Multidisciplinary
SCIENTIFIC JOURNAL OF
MARITIME RESEARCH

University of Rijeka
Faculty of Maritime
Studies Rijeka

Multidisciplinarni
znanstveni časopis
POMORSTVO

Modeling of economically sustainable information security management systems in seaport clusters

Saša Aksentijević[1], Edvard Tijan[2], Dragan Čišić[3]

[1] Aksentijevic Forensics and Consulting Ltd., Gornji Sroki 125a, Viškovo, Croatia
[2] University of Rijeka, Faculty of Maritime Studies, Studentska 2, 51000 Rijeka, Croatia
[3] University of Rijeka, Faculty of Maritime Studies, Studentska 2, 51000 Rijeka, Croatia

ABSTRACT

The paper researches the usage of ARIS Express process modeling tool in creation of economically sustainable information security management system in seaport clusters. Basic concepts of information security in seaport cluster stakeholder's organizations are detailed, and relations and interactions between organizations and their environment are researched. Portfolio approach to information security is being endorsed along with quantification of total levels of the risk and the resulting cost of information security. The authors identify two basic process paths of information security in seaport clusters: basic activities and supporting activities. Furthermore, main components of both are being researched in detail, along with their interactions that create a robust system of information security management in seaport clusters. Process flow of all activities is constructed by using business process model implementation of ARIS Express software.

ARTICLE INFO

Preliminary communication
Received 14 March 2014
Accepted 28 March 2014

Key words:
Seaport clusters
Information security management
Business process modeling
ARIS

1. Introduction

ARIS approach to business process modeling provides methodology for process analysis and holistic approach to process design and action workflows. This paper will explore possibilities of usage of ARIS Express 2.4, a product from ARIS modeling software package range, in creation of solid, all-around model of information security management implementation in seaport clusters and involved stakeholders. ARIS line of products is a brand of German company IDS Scheer, acquired by Software AG in 2009 with dominant Business Process Modeling marketshare in Europe and well-positioned in the US market. Two distinct model blueprints will be used for this purpose – process landscape model and business process model.

ARIS Express is a freeware software from the line range used for introductory business process modeling, even though it also includes functionalities required to create extensive business process models that follow BPMN 2.0 standard – Business Process Model and Notation, a graphical representation used to specify business processes in a business process model. The goal of usage of ARIS Express is to provide a standard notation for representation and notation of necessary steps and resources to implement, operate and evaluate information security processes in seaport clusters, and especially to extent required by implementations of Port Community Systems (PCS). As of March 2011, current version of BPMN is 2.0.

In this paper, authors will prove that ARIS Express 2.4 is an appropriate tool for modelling process diagrams of information security in seaport clusters. Prior to that, all steps required for implementation of information security management system will be identified. The treatment of information security system implementation will not be purely technical in nature, it will also include exact risk assessment and financial impact on seaport cluster's operations.

This process model is aimed to ensure compliance of information systems in seaport cluster and all its stakeholders, both conventional and those built around the paradigm of Port Community Systems, with legal requirements, requirements of business certification and best practices in a way that is financially sound. It is also aimed to provide for algorithmic repetitiveness of the process to ensure further adjustments of that system to the eventual change in business processes, business requirements, changes in legislation and development of underlying technology.

2. Process paths of information security in port clusters

Seaport clusters are concentrations of various activities related to the seaport, and a powerful source of economic effects for the region that the cluster includes. [1; p. 373] Port community systems (PCS) are holistic, geographically bound information hubs in global supply chains that primarily serve the interests of a heterogeneous collective of seaport related companies [2; p.14]

Their complexity is derived from organizational requirements oriented towards the promotion of efficiency, ensuring the flawless transport of goods through seaport systems, compliance with local legislation and provision of stability and information flow security and business continuity while each entity included in the PCS maintains its own autonomy and self-sufficiency [3; p. 2].

Using ARIS Express business process modeling, two-tiered basic information security processes in seaport clusters are shown in Fig 1. Process landscape model specifies those processes in information security management system that are primary processes – they add value to seaport clusters information security. These processes are highest level processes, and they are interconnected in a functional sequence, creating a process landscape model of seaport cluster information security. These processes stand in a hierarchical order, and process oriented hierarchy is strictly maintained. Process line on the left side of the model is represented by processes executed in continuity, because information security management process is never complete, but in a constant state of evaluation due to change of characteristics or types of information assets, changes in the business process or external legal or formal certification (best practice) requirements.

On the right side of the model are supporting process line activities that provide support to the left side of basic process line activities of information security in seaport clusters. They are also set up in a hierarchical manner and are basically related to the activity of information risk assessment that is economically (financially) quantified, compared to the cost of incident occurrence. Based on this analysis, decision is made about investing or avoiding investments in information security measures (controls).

