CYSM: An Innovative Physical/Cyber Security Management System for Ports

Spyridon Papastergiou[1(✉)], Nineta Polemi[1(✉)], and Athanasios Karantjias[2]

[1] Department of Informatics, University of Pireaus, Karaoli and Dimitriou 80, 18534 Pireaus, Greece
{paps,dpolemi}@unipi.gr

[2] Information Management Department, SingularLogic S.A., Al. Panagouli and Siniosoglou St., 14234 Nea Ionia, Athens, Greece
tkarantjias@singularlogic.eu

Abstract. The goal of the paper is to describe the main results of a European research project, namely CYSM, (The authors serve as technical managers of the CYSM project.) which is oriented to address the security and safety requirements of the commercial ports' Critical Information Infrastructures (CII). It aims to introduce an integrated security management system (for port operators) enabling asset modelling, risk analysis, anticipation/management of attacks, as well as stakeholders' collaboration. The proposed system helps port to identify, assess and treat their security and safety problems in an efficient, harmonized and unified manner.

Keywords: Security · Safety · Port's risk assessment

1 Introduction

Ports support a number of business processes that are complex, diverse and involve various external entities (e.g. maritime companies, ministries, banks, other Critical Information Infrastructures -CII-). These operations rely not only upon the physical infrastructures of the ports (e.g. terminals, gates, storage houses) but more substantially upon their ICT infrastructure (e.g. networks, telecom/ICT systems, data, users). The resilience of their infrastructure to complex, persistent and fierce attacks is a primary requirement to guarantee their business continuity.

The adopted ports' security management approaches are ineffective in addressing and treating physical and cyber risks, imposing the need for a holistic and unified approach to secure their dual nature [11]. Usually, a contributory analysis of the inherent risks takes an inordinate amount of operational effort, considering the complexity of the underlying infrastructure and the fact that the security and safety requirements are evolving rapidly. Therefore, it is essential to have a comprehensive and integral approach that facilitates and optimizes the proactive risk identification and treatment of the ports' ICT and physical related risks and threats from an integrated perspective. A holistic methodology for managing security and safety risks could help ports to check their compliance with existing legal, regulatory and standardization regime (e.g. ISO27001

T. Tryfonas and I. Askoxylakis (Eds.): HAS 2015, LNCS 9190, pp. 219–230, 2015.
DOI: 10.1007/978-3-319-20376-8_20

[3], ISO 28005 [5, 6], ISPS code [1, 2]), to detect possible violations and gaps and finally to adapt new regulations and directives.

The authors of this paper share the view (of the European Project CYSM [12]) that the evaluation and mitigation of the cyber and physical risks should not rely only upon highly personalized experience and expertise. It should be an inherently rational and collaborative process that engages corporate personnel with different roles, responsibilities and technical capabilities (e.g. administrators, security officers, maintenance personnel, security guards etc.) and external users, utilising diverse perspectives, knowledge and experiences in order to produce and provide well-defined, acceptable and reliable proofs and information that facilitate the identification and evaluation of potential threats and weaknesses and the estimation of the ports' infrastructure resilience.

Toward this direction, the paper contributes to the effective protection of the ICT and physical ports' infrastructure, by proposing an innovative, evolutionary and sophisticated Collaborative Cyber/Physical Security Management (CYSM) system that helps ports to assess their facilities and revise their risks mitigation plans. This system provides the opportunity to better understand, interpret and finally deal with their security and safety related risks. The paper outlines results from the CYSM project [12] and it is structured as follows: Sect. 2, provides a desk-research analysis and assessment of the available risk management approaches and the existing legal and regulatory framework related to ports' CIIs. Section 3, provides a brief overview of the capabilities and the supported functionality of the proposed Collaborative Cyber/Physical Security Management System, CYSM. The paper concludes with Sect. 4, outlining the most innovative features of CYSM and draws conclusions and directions for further research.

