ICIC Express Letters
Part B: Applications
Volume **8**, Number **3**, March **2017**

ICIC International ©2017 ISSN 2185-2766
pp. 633–638

DEVELOPMENT OF REFRIGERATED WAREHOUSES LOGISTICS SYSTEM BASED ON THE ISMS

Gyusung Cho[1,*], Hyun-Sik Kim[2] and Minsoo Kim[3]

[1]Department of Port Logistics System
[2]Department of Mechanical Engineering
Tongmyong University
428, Sinseon-ro, Nam-gu, Busan 48520, Korea
[*]Corresponding author: gscho@tu.ac.kr; hyunskim@tu.ac.kr

[3]Division of Systems Management and Engineering
Pukyong National University
45, Yongso-ro, Nam-gu, Busan 48547, Korea
minsky@pknu.ac.kr

Received August 2016; accepted November 2016

Abstract. *Ports are important facilities and are responsible for over 90% of imports and exports in South Korea. A series of procedures that make ports perform exportation and importation more smoothly is termed port logistics. Informative communications between freight information facilities and carrier information facilities are crucial for processing the freight shipped through importation and exportation. The various information generated by refrigerated warehouses logistics is currently under the control of national authorities; however, the focus on refrigerated warehouses logistics information security has been very low. Accordingly, this research will provide plans, based on an information security management system, to build and operate the information security management system required for refrigerated warehouses logistics information system that is appropriate for South Korea. In this study, we suggest a framework to enhance the information security and performance of logistics system. The build plans suggested by this research will serve as the basis for building an information security system required for national port logistics & refrigerated warehouses logistics industries.*

Keywords: Refrigerated warehouses logistics system, Information security management system, Information

1. **Introduction.** Client information leakage may lead to social liabilities in the corporate information security of a company. These liabilities include bankruptcy owing to damage to the reliability of the company when a class action lawsuit is suggested [1]. Accordingly, the company needs a continuous process reformation activity to build and operate a risk-management-based system. This will protect information assets from various threats and eventually secure the continuity of the business. Recently corporate and organizational information, including corporate information, industrial information, and personal information, have been recognized as important corporate assets; therefore, intensive management plans are being carried out for these assets [2]. Accordingly, an Information Security Management System (ISMS) is being built mostly in the financial industry to efficiently manage and maintain information security [3].

Port logistics is an important industry that conducts the import and export functions of a company; therefore, various information pertaining to port logistics should be intensively managed. However, there have been insufficient efforts to secure various logistics information in the port logistics industry from external threats. Various information security-related policy reviews and research studies are being conducted by national authorities, but the security measures and research related to port logistics information still fall short [4,5]. These studies have just focused on the private security of port security workforce improvement plan of operation system [6,7]. South Korea requires the management of various logistics information that is used in the logistics industries, and needs to build a security management system for integrated logistics information. Functions that integrate and adjust logistics security are spread around each central office group, and basic plans to manage these functions are currently lacking despite the global importance of logistics security policies.

This research suggests plans for building and operating a port logistics Information Security Management System (ISMS) that is suitable for port logistics industries based on ISMS in order to efficiently manage and utilize port logistics information. Accordingly, Section 2 explains information security concepts and management procedures, Section 3 presents the definition of port logistics ISMS, and Section 4 suggests build plans for the port logistics ISMS and conclusions for these.

2. Information Security Management.

2.1. Information security synopsis.

Information security is a preservation of confidentiality and integrity and provision of availability of information. Additionally it refers to other properties, such as authenticity, accountability, non-repudiation, and reliability [8].

Information security has 8 principles as follows.

1) Information should be classified according to an appropriate level of confidentiality, integrity and availability and in accordance with relevant legislative, regulatory and contractual requirements and IOE policy.
2) Staff with particular responsibilities for information are responsible for ensuring the classification of that information; for handling that information in accordance with its classification level; and for any policies, procedures or systems for meeting those responsibilities.
3) All users covered by the scope of this policy must handle information appropriately and in accordance with its classification level.
4) Information must be complete, accurate, timely and consistent.
5) Information should be both secure and available to those with a legitimate need for access in accordance with its classification level.
6) Information will be protected against unauthorized access and processing in accordance with its classification level.
7) Information will be protected against loss or corruption.
8) Breaches of this policy must be reported.