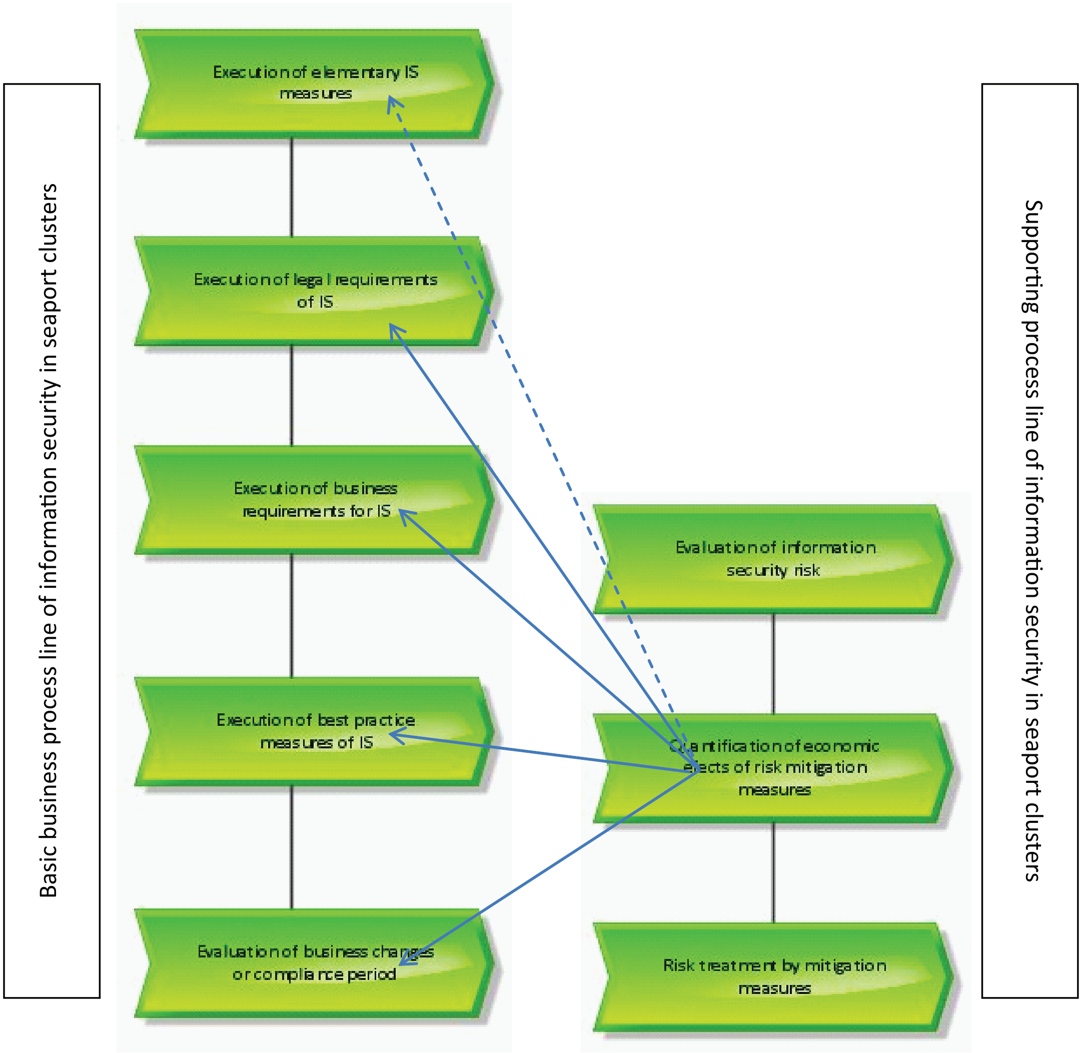

Basic business process line of information security in seaport clusters
Execution of elementary IS measures
Execution of legal requirements of IS
Execution of business requirements for IS
Execution of best practice measures of IS
Evaluation of business changes or compliance period
Evaluation of information security risk
Quantification of economic effects of risk mitigation measures
Risk treatment by mitigation measures
Supporting process line of information security in seaport clusters

Fig. 1 Basic and supporting process paths of information security in seaport clusters [4; p. 252]

Supporting process line activities are in fact executed in all processes of the basic information security process line in seaport clusters, except during the first activity (implementation of basic information security measures). These measures do not require significant investments, especially not compared to the remaining four processes. Focus of the implementation of these measures is on the elevation of management awareness in respect to importance of information security in business development and operations. As a part of implementation of these measures, the management clearly demonstrates that information security is one of the basic business functions, integrated in all other functions, whose proper implementation may have both positive and negative impact on business results. Therefore, risk assessment and quantification of financial impact of elementary measures of information security is not a supporting activity that should be implemented within the first process of the basic process line of information security. It is not realistic to expect that the management of the seaport cluster stakeholders is initially able to perform proper risk assessment analysis, financial evaluation and risk mitigation measures. Supporting process line will have its full impact only after all seaport cluster stakeholders reach a minimum level of knowledge and basic measures implementation, that is to say, when the information security becomes a key factor in the business case of each individual seaport cluster stakeholder.

Both process lines are equally applicable both in the initial implementation of structured information security process (if it did not exist before in an organized form) and later maintenance of the system, because the cycle itself is closed (endless), in line with PDCA cycle ("Plan-Do-Check-Act") of quality management in organizations [5]. Therefore, as part of relevant basic sub processes of information security management, procedures of supporting processes are being invoked in order to evaluate the exact levels of risk and financial impact of mitigating that risk to an acceptable level. Considering that implementation of risk controls to a portfolio of information security solutions always follows risk assessment, no information security measure in this model is implemented unless both technical and financial evaluations are completed. According to business process modeling requirements, in appropriate points of the model, operators that separate different branches of the process paths are being used, depending on whether certain requirements are being met or not, and then, execution activities (functions, using terminology of process modeling) are performed. The model also outlines all possible risks, documents, databases and deliverables that are used or produced during the execution of the process itself.