2 Ports' Security and Risk Management Approaches

The main goal of risk management is to protect business assets and minimize costs in case of failures and thus it represents a core duty of successful corporate governance. Hence, risk management describes a key tool for the security within organizations and it is essentially based on the experience and knowledge of best practice methods. These methods consist of an estimation of the risk situation based on the business process models and the infrastructure within the organization. In this context, these models support the identification of potential risks and the development of appropriate protective measures. The major focus lies on companies and the identification, analysis and evaluation of threats to the respective corporate values.

The outcome of a risk analysis is in most cases a list of risks or threats to a system, together with the corresponding probabilities. International standards in the field of risk management are used to support the identification of these risks or threats as well as to assess their respective probabilities. These standards range from general considerations and guidelines for risk management processes (e.g. [14–16]) to specific guidelines for the IT sector (e.g. [4, 17–20]) all the way to highly specific frameworks as, for example, in the maritime sector (e.g. [1, 2, 21]). Most of these standards specify framework conditions for the risk management process, but rarely go into systematic, homeomorphic risk analysis methods; making a direct

comparison of the results difficult. Furthermore the above-mentioned efforts are not sector-specific; as a result they are too generic and difficult to in the complex maritime sector.

In principle, selecting an appropriate method and tool for risk evaluation proves to be complicated. In recent years, a number of methods, algorithms (OCTAVE [22, 23], EBIOS [24], MEHARI [25], CORAS [26], NIST [27], ISAMM [28], STORM-RM [30]) and tools (CRAMM [29], S-PORT [10, 31]) have been evolved from research, specially designed to protect the ICT infrastructure and related systems without holistically covering the dual nature (physical and cyber) of the ports CII.

In contrary to the aforementioned general and ICT-specific guidelines for risk management, the International Ship and Port Facility Security (ISPS) Code [1, 2] (as well as the respective EU regulation [21]) defines a set of measures to enhance the security of port facilities and ships, putting emphasis on the physical facilities and the organizational aspects of security not covering sufficiently the cyber facilities and ports' ICT assets. Additionally, a number of risk management methodologies and tools [32, 33] exist, compliant with ISPS but not with the cyber related security standards (e.g. ISO27001, 27005).

3 CYSM Risk Assessment System

This section introduces the collaborative cyber/physical security management, system, CYSM for identifying, classifying, assessing and mitigating risks associated with ports' CII raised by security and safety incidents. This approach has been developed based on a number of customized and specialized self-management functions that aim to optimize, merge and enhance the existing approaches identified in the previous Section. The Section provides an in-depth analysis of the CYSM system, presenting the supported functionality and the adopted processes.

3.1 CYSM Goals and Services

The CYSM system [8, 9] - is an innovative, scalable Risk Assessment Toolkit, which facilitates the ports' security team to efficiently identify, assess and treat their security and safety incidents involving all port operators and users. The toolkit adopts and implements a bouquet of flexible and configurable self-driven functions and procedures [7] which constitute the conceptual pillars for building a solution that assists ports to improve their current cyber and physical level and:

- incorporates a conformance approach that checks and defines the compliance of the ports against the requirements, rules and obligations imposed by a set of security management standards (ISO 27001, ISPS) and the relative security and safety legal and regulatory framework;
- implements a collaborative, multi-attribute, group-decision making algorithm that collects the diverse security-related knowledge located in the ports and the results (e.g. threats, vulnerabilities metrics, prioritization of countermeasures) produced by the automated and semi-automated risk assessment routines and processes in order

to: (i) determine the value of the information assets; (ii) identify the applicable threats and vulnerabilities that exist (or could exist); (iii) identify the existing controls and their effect of the identified risks; (iv) determine the potential consequences; and (v) prioritize the derived risks and ranks them against the risk evaluation criteria set in the context establishment.
- integrates a security policy growing mechanism that provides a flexible way for creating and updating customized security policies and procedures;
- implements a social, collaborative working environment, which facilitates and encourages the ports to jointly work and cooperate, by exchanging ideas and information pertaining to security and safety issues and by allowing them to reach targeted solutions in a collaborative and time effective manner.

