CHAPTER 3

Security of Ports' Critical Information Infrastructures

The main concern of all organizations is to be able to identify their threats and estimate their risks, which is the main goal of risk management, i.e., to protect business assets (physical and cyber) and minimize costs in case of failures. Security management 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 the organizations (e.g., port authorities) for 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 to specific guidelines for the IT sector all the way to highly specific frameworks as, for example, in the maritime sector. Most of these standards specify framework conditions for the risk management process but rarely go into detail on specific methods for the risk analysis or risk assessment. This is one reason why differences in the risk assessment often arise within the specific areas of application, making a direct comparison of the results difficult. Furthermore, the aforementioned efforts are not sector specific; as a result, they are too generic and difficult to be applied in the complex maritime sector.

In principle, choosing the right method and the right tool for risk analysis and risk evaluation proves to be complicated. A huge emphasis in the security and risk management in the maritime sector is laid on the physical security. The International Ship and Port Facility Security (ISPS) Code (as well as the respective EU regulation) defines a set of measures to enhance

Port Cybersecurity
ISBN 978-0-12-811818-4
http://dx.doi.org/10.1016/B978-0-12-811818-4.00003-4

the security of port facilities and ships. Additionally, several methodologies and tools exist aimed at strengthening the safety level of the ports' infrastructures (physical risk assessment). Nevertheless, due to the increased interaction and exchange of port's information with other critical infrastructures in the maritime ecosystem (e.g., port authorities, ministries, maritime companies, ship industry, etc.) the sole focus on physical security is not sufficient anymore. In the same way, the security of the ports' ICT and physical-related components, elements, and systems becomes equally important.

However, by security management, we mean the effective implementation, establishment, assessment, monitoring, improvement, and auditing of the security of the ICT system (all assets in the six layers of the ports' ICT systems). Managing security requires a continuous and systematic process of identifying, analyzing, mitigating, reporting, and monitoring technical, operational, and other types of security risks (risk management) as well as implementing appropriate security measures and controls. Although various efforts and processes can be found in security management of ports' critical infrastructures (CIs), none of them address the security management of all layers of ports' CIs. They only treat the physical security, and they only deal with safety management of port systems.

SAFETY MANAGEMENT: A RESTRICTING APPROACH

Traditionally, targeted methodologies for risk assessment of ports like MSRAM (Maritime Security Risk Analysis Model) and its extended version MSRAM-PLUS/FORETELL address only physical security, and they are only compatible with the ISPS. Similarly, the available maritime risk assessment systems like MARISA concentrate on the safe navigation of ships during their presence in the port. The risk assessment system CMA detects abnormal behavior of ships and identifies respecting physical threats.

The ILO Port Health and Safety systems recognizes that risk assessment is an essential part of safety management. It provides a sound basis for the improvement of safety. It covers tasks and physical hazards in the workplace and allows hazards to be assessed to see how harmful they are. But cybersecurity threats are not covered in the ILO code.

The World Bank Group, together with the International Finance Corporation, released in 2007 a document called "Environmental, Health, and Safety Guidelines for Ports, Harbours, and Terminals." The Environmental, Health, and Safety Guidelines are technical reference

documents with general and industry-specific examples of Good International Industry Practice concentrating on physical hazards.

Various research efforts concentrate on physical threats, ignoring the cyber risks. Some examples follow.

Safety4Sea is a dedicated Maritime Safety and Environmental portal, a PRO BONO project to promote maritime safety and environmental awareness, operational safety, and environmental excellence. Safety4Sea's mission is to make practical safety and environmental excellence easy to understand for everyone in the industry, promote best practices, and improve people perception by promoting safety and environmental awareness in a wide range of maritime aspects.

FLAGSHIP is a partially EU-funded project, focusing on improvement of safety, environmental friendliness, and competitiveness of European maritime transport. The project contributes to a further increase in the capacity and reliability of freight and passenger services and to a reduction of negative impact from accidents and emissions. The emphasis of the project is on onboard systems and procedures, ship management systems on shore, impact of new technology on present ship owner and operator organizations, effective and efficient communication interfaces, and impact of standards and regulations. FLAGSHIP aimed to create the mechanism by which the expertise of all the required actors can be brought together in real time, independently of their location, and given to the right people, in the right format, at the right time, and incorporating the highest level of knowledge, so they can better manage all the questions that confront a ship operator: issues relating to the ship itself and its equipment (e.g., hull monitoring, equipment diagnostics, maintenance planning), its day-to-day operation (e.g., navigation, cargo, rule compliance), as well as emergencies and other exceptional situations (collision, fire, etc.).

The SafePort was a collaborative project under the EU Seventh Framework Programme. Many European ports will reach full capacity in the next few years. SafePort takes its cue from the aviation industry, which has addressed safety issues created by increased traffic through increasing automation and the use of sophisticated traffic management systems. SafePort developed and demonstrated an active vessel traffic management and information system (A-VTMIS) to manage vessel movement within its jurisdiction. This will ensure that vessels follow safe paths without conflicting with other vessels and improve the efficiency of port operations.

Several Preparatory Action on Security Research and EU FP7 Security Research programs initiated over the last decade addressing issues relating

to strengthening the safety of ports and/or their ports' CI systems. Most of these projects have fallen in three main categories, as follows:

Improved maritime surveillance systems: by enhancing the interoperability of local and national surveillance systems through the pooling of cross-sectoral surveillance information and its fusion into a central database. Representative examples are the following:

- The Autonomous Maritime Surveillance System (AMASS) project focused on strengthening maritime surveillance and on better integrating information and data between relevant agencies. The focus was on developing a cutting-edge early warning system that provides maritime authorities and law enforcement agencies with information about attempts at illegal immigration and other criminal activities at sea.
- The Underwater Coastal Sea Surveyor project is a cost-effective response to new terrorism attacks especially against underwater improvised explosive device threats. It provides a fundamental technology for the global issue of maritime surveillance and port/naval infrastructure protection.
- The Surveillance of Borders, Coastlines and Harbors project attempted to combine and maximize the use of existing surveillance technologies to model the most effective operational procedures for enhancing the surveillance of borders, coastlines, and harbors.
- The Sea Border Surveillance (SEABILLA) project aims to define the architecture for cost-effective European sea border surveillance systems, integrating space, land, sea, and air assets, including legacy systems. The project is applying advanced technological solutions to improve the performance of surveillance functions.