The model is constructed in a way to be process and methodology oriented, but it is not technology oriented. This notion has been respected from the inception of the model, considering that seaport cluster stakeholders sometimes do not have own or dedicated resources just for information security function, and information security is haphazard and often undertaken by management of operative instances that do not necessary expertise in the area of information security. Also, information security technology is subject to constant change and improvements in very short technology cycles and changes in risk and information asset types, so it is advisable to use this

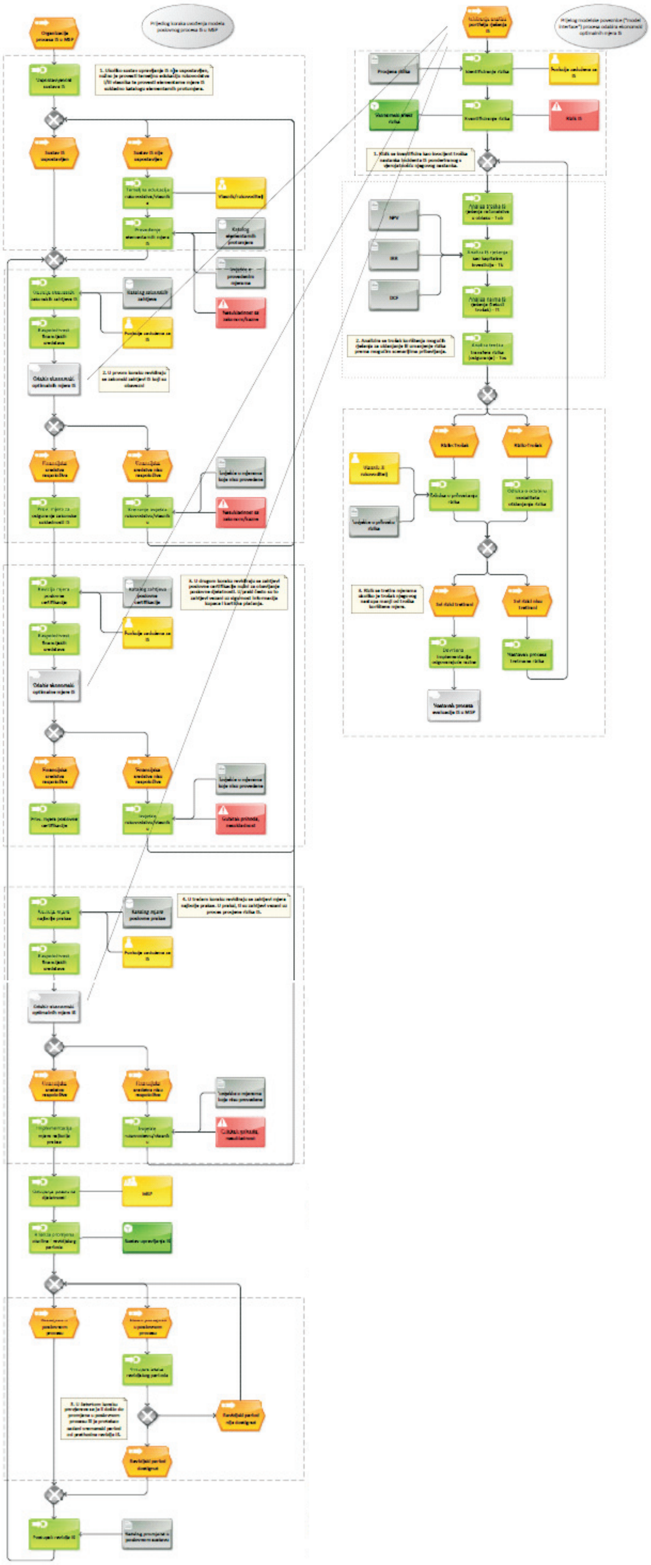

Organizacija procesa IS u MSP
Prijedlog koraka uvođenja modela poslovnog procesa IS u MSP
Sustav IS uspostavljen
Sustav IS nije uspostavljen
Vlasnik/rukovoditelj
Katalog elementarnih protumjera
Nesukladnost sa zakonom/kazne
MSP

Fig. 2 ARIS Express model of information security management in seaport clusters [4; p. 255]

approach in order to create a model that would be more resilient to technological and organizational changes.

From the description, it is obvious that exact material and organizational realities are not described in the model, except in a process path terminology. This is in order not to interfere with the managements' vision of development, already achieved level of development of information security, available financial resources, market position, business strategy and maturity level of business development. Functional borders of individual macro processes are outlined with dashed lines. In the following Fig 2. that shows the overall model of information security management in seaport clusters, there is a clear distinction between two vertices of process paths (**implementation of elementary information security measures** – left, and **supporting process path activities** – right).

3. Basic process path activities of information security in port clusters

Basic process line starts with the initiation of information security introduction in a seaport cluster, or some of its stakeholders. There are several possible motivators for this process and in case of a new organization, they are usually subjective because information security is rarely a core business activity in such organizations. In case of already existing (functioning) organizations, motivation can be found in the following:

- **Previous experience** of the management and inclination towards deployment of the basic information security measures,
- **Legal compliance requirements** in the area of information security; in case of smaller organizations these requirements are usually represented by the needs for protection of personal data,
- **Minimum certification system requirements** for information security, in reality usually because of credit card usage and payments,
- **Losses (unplanned cost**) caused by information security incidents,
- **Subjective factors** like **best practice** and comparable experiences of other organizations.

Five sub processes of the basic implementation of information security management system and three sub processes of supporting activities shown in fig 2. will be explained in details.

Macro sub process shown in fig 3. is equally applicable in case of initial implementation and later periodical evaluations. It includes checks that evaluate the need for repeated activities. The only activity that is not constantly monitored and repeated is the implementation of elementary information security measures and controls.

In case of **initial information security implementation**, it is possible to identify two distinctive activities:

1. **Elementary education of the management.** The purpose of this activity is elementary introduction of the management to the model of information security management in seaport clusters, advantages of its utilization, possibilities of risk measurement, connection between perceived risk levels and investment required to mitigate the risks, operational cost, and possible and foreseeable consequences of information security incidents. A part of elementary education is also understanding of basic concepts and terminology of information security, overview of the best practice models and certification and identification of those legal requirements that require organization's compliance. Education can be a self-initiated activity or a partially/fully outsourced activity.

