 Rijeka