The aforementioned elements are combined in an effective and efficient manner to develop the automated routines and workflows that comprise and construct the meaningful CYSM Security Assessment Services [8, 9] i.e. Cyber Risk Assessment Services (CRAS), Physical Risk Assessment Services (PRAS) and the Security Framework Service (SFS). These services are fully customizable depending on the ports' security profile (like the enterprise size, the interdependencies with other IT systems, the services offered, the number of administrators and the security and safety awareness level), covering various aspects such as complexity, automation, terminology, simplification and understanding.

3.2 CYSM System Components

In order for CYSM to meet its objectives, it integrates a set of primary components (Fig. 1). From a conceptual perspective, the main components are the following:

- Community Portal: this area is accessible by all users of the involved ports and comprises of:
  - *Collaboration* suite: encapsulates a set of specialized Web2.0 elements (e.g. blogs, forums) suitable for e-collaborate, collecting and sharing knowledge. These elements enable ports to work together in building open working groups, providing diverse opinions, thoughts and contributions and sharing information, experience and expertise.
  - *e-Library*: acts as the knowledge source of all ports' physical and cyber related information (e.g. European legal and regulatory framework, security related standards, specifications, methodologies and frameworks).
- Port Private Portal: this area provides the appropriate functionality that enables the users to assess and improve the security and safety level of their port's infrastructure. Actually, this area executes the risk assessment processes and routines integrated in the system and consist of the following modules offering the corresponding services:
  - Port *collaboration* suite: encourages and facilitates members of each port to closely cooperate and exchange information and ideas during the risk assessments.
  - Port *e-Library*: is an inventory of confidential announcements, security and safety policies and procedures, guidelines etc.

- *Administration* module: allows customizing of the risk assessment's parameters (e.g. threats, vulnerabilities, controls).
- *Management* module: allows the initiation of a risk assessment.
- *Risk Assessment* module: gives the opportunity to the ports to identify and measure their threats, their vulnerabilities and possible impacts.
- *Security Policy* Reporting module: facilitates the formulation of customized security and safety-related policies and procedures.
- *Risk Assessment Results* module: allows the review of the risk assessment results and the formulation of a mitigation plan.

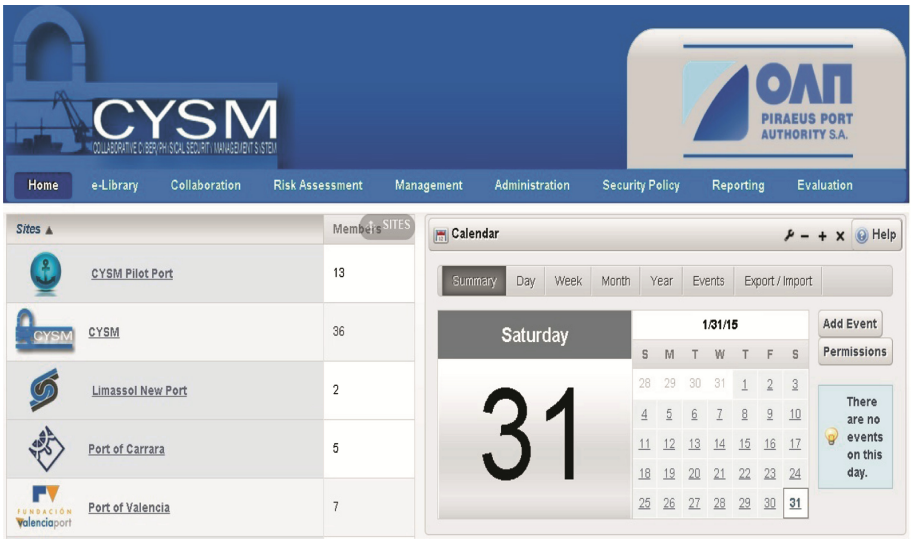

Fig. 1. Collaborative Cyber/Physical Security Management (CYSM) System

The above services are provided through customized intuitive and interactive Web Interfaces (including interactive screens, online forms, Dynamic Questionnaires) to represent the scenarios and steps as well as the information and content (e.g. requirements, rules, obligations, and recommendations of the standardization framework and regime) required by the supported risk self-assessment routines and functions, presented in the previous Section.