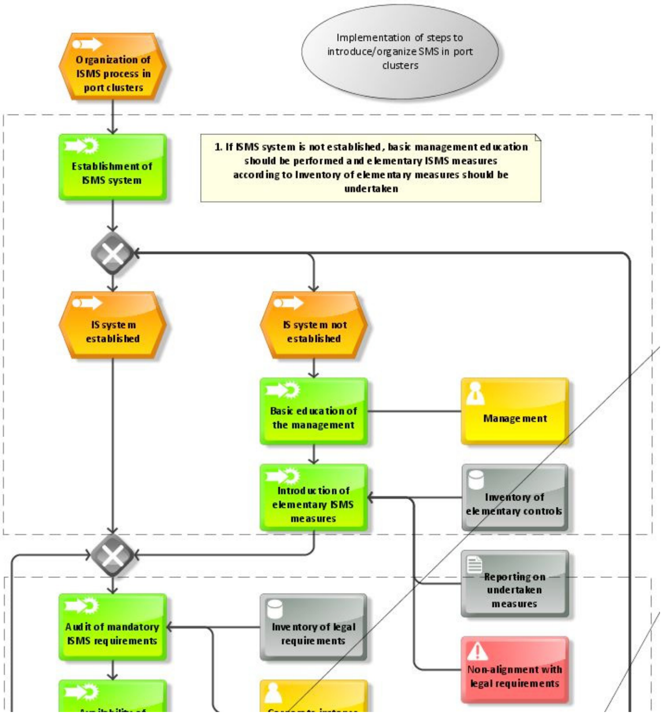

Implementation of steps to introduce/organize SMS in port clusters
Organization of ISMS process in port clusters
Establishment of ISMS system
1. If ISMS system is not established, basic management education should be performed and elementary ISMS measures according to Inventory of elementary measures should be undertaken
IS system established
IS system not established
Basic education of the management
Management
Introduction of elementary ISMS measures
Inventory of elementary controls
Reporting on undertaken measures
Audit of mandatory ISMS requirements
Inventory of legal requirements
Non-alignment with legal requirements

Fig. 3 Introduction of elementary measures of information security [4; p. 259]

2. **Execution of basic information security measures in seaport clusters.** Similar to elementary education of the management, this measure can be insourced, or partially or fully outsourced. Basic information security measures can be implemented without significant related investment or operational cost. Their importance is very high and they also include those measures that are aimed towards the promotion of information security culture in various seaport cluster stakeholders. Quantity and extent of basic measures depends on several factors. The most important among them is the influence of technical and technological related risks that is exerted on organization's information systems. It would be highly advisable that an **inventory of basic measures of information security** for seaport clusters is maintained by an independent body. Final deliverable of this process is the creation of the **report on non-implementation of ISMS measures**.

In Fig. 4, a process of **implementation of legally required measures** related to information security in seaports is shown in detail. In the beginning of this phase, the seaport cluster's management has demonstrated that it is dedicated to execution of measures of information security by implementation of basic measures of information security. However, no risk assessment has been done yet, there is no financial evaluation of investments or calculation of operative costs. Within the borders of this macro process, the basic activity is checking of compliance with legal requirements gathered in the second repository whose existence this model anticipates – **inventory of legal requirements**. It is quite customary in this phase of implementation that the management has already identified a person or instance in charge for coordination and organization of measures of information security. However, this is not a mandatory activity because information security coordination and management is a business process that has to be treated more as function than something pertinent to a single role or person. After the audit (effectively, creation of list of legal requirements that carry the need to create and implement information security controls), for the first time in the model flow a supporting process path is invoked in order to select financially optimal measure of information security. This activity also includes risk assessment, but this particular activity is rather simple because measured by a single incident occurrence it is equal to legal penalty for non-compliance. Availability of financial resources for measure implementation is not a part of the supporting process path: its end result is the selection of optimal measure (information security control) and form of its implementation (**cloud solution, as investment, as a service or risk transference**). Comparison with budgeted financial value is executed in the basic process path. In case that such financial resources are available, selected measures are implemented. This model anticipates certain reality that some seaport cluster stakeholders will not have available financial resources adequate to ensure legal requirements. For this reason, end result of this process is a document – **report on measures undertaken to ensure legal compliance.** In each next iteration of the process, on the top of the list of measures to be implemented are those measures related to legal compliance that were not previously implemented because of lack of funds.

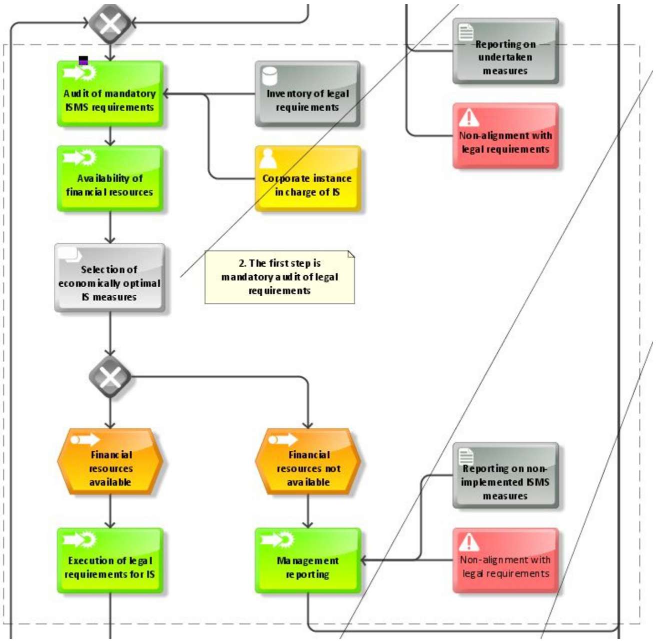

Reporting on undertaken measures
Audit of mandatory ISMS requirements
Inventory of legal requirements
Non-alignment with legal requirements
Availability of financial resources
Corporate instance in charge of IS
Selection of economically optimal IS measures
2. The first step is mandatory audit of legal requirements
Financial resources available
Financial resources not available
Reporting on non-implemented ISMS measures
Execution of legal requirements for IS
Management reporting
Non-alignment with legal requirements