Information security management is a series of activities that oversee various security measures to maintain the confidentiality, integrity, and availability of personal or corporate information assets. Information security management efficiently secures information over a certain period of time through the building, implementation, operation, monitoring, review, and improvement of a risk-based approach.

2.2. ISMS: Information Security Management System.

ISMS is a system built for the efficient management of corporate information security. ISMS is being built and operated by the national authorities to efficiently secure corporate information. ISMS is a regime granting compatibility verification of the total system (ISMS) for the establishment, management, and operation of protections in order for a company (or an organization) to secure important information assets from various internal and external threats.

ISMS has the following purposes.

1) It minimizes the possibility of private information invasion owing to carelessness or neglect by a private information handler by providing a methodology that allows an invasion-free company to perform continuous private-information security activities.
2) It serves as detailed and trustworthy evidence for evaluation by providing verification, which works as a standard for individuals to recognize secure private-information management companies, so that the individuals can decide whether to provide their personal information.
3) It works as a leakage prevention for the internal information of national companies and for local information. It not only works as a national verification service related to private information security and protection of consulting markets, but also prevents corporate information and goods from leaking into foreign authentication institutions.

ISMS must be continuously maintenance-controlled while operating through its five-stage procedure, as shown in Figure 1. The stages are as follows: Information Security Policy Establishment and Range Setting, Management Responsibilities and Organization Construction, Risk Management, Information Security Measure Implementation, and Oversight.

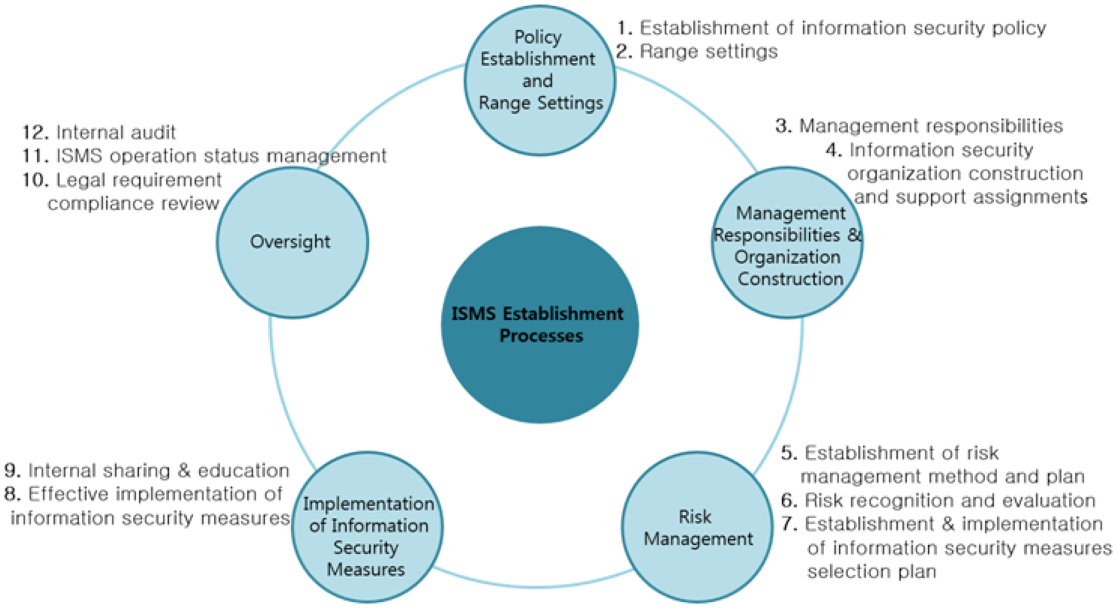
Policy Establishment and Range Settings
1. Establishment of information security policy
2. Range settings
Management Responsibilities & Organization Construction
3. Management responsibilities
4. Information security organization construction and support assignments
Risk Management
5. Establishment of risk management method and plan
6. Risk recognition and evaluation
7. Establishment & implementation of information security measures selection plan
Implementation of Information Security Measures
8. Effective implementation of information security measures
9. Internal sharing & education
Oversight
10. Legal requirement compliance review
11. ISMS operation status management
12. Internal audit
ISMS Establishment Processes