3.3 Showcase Scenario

The scope of this Section is to describe a use case in order to illustrate the functionality of the CYSM system. The scenario involves a commercial port, Piraeus Port Authority (PPA) that supports a number of business operations including the transport and accommodation of people, freight, natural gas, oil, cargoes and manufactured goods. For this reason, PPA manages and operates multiple and dispersed cyber (e.g. computer center) and physical (e.g. facilities for handling all types of cargoes) facilities. According to the

scenario, the Port Security Officer (PSO) of the PPA utilizes the CYSM System in order to identify, evaluate and manage the cyber and physical risks associated with the Cruising Facility of the port and to formulate a mitigation plan. The CYSM system guides and directs the PSO via dynamic, interactive and evolutionary interfaces to perform the evaluation process. This process can be divided into the following (5) five sub-processes:

A. Customization Phase

Initially, the PSO, authenticates himself (using his credentials) into the CYSM system. Upon approval the PSO gains access to the Community Portal and directed to the PPA Private Portal where he accesses the Administration module (Fig. 2). This module allows the PSO to set various boundaries and constraints, i.e.:

- select standards that will be used to perform the risk assessment (e.g. ISPS, ISO27001, both);
- define the correlation between the controls that can be applied from a port and the requirements imposed by the standards;
- customize the fundamental elements and parameters of the risk assessment procedure (e.g. the scales related to the likelihood of occurrence of the threats, the exploitation level of the vulnerabilities etc.);
- generate the list of threats possible for the port assessed;
- categorise the list of vulnerabilities;
- list the controls that are deployed or can be applied from the port in order to mitigate the risks and deal with their identified threats and weaknesses;
- define the correlation among controls, vulnerabilities and threats;
- classify ports' assets into categories and sub-categories based upon their nature (physical, cyber);

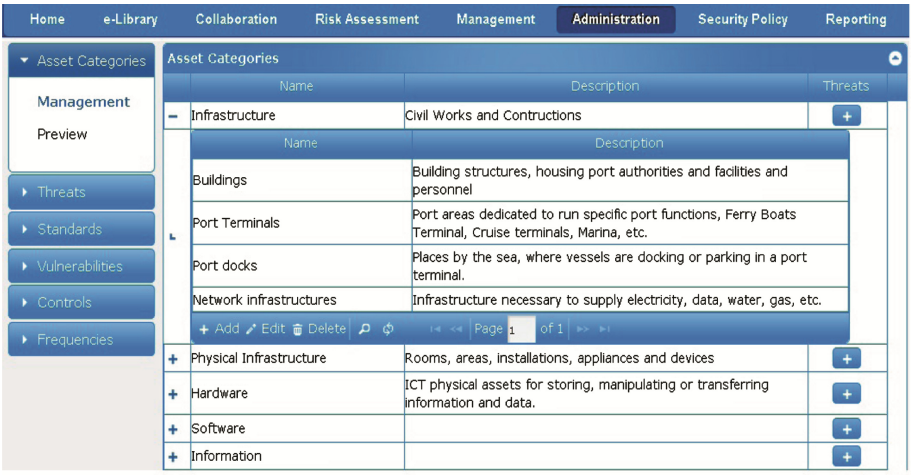

Fig. 2. Administration module

The PSO generates and updates the above mentioned information taking into consideration the literature, the port's particularities, the adopted technological solutions, the knowledge gained from the daily operation of the port, online repositories available from industry/standardization bodies, national governments etc.