Fig. 4 Macro process of ensuring compliance with legal requirements of information security in port clusters [4; p. 261]

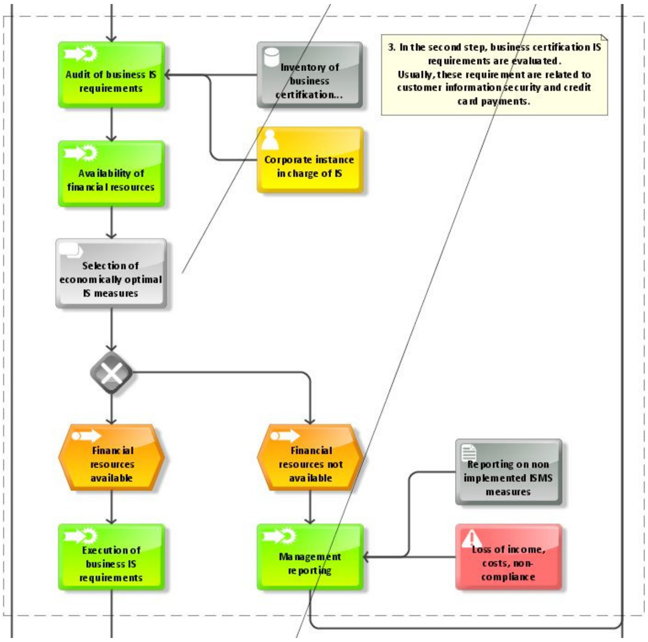

Audit of business IS requirements
Inventory of business certification...
3. In the second step, business certification IS requirements are evaluated. Usually, these requirement are related to customer information security and credit card payments.
Corporate instance in charge of IS
Availability of financial resources
Selection of economically optimal IS measures
Financial resources available
Financial resources not available
Reporting on non implemented ISMS measures
Execution of business IS requirements
Management reporting
Loss of income, costs, non-compliance

Fig. 5 Evaluation of business certification requirements [4; p. 262]

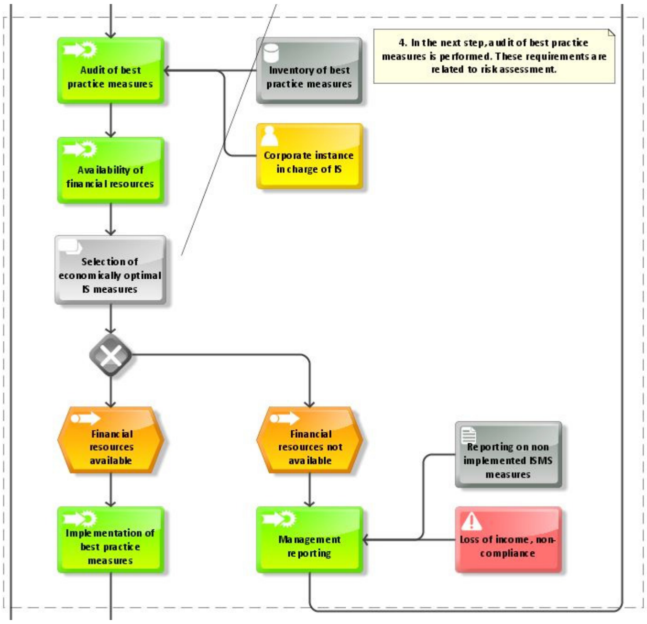
The next step of the process is shown in Fig. 5 – **evaluation of business certification requirements**. Business certification requirements are special measures required by seaport cluster's vendors or clients to endorse uninterrupted business activity by raising levels of information security. Implementation of these measures is also aimed at protection of cooperation and information systems of the clients and other stakeholders. In this model, it is possible to identify two basic sequential activities: **creation of the catalogue of measures of business certification** and **analysis of available financial resources** to implement those information security controls identified within supporting process path of economic evaluation of information security measures. In case that a seaport cluster derives business certification requirements from several sources, the function in charge of information security has to ensure that comparable or identical measures are implemented only once. This activity requires comparative analysis of requirements of two or more business certification systems.

In case that financial resources are available for implementation of business certification measures, related solutions are procured and implemented. In case that financial resources are not available, a **report on non-compliance**

with required business certification requirements is created for the management and this document represents the output of the process. Risk occurrence consequence can be also identified at this stage – loss of income caused by non-compliance with business certification requirements. As with legal requirements, in the next iteration of the process the accent is given to those measures that are not implemented in previous iteration because of lack of funds.