Interoperability of ports' CI systems: by enhancing the capability to collect and merge maritime-related data into a common and comprehensive picture to be shared among relevant organizations. Projects of this category are the following:

- The InterOPERAble Approach to European Union MARitime Security Management (OPERAMAR) project attempted to solve the issue of fragmentation between member states caused by the persistence of nation-specific procedures, legislations, and systems that hamper interoperability, greater information sharing, and improved coordination.
- The SECure CONtainer Data Device (SECCONDD) project was designed to initiate the international standardization of the technical interface between a secure container or vehicle and a data reader at a port or border crossing. The interface should enable law enforcement

and trade officials to read security data, including stored information from internal security and location sensors.

Protection of critical maritime infrastructure: by mitigating the risks of maritime safety (physical) incidents. A notable number of projects are the following:

- The Security System for Maritime Infrastructure, Ports, and Coastal Zones (SECTRONIC) project attempted to improve the safety of civilian ships (passenger and cargo carriers), energy platforms and facilities, and ports through advanced information, sensor, and response technologies. It aimed to develop an integrated security system combining surveillance, intrusion detection, and response to events and incidents.
- The Security Upgrade for Ports (SUPPORT) project aims to raise the current level of port safety by integrating legacy port systems with new surveillance and information management systems. Furthermore, the SUPPORT project has a special focus on border control, aiming to secure uninterrupted flows of cargos and passengers while allowing for the effective elimination of illegal immigration and trafficking.

CYBERSECURITY REGULATIONS AND STANDARDS

Most ports are compliant with ISPS code; however, this compliance does not imply secure ports since ISPS only addresses organizational and safety issues. However, the most recent regulations and directives are cybersecurity focused, and their implementation at the EU and international level will help the port authorities to secure their ICT systems and to better mitigate existing and upcoming cyber risks. In the upcoming years, the ports will need to implement the following new regulatory framework:

- **CIIP Directive** (2012), critical information infrastructure protection: toward global cybersecurity;
- **The Cybersecurity Strategy for the European Union** (2013) and the **European Agenda on Security** (2015) provide the overall strategic framework for the EU initiatives on cybersecurity and cybercrime;
- **eIDAS Regulation** (2014) on electronic identification and trust services for electronic transactions in the internal market;
- **European Parliament** (2015) concerning measures to ensure a high common level of network and information security across the union;
- **NIS Directive** (2016) applies only to those public administrations that are identified as operators of essential services;

- **cPPP Initiative** (2015) ensures that Europe will have a dynamic, efficient, and effective market in cybersecurity products and services;
- **Enhanced Privacy Directive** (2016), mandatory reporting of security breaches;
- **USA H.R. 3878**, House of Representatives, "Strengthening Cybersecurity Information Sharing and Coordination in Our Ports Act of 2015."

Besides the new upcoming regulatory framework, standards and best practices embrace the effort for better ICT security management. An overview of ICT security management standards is presented in this section. It should be noted that these standards do not constitute risk management methods, but rather, they fix a minimal framework and describe requirements, for the risk assessment process itself, for the identification of the threats and vulnerabilities allowing to estimate the risks, their level, and then to be able to define an effective treatment plan.

The most well-known cybersecurity standards are these:

ISO/IEC 27001 36 is a commercial standard that specifies requirements for the establishment, implementation, monitoring and review, maintenance, and improvement of an information security management system (ISMS). The ISMS is an overall management and control framework for managing an organization's information security risks. The ISO/IEC 27001 does not mandate specific information security controls but stops at the management and operational level. Usually, a group of analysts with high ICT expertise and experience verifies the compliance of the organization with the defined requirements. However, although the compliance process requires the involvement of multiple users, the collaborative abilities of the standard are limited due to its inherent complexity. The standard covers mostly large-scale organizations (e.g., governmental agencies and large companies), while it is considered too heavy for micro, small, and medium size businesses.

The ISO/IEC 27001 ISMS incorporates several Plan-Do-Check-Act cycles: for example, information security controls are not merely specified and implemented as a one-off activity but are continually reviewed and adjusted to take account of changes in the security threats, vulnerabilities, and impacts of information security failures, using review and improvement activities specified within the management system. There exist a variety of freeware (e.g., EBIOS developed by Central Information Systems Security Division [France]) and commercial software (e.g., CRAMM developed by Insight Consulting) that verify the compliance of the organization with the ISO/IEC 27001.

ISO/IEC 27005:2008 38, a commercial standard from the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), describes the risk management process and its activities for information security and provides guidelines for information security risk management and supports the general concepts specified in ISO/IEC 27001:2005 as well as the main principles and rules described in ISO/IEC 27002:2005. It is applicable to all types of organizations (e.g., governmental agencies, large companies, small and medium size enterprises) that intend to manage cyber risks that could compromise the organization's information security. Essentially, the ISO information security risk management process can be applied to the whole organization; any discrete part of the organization (e.g., a department, a physical location, a service); any ICT system; and any existing, planned, or aspect of control (e.g., business continuity planning).

ISO 27005 proposes the use of both quantitative and qualitative methods for the calculation of the