B. Risk Assessment Initiation Phase

After the successful customization of the system, the PSO accesses the Management module (Fig. 3) where he is able to initiate a risk assessment. For the definition of a new assessment, the PSO should specify: (i) the basic information (e.g. name, the start and end date and a short description); (ii) the boundaries of the risk assessment (the physical or ICT port facility that will be assessed); (iii) the departments that will be involved and the role and weight of each department to the risk procedure; and finally (iv) the standards or the areas of the standards (ISO27001 and ISPS code) against which the defined area will be evaluated.

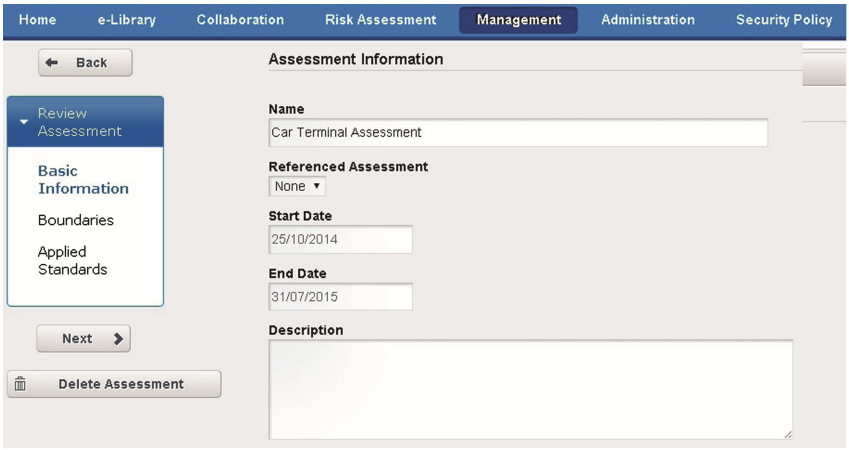

Fig. 3. Management module

C. Evaluation Phase

Having initiated the risk assessment, all members (participants) of the ports' departments, invited to participate in the risk assessment process, login to the CYSM system using their accounts and access the Risk Assessment module (Fig. 4) of the PPA Private Portal. In this module, a list of available assessments appears and the participants select the assessment related to the evaluation of the Cruising Facility (this selection serves as example) in order to complete the following steps:

i. *Assets Identification:* define the assets comprise the Cruising Facility and categorize them in the main categories (e.g. Infrastructure, Physical Infrastructure, Hardware, Software, Information) and sub-categories (e.g. terminals, docks, servers) defined in the Administration module.
ii. *Impact Assessment:* determine the value of each asset to the organization. In particular, they should define what are the consequences (e.g. financial losses, damage to

the reputation, legal consequences) of the loss of integrity, confidentiality and availability of each asset.

iii. *Control Identification:* define the controls applied to each asset.

iv. *Threat Assessment:* estimate the likelihood of occurrence of a predefined list of threats to each asset.