Figure 1. ISMS establishment process

3. Port Logistics ISMS Definitions.

3.1. **Port logistics information summary.** Port logistics information is various information that is gathered while performing port logistics functions. Port logistics informatization refers to a system that is built based on port logistics information. The ultimate purpose of a port logistics information network built upon port logistics informatization is to minimize offline freight congestion that occurs owing to incomplete freight transit information. In addition, individual logistics information networks such as ground vehicles, airlines, and shipping provide for the One-Stop Service of freight through mutual contact with relevant networks such as trade, customs clearance, finance, and insurance, and with national computer networks in other sectors. In this respect, a logistics information system for port logistics informatization becomes a combination of software and hardware that provides for the efficient transition of freight by utilizing national physical networks and application service networks. At present, South Korea is building and operating a

Port Management Information System (Port-MIS) to maintain port logistics information under control of the national authorities.

Port-MIS is a port logistics information integration system that is installed and operated in order to promote efficiency in port management and operation. Port-MIS was launched as an online system in 1992. The system supports policy decisions for scientific port management and provides convenient functions to port users. The operation system of Port-MIS, built upon the previously mentioned port logistics information integration system.

3.2. **Concept of the Port Logistics Information System Information Security Management System (Port-MIS ISMS).** The Port Logistics Information System Information Security Management System (Port-MIS ISMS) systematically and efficiently performs port logistics information-security activities and operates at port logistics companies. Port-MIS ISMSs favorable to each company should be established and operated so that port logistics companies can effectively perform information security activities.

3.3. **Building conditions for Port-MIS ISMS.** Organizational, technical, physical, and integrated aspects should be considered before building a Port-MIS ISMS. Organizational aspects set the organization composition, operation range, and boundary clarification of port logistics companies. Technical aspects set the technical range and boundaries for security performance. Physical aspects set the physical implementation range and boundaries. Integrated aspects combine the previous three aspects. All of these aspects must be considered. The mentioned build procedure is shown in Figure 2.

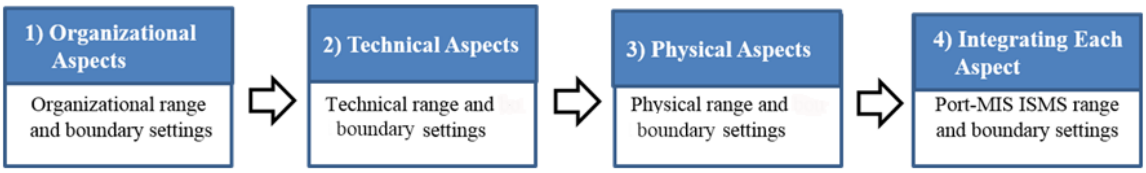
1) Organizational Aspects
Organizational range and boundary settings
2) Technical Aspects
Technical range and boundary settings
3) Physical Aspects
Physical range and boundary settings
4) Integrating Each Aspect
Port-MIS ISMS range and boundary settings

Figure 2. Port-MIS ISMS build procedure

3.3.1. *Organizational aspects.* Port-MIS ISMS ranges for organizational aspects should include the department or team that performs the primary activities, considering the main industries and work characteristics of the organization. Moreover, not only the department or team of companies and governmental agencies linked to Port-MIS which cover all ports operating including management of vessel and cargo movement, but also the manpower from partnered companies and charging companies performing work mandated by those organizations, should be included in this range. To clearly define the boundaries of the organization, responsible areas within the organization should not be horizontally nested with others. Responsible areas may be subject to redefinition if the responsible areas or ownership are unclear.