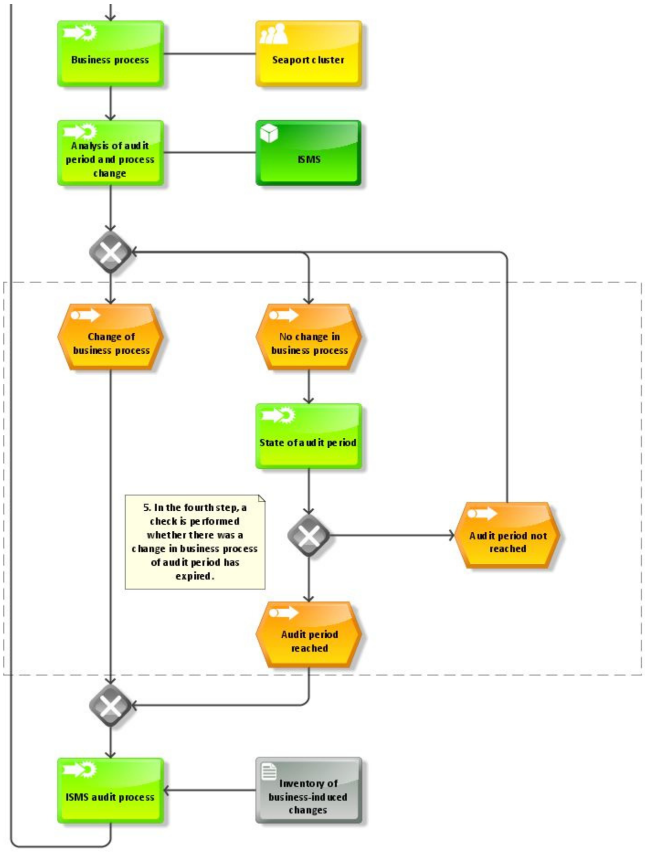
As it is clearly visible from the model, second and third macro-process of the information security in seaport clusters includes a feedback loop to the beginning of the sub-process that is currently implemented in order to include all identifiable risks by implementation of legal compliance and professional certification. After all identified risks are mitigated, the model continues towards the next macro-process: **implementation of the best practice measures of information security**. At this point, the seaport cluster has already covered a long way from implementation of elementary measures, compliance with legal requirements and business certification, risk assessment and creation of reports related to those measures (controls) that are identified but not implemented because of lack of funds. Process of implementation of measures of the best practice is the most similar to those measures used in the management of information systems management system within the quality management systems. This model defines another repository – **inventory of best practice measures.** This inventory can be taken over from best practice systems or closed formal certification systems, or it can be constructed internally, using own seaport cluster's knowledge and experience in information security management. In this step of the main process path, supporting process path is also being invoked to evaluate risk and financial effects of implementation of the best practice measures. Output document of this process is the **report detailing those measures that are necessary but not implemented**, while the process itself is also circular until all best practice measures are implemented. In this stage of implementation of information security management system in seaport clusters, total levels of residual risk are clearly identified.

The fifth step of implementation of information security model in seaport clusters, shown in Fig. 7, is a subprocess in which **criteria for the next iteration** of the basic process path are clearly established. After initial and iterative implementation of measures of information security according to the inventory of basic measures, legal requirements and best practice is completed, the management has to repeat the whole process in set or predetermined time cycles. Usually this time frame is one year. Except in complex changes of the business process or legal requirements, it is expected that following iterations will require less and less time and resources (and less implemented measures). Seaport cluster stakeholders should carefully evaluate whether changes in the business process have resulted in increased or decreased information security requirements. Even if there were no significant changes in business processes or organization, this activity is important for the process approach, maintenance of the corporate culture of information security and organization of this function. This cycle is repeated **until set audit time period is reached**, or **until there is significant**


Audit of best practice measures
Inventory of best practice measures
Availability of financial resources
Corporate instance in charge of IS
Selection of economically optimal IS measures
Financial resources available
Financial resources not available
Reporting on non implemented ISMS measures
Implementation of best practice measures
Management reporting
Loss of income, non-compliance

4. In the next step, audit of best practice measures is performed. These requirements are related to risk assessment.

Fig. 6 Evaluation of the best practice requirements [4; p. 264]


Business process
Seaport cluster
Analysis of audit period and process change
ISMS
Change of business process
No change in business process
State of audit period
Audit period not reached
Audit period reached
ISMS audit process
Inventory of business-induced changes

5. In the fourth step, a check is performed whether there was a change in business process of audit period has expired.

Fig. 7 Evaluation of the state of audit period and changes in business process [4; p. 265]

change in organization of business processes in seaport clusters and the next risk assessment becomes necessary.

According to the described model, an **internal inventory of business-induced changes** is necessary as a formal repository. This is a tool used by the management to evaluate current state of the information assets and whether changes in the business process had such impact and influence that there is a need for the process to be repeated.

4. Supporting process path activities of information security in seaport clusters

there are **three distinctive sub-processes** that constitute the **supporting process activity path** of information security in seaport clusters. This process path is a procedure called during macro-processes of ensuring compliance with legal requirements, business certification requirements and best practice measure implementation. The supporting process path is invoked every time there is a need to assess financial impact and appropriateness of implementation of information security measures (controls) in seaport clusters. This particular process path contains three separate macro-processes: **risk assessment, quantification of financial effects of risk mitigation, and risk treatment using selected mitigation measures.**

The first process is shown in Fig. 8. It is an **initial supporting macro process** of information security in seaport clusters. Its goal is to identify whether the implemented measures of information security are adequately addressing legal requirements, business certification requirements and best practice requirements of information security, by checking and comparing existing portfolio of information security measures towards set requirements. Risk levels are identified using risk assessment activities and then the risk is quantified in monetary terms. Risk quantification determines a range of expected financial impacts the information security incident occurrence might have on the organization's cash flow in case when mitigation measures are not implemented, and vulnerability of a certain information asset is identified. The product element of this process diagram is **financial impact – economic (financial) representation** of the identified risk.

In order to quantify all mitigation measures, it is necessary to analyze alternatives applicable to the same measure (control) of information risk, both in operative form and financial impact sense. It is possible to identify four different delivery forms of information security controls in seaport clusters:

- **cloud-based** information security solutions
- **information security investments**
- **leased information security** solutions
- **risk transfer** (insurance)

These possibilities are shown in Fig. 9.