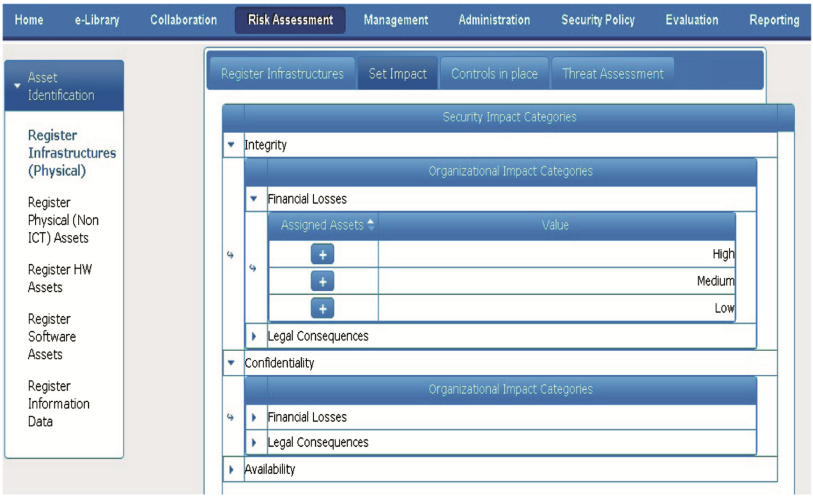

Fig. 4. Risk assessment module

D. Risk Assessment Results Calculation and Review Phase

Once all the participants completed the evaluation phase, the PSO accesses the Risk Assessment Results module (Fig. 5) in order to produce and review the results of the risk assessment. More specifically, the PSO selects the assessment that he is interested in and forces the system to calculate the potential risks associated with the Cruising Facility taking into consideration the answers of the participant completed the evaluation. Now, the PSO is able to review the produced results based on which he can select and prioritize the countermeasures that should be adopted by the PPA in order to handle and mitigate the identified risks. In this way, the PSO can formulate an effective and efficient risk mitigation plan.

E. Security Policy Reporting Phase

Finally, the PSO accesses the Security Policy Reporting module (Fig. 6) in order to formulate the security and safety policies required by the existing regulatory regime (ISO27001 and ISPS code). These policies can be exported in various formats (e.g. pdf, txt, jpg).

CYSM enables the ports to address their specific requirements, identify their specific threats that their assets may face, and meet their business goals by generating targeted security policies. The nature of the CYSM system is associated with a high degree of

Fig. 5. Risk assessment results module

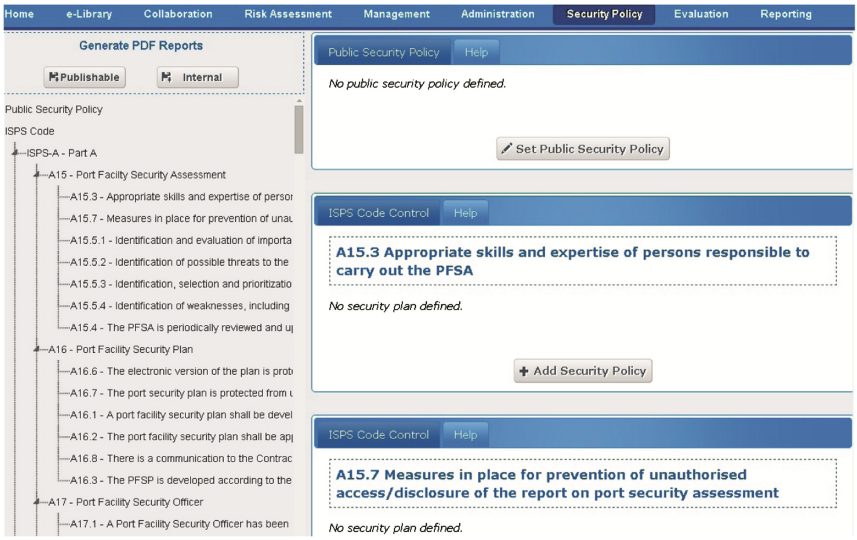

Fig. 6. Security policy reporting module

innovation since it implements new upgrading security and safety self-management functions and processes for the evaluation and mitigation of the risks and threats associated to the ports' infrastructure.

4 Conclusions

The CYSM system adopts a simplified and optimized approach as a response to the traditional time-consuming, not holistic risk assessment procedures. CYSM is represented by a number of automated, customized and specialized self-risk assessment processes and routines that are modeled and implemented in the system in a graphical manner using visualization tools and structured content. CYSM offers open source "easy-to use" tools enabling the security and safety management in intuitive and graphical way. In a Nutshell, the basic design principles of all the related functions developed within CYSM include:

- *Easy to use for non-experts.* Simplification and automation of the supported risk assessment procedures and activities making possible for the ports' personnel to conduct self-assessments.
- *Self-driven.* Deployment of the procedures without the need of external resources. The personnel of the ports are guided and directed through automated work-flows and routines and on-line intuitive and interactive graphical representations (e.g. dynamic questionnaires) to use the provided functionality.
- *Collaborative.* The risk assessment process is treated as a participatory challenge and activity involving various user groups with different roles, visions, and experience, expertise and business expectations, aiming at raising the security awareness, consciousness and responsibility.