3.3.2. *Technical aspects.* Definitions of technical range and boundaries should not consider IT equipment-based aspects but Port-MIS aspects. If a certain information system work process is included in the Port-MIS ISMS range, then all technical elements related to this information system should be included in this range. This range contains the related main information and the saving of this information, and all technical elements related to the transfer process and assets related to these elements. Information systems can occasionally be operated beyond the boundaries of an organization or a country. In this case, the following points should be considered:

- Sociocultural environments

- Laws, regulations, and contract requirements applied to the organization
- Organizations having management responsibilities for communication infrastructures (wireless, cable, or data/sound networks)
- Organizational software used and controlled by organizations
- Networks, application programs, and hardware equipment that comprise information systems, roles and responsibilities of hardware, software, and networks

3.3.3. *Physical aspects.* These are security management processes using physical tools to secure Port-MIS from tools that are used at port logistics container terminals but threaten their operation (men, vehicles, etc.) in physical aspects. Subjects of security management work are men, and the security from physical aspects makes the security systems support men, allowing them to perform security management work more effectively:

Definitions of physical range and boundaries include buildings, data centers, and facilities of the organization included in Port-MIS ISMS. If information systems that traverse the physical boundaries (such as mobile communications) exist, then these systems should be included in the physical aspects. Physical aspects consider the following points:

- Remote installations
- Interface for services provided by external users' information systems and third parties
- Applicable interface and service levels

3.3.4. *Integrated aspects.* Port-MIS ISMS settings and operations must be performed from integrated aspects that consider the three previous aspects simultaneously:

- Main characteristics of an organization, work features, structures, services, assets, and responsibilities, and limitations of these assets
- Maps showing physical locations and boundaries within the boundaries
- Organizational structures, related roles and responsibilities, and relationships among them within the range

3.4. **Port-MIS ISMS requirements.** Thirteen control areas and the requirements for each control area exist in order to build a Port-MIS ISMS, and an efficient Port-MIS ISMS can be only built upon these details. Finally, continuous management should be performed through the five-stage management procedure when Port-MIS ISMS is built. In other words, all procedures from the establishment of information security policy to ISMS range setting, risk management, implementation of information security systems, and oversight must be continuously performed.

4. **Conclusions.** This research suggests Port-MIS ISMS concepts considering various factors such as work characteristics that actively perform logistics work at port logistics companies based on the conventional ISMS in order to build Port-MIS ISMS, physical locations, main assets, and technologies. This research also suggests the build plans for these concepts. Accordingly, Port-MIS ISMS suggested in this research establishes ISMS in order for logistics-related companies to secure their information from other parties and to efficiently perform information security activities and work. In addition, this research hopes to improve security levels by allowing the ISMS of port logistics companies to be established and operated within an appropriate range. Moreover, this research hopes to contribute to authentication policy activation by supporting the companies that are preparing to obtain authentication. In the future, the application and evaluation of cooperation based on Port-MIS ISMS are expected through the development of an information-security weakness diagnosis system of Port-MIS.

Acknowledgements. This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIP) (No. 2015R1D1A1A0106111 5).

REFERENCES

[1] T. D. Kim, The research regarding an information system risk management process modeling, *Journal of the Korea Society of Computer and Information*, vol.11, no.6, pp.157-164, 2006.

[2] S. S. Jang and S. C. Ko, An empirical study on the effects of business performance by information security management system, *Journal of Information and Security*, vol.15, no.3, pp.107-114, 2015.

[3] KISA, *Information Security Risk Management Guide*, 2004.

[4] K. H. Kwon and J. Y. Kang, Thoughts on security system to ensure safety of port logistics, *Han Yang Law Review*, vol.29, no.4, pp.301-322, 2012.

[5] M. J. Kim and S. S. Shin, A study on the evaluation of the service quality of Port-MIS, *Journal of Korea Port Economic Association*, vol.29, no.2, pp.211-238, 2013.

[6] L. Urciuoli, Port security training and education in Europe – A framework and a roadmap to harmonization, *Maritime Policy & Management*, vol.43, no.5, pp.580-596, 2016.

[7] E. Moulton, Policing the waterfront: Networks, partnerships and the governance of port security, *Police Practice and Research*, vol.16, no.4, pp.356-357, 2015.

[8] T. H. Kang and S. Y. Ryu, Financial information system, risk management, predictive risk model, *Information Systems Review*, vol.14, no.2, pp.103-115, 2012.