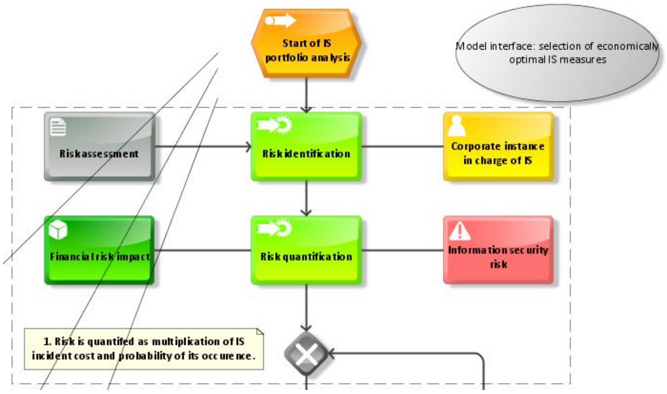

Start of IS portfolio analysis
Model interface: selection of economically optimal IS measures
Riskassessment
Risk identification
Corporate instance in charge of IS
Financial risk impact
Risk quantification
Information security risk
1. Risk is quantifed as multiplication of IS incident cost and probability of its occurence.

Fig. 8 Risk assessment of information security in seaport clusters [4; p. 267]

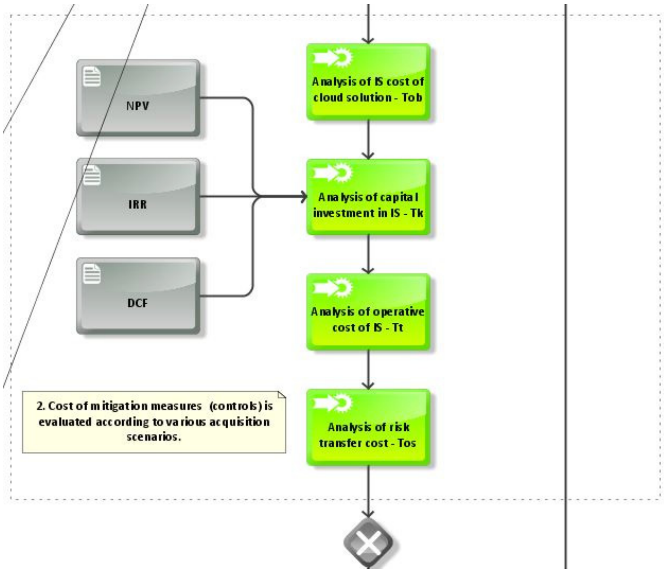

NPV
IRR
DCF
Analysis of IS cost of cloud solution - Tob
Analysis of capital investment in IS - Tk
Analysis of operative cost of IS - Tt
Analysis of risk transfer cost - Tos
2. Cost of mitigation measures (controls) is evaluated according to various acquisition scenarios.

Fig. 9 Quantification of financial impact of risk mitigation measures in port clusters [4; p. 268]

Outgoing result of this process are **financial indicators clearly comparing alternative sets of measures** that are equally mitigating identified risks at a desired level. The management has to take special care not to compare different measures that provide partial or different-level risk mitigation, but to compare those measures that provide same level of risk mitigationion. Furthermore, this process is important because it provides several possibilities of achieving the same goal while optimizing seaport cluster's cash flow, depending on the business goals and policies related to implementation of solutions: analysis of the investment is represented by three (or more) indicators derived from analysis of **net present value, internal rate of return and time preference of money** invested in information security solution (risk control). In case that seaport cluster's management prefers investments, they can choose the purchase of particular solution, while in case that they prefer cash flow optimization and they are not preoccupied by depreciation cost (tax credit), they can select a measure implemented as a cloud solution or one paid in installments as a service. Risk transference cost of information security through insurance is not yet particularly developed, especially not in Europe, but there are indicators it will become more prevalent in near future. [6; p. 14]

The final step of the supporting process path of information security in seaport clusters is **risk treatment by selected measures** (controls) of information security. This macro process is a final process before the process line transfers the process back to the basic process path of information security implementation process, where it was invoked from. The process is shown in fig 10. Input parameters of this macro process are previously clearly identified risks, their financially quantified impact, mitigation possibilities and all possible ways to mitigate risks using controls (using own financed assets through investment process, operative cost in form of leasing, rental or software as a service concept, cloud computing or risk transference – insurance). Main goals of this macro process are the following:

Financially quantified risk as compared to the implementation cost and decision about financial feasibility is reached. In case that quantified risk is lower than the cost of mitigation measures, it is not financially viable to implement that particular measure. This type of decision must be formalized in risk acceptance by the management.