The CYSM system has been tested and evaluated by a number of commercial ports (including Port of Piraeus, Valencia Port Authority and Port of Mykonos). During the evaluation operation various ports' users (e.g. Port Security Officers, Members of Ports' Security Teams, Ports administrators and internal users interacting with ports' ICT systems) have been engaged in risk identification, assessment and mitigation based on the on-line services of the CYSM system.

The authors, had identified an open problem, led by their involvement in CYSM, driven by the question: How can the ports identify and evaluate interdependent threats, evaluate risks and their cascading effects not only to their own CII but also to the other entities that interconnect and interact with them (e.g. supply chain business partners). Medusa[1] [13] is a running European Commission (E.C.) Project that aims to respond to this research question by providing a new risk assessment methodology compliant not only with the ISPS, ISO27001 (as CYSM) but also with the supply chain security standard (ISO28000), and extend the CYSM system to offer supply chain risk assessment modules to the ports and their supply chain business partners.

Acknowledgments. The authors are grateful to the E.C. Programme "Prevention, Preparedness and Consequence Management of Terrorism and other Security related Risks for the Period 2007-2013" for their support in funding the CYSM and MEDUSA projects. The authors also thank all CYSM partners (Port Institute for Studies and Co-Operation in the Valencian Region – FEPORTS, Singular Logic, Electrical, Electronics and Telecommunication Engineering and

[1] The authors serve as Project managers in this E.C. project.

Naval Architecture Department (DITEN) - University of Genoa (UNIGE), University of Piraeus Research Centre, Piraeus Port Authority (PPA), Fundacion Valencia Port (VPF)) and Medusa parners (University of Piraeus Research Centre, Singular Logic, University of Cyprus (UCY), EUROPHAR EEIG, Austrian Institute of Technology) for their contributions.

References

1. International Maritime Organisation: International Ship and Port Facility Security Code, London, UK (2004)
2. International Standardization Organization: Ships and marine technology – Maritime port facility security assessments and security plan development, Geneva, Switzerland (2007)
3. International Standardization Organization: ISO 27001: Information Security Management System Requirements, Geneva, Switzerland (2013)
4. International Standardization Organization: ISO 27005: Information security risk management, Geneva, Switzerland (2011)
5. International Standardization Organization: ISO 28000: Specification for security management systems for the supply chain, Geneva, Switzerland (2007)
6. International Standardization Organization: ISO 28001: Security management systems for the supply chain – Best practices for implementing supply chain security, assessments and plans – Requirements and guidance, Geneva, Switzerland (2007)
7. Makrodimitris, G., Polemi, N., Douligeris, C.: Security risk assessment challenges in port information technology systems. In: Sideridis, A.B., Yialouris, C.P., Kardasiadou, Z., Zorkadis, V. (eds.) E-Democracy 2013. CCIS, vol. 441, pp. 24–36. Springer, Heidelberg (2014)
8. Papastergiou, S., Polemi, N.: Harmonizing commercial port security practices & procedures in mediterranean basin. SSMDE: Secure and Sustainable Maritime Digital Environment. IISA 2014, pp. 292–297. Springer, Heidelberg (2014)
9. Karantjias, A., Polemi, N., Papastergiou, S.: Advanced security management system for critical infrastructures. IISA 2014. 43(1), pp. 136–158. Springer, Heidelberg (2014)
10. Polemi, D., Ntouskas, T., Georgakakis, E., Douligeris, C., Theoharidou, M., Gritzalis, D.: S-Port: collaborative security management of port information systems. In: Proceedings of the 4th International Conference on Information, Intelligence, Systems and Applications (IISA-2013). IEEE Press, Greece, July 2013
11. ENISA report: Cyber security aspects in the maritime sector. ENISA (2011). http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/dependencies-of-maritime-transport-to-icts
12. CYSM European Commission: Programme prevention, preparedness and consequence management of terrorism. CIPS (2012). http://www.cysm.eu/index.php/en/
13. MEDUSA: Multi-order dependency approaches for managing cascading effects in ports' global supply chain and their integration in risk assesment frameworks. European Commission, Programme Prevention, Preparedness and Consequence Management of Terrorism, CIPS (2014). http://athina.cs.unipi.gr/medusa/
14. International Standardization Organization: ISO 31000: Risk Management – Principles and Guidelines, Geneva, Switzerland (2009)
15. International Standardization Organization: ISO 31010: Risk management – Risk assessment techniques, Geneva, Switzerland (2009)
16. Austrian Standards Institute: ONR 49000: Risikomanagement für Organisationen und Systeme: Begriffe und Grundlagen. Wien, Österreich (2004)

17. International Standardization Organization: ISO 20000: information technology service management. Geneva, Switzerland (2005)
18. Bundesamt für Sicherheit in der Informationstechnik. IT-Grundschutz Kataloge (2013). https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html
19. The Stationery Office (TSO): Continual service improvement. ITIL V3 (2007)
20. Common Criteria Working Group: Common methodology for information technology security evaluation - evaluation methodology. CCMB-2007-09-004 (2007). http://www.commoncriteriaportal.org
21. European, Commission: Regulation (EC) No 725/2004 of the European parliament and of the council of 31 March 2004 on enhancing ship and port facility security. Off. J. Eur. Union **L 129**(6), 6–91 (2004)
22. Alberts, C.J., Dorofee, A.: Managing Information Security Risks: The Octave Approach. Addison-Wesley Longman Publishing Co., Inc., Boston (2002)
23. Alberts, C., Dorofee, A.: Operationally critical threat, asset, and vulnerability evaluation (Octave) method implementation guide, v2.0. Software Engineering Institute, Carnegie Mellon University (2001). http://www.cert.org/octave/
24. Expression of needs and identification of security objectives PREMIER MINISTRE Secrétariat général de la défense nationale Direction centrale de la sécurité des systèmes d'information Sous-direction des opérations Bureau conseil. www.ssi.gouv.fr
25. Clusif Methods Commission: MEHARI V3 risk analysis guide (2004)
26. EU Project Nr. IST-2000-25031: CORAS - risk assessment of security critical systems (2003). http://www2.nr.no/coras/
27. Stoneburner, G., Goguen, A., Feringa, A.: Special publication 800-30: risk management guide for information technology systems. Technical report, National Institute of Standards and Technology, Gaithersburg (2002)
28. Information Security Assessment & Monitoring Method (ISAMM). http://www.telindus.com
29. Insight Consulting: CRAMM User Guide, Issue 5.1, United Kingdom (2005)
30. Ntouskas, T., Polemi, N.: STORM-RM: collaborative and multicriteria risk management methodology. Int. J. Multicriteria Decis. Mak. **2**(2), 159–177 (2012)
31. Ntouskas, T., Polemi, N.: Collaborative security management services for port information systems. DCNET/ICE-B/OPTICS, pp. 305–308 (2012)
32. Balmat, J.-F., Lafont, F., Maifret, R., Pessel, N.: MAritime RISk Assessment (MARISA), a fuzzy approach to define an individual ship risk factor. Ocean Eng. **36**(15), 1278–1286 (2009). doi:10.1016/j.oceaneng.2009.07.003
33. SAFESEANET, a European platform for maritime data exchange between member states' maritime authorities, is a network/internet solution based on the concept of a distributed database. http://ec.europa.eu/idabc/en/document/2282/5926.html