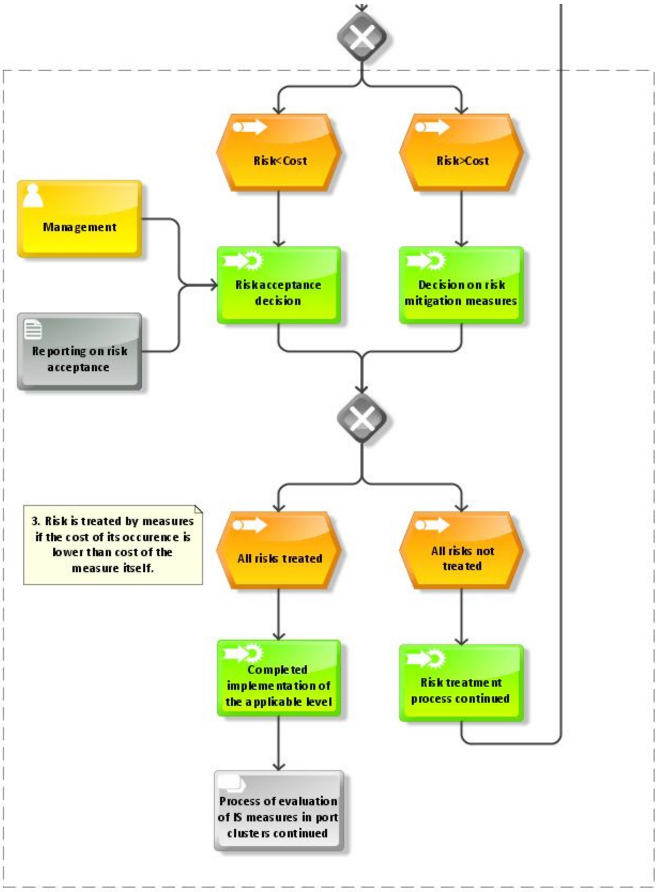

Risk<Cost
Risk>Cost
Management
Risk acceptance decision
Decision on risk mitigation measures
Reporting on risk acceptance
3. Risk is treated by measures if the cost of its occurence is lower than cost of the measure itself.
All risks treated
All risks not treated
Completed implementation of the applicable level
Risk treatment process continued
Process of evaluation of IS measures in port clusters continued

Fig. 10 Information security risk treatment in seaport clusters [4; p. 270]

Inside this macro process, an additional evaluation is performed, whose goal is to assess **if all relevant information security risks in seaport clusters are treated or not**. If not, the process continues until all risks are treated.

All output results of the risk quantification macro process have to be treated as temporary because of changes in the business process in seaport clusters, changes in legal requirements, professional information security certification requirements and requirements of available best practice. Also, the number of various risks and mitigation measures tends to increase with time, while the cost of individual measure implementation tends to decline. These facts additionally support the existence and inclusion of the mechanism of periodical assessments and re-evaluations. Furthermore, this model of information risk management is also endorsed by changes in seaport clusters' environment, acquisition of additional information assets that carry more inherent vulnerabilities that can be exploited by threats, especially if they are a part of seaport cluster's development or information systems development projects.

With this step, both process paths (basic and supporting) of information security management process are described in detail and completed. They are **based around cyclical activities, several external catalogues of required information and a limited set of internal products** inside process paths, aligned to produce best results in selection of appropriate information security risk mitigation measures that are financially quantified and support the business case.

5. Conclusion

Seaport clusters are an expression of strategic planning and aggregation of activities and stakeholders' efforts in seaport areas. Each of the stakeholders brings in the community its own distinctive information system, with inherent characteristics that have impact on the information security process, described in terms of information assets, vulnerabilities, threats and imposed risks. Furthermore, the blueprint for information security in seaport clusters becomes even more complicated if information systems of seaport clusters are formed as Port Community Systems – a form of integrated business information systems specially tailored for seaport operations.

In the research, the basic premise was the usage of business process management methodology and creation of models that describe organizational structures, application systems, data and processes that form information security management in seaport clusters. ARIS Express application platform was used for modeling and two different model sets were created: macro outlook at the basic and supporting information security process paths was created using process modeling, while granular approach was then used by further analysis of both process paths into sub-processes.

Basic process path of information security in seaport clusters is a circular, repetitive process path inside of which four different macro processes of information security can be identified: implementation of elementary measures of information security, implementation of measures aimed towards alignment with legal requirements, alignment with professional certification requirements and, finally, compliance with best practice. All of these macro processes use appropriate catalogues of elementary measures, professional certification measures, legal requirements and best practice requirements, maintained by a professional authority. Execution of business processes within macro processes of the basic path procedurally calls supporting (auxiliary) process path, engineered to provide financial analysis and risk assessment of information security controls to be implemented in the information security management system. It is possible to identify three different processes that are a part of the supporting process path: risk assessment, selection of the form of risk mitigation and financial impact analysis.

Overall process of information security management in seaport clusters is circular in nature, and in line with quality management systems that use PDCA ("plan-do-check-act") methodology. The next iteration of the implementation is triggered either by a change in business processes in seaport clusters, or expiration of the verification timeframe (usually one year). This approach allows for incorporation of all possible changes in seaport clusters' information systems that have impact on information security.

ARIS Express proved to be an appropriate tool for the modeling purposes because its usage allowed for graphical representation and understanding of basic and supporting process paths of the information security in seaport clusters. Further developments and research on this topic could be in the area of implementation of BPMN 2.0 notation in creation of detailed process descriptions of different macro processes and process paths of information security.

References

[1] Agatić, A., Čišić, D., Tijan, E. "Information management in seaport clusters", Pomorstvo: Scientific Journal of Maritime Research, Vol. 25, No. 2, December 2011.

[2] Srour, F. J., et al., "Seaport community system implementation, lessons learned from international scan", Transportation Research Board 87th Annual Meeting, Washington DC, 2008.

[3] Rodon, J., J Ramis-Pujol, "Exploring the Intricacies of Integrating with a Seaport Community System", 19th Bled eConference, Bled, Slovenia, June 5 – 7, 2006.

[4] Aksentijević, S, "Sustainable economic model of information security management in small and medium enterprises", doctoral dissertation, Faculty of Economy, Rijeka, Croatia, March 2014. (Unpublished)

[5] Miles, F., "Adapting the Deming Cycle to the Management Process", Production Machining, 18.06.2012., ttp://www.productionmachining.com/articles/adapting-the-deming-cycle-to-the-management-process (accessed 04.04.2014.)

[6] "Incentives and barriers of the cyber insurance market in Europe", European Network and Information Security Agency (ENISA), Heraklion, Greece, June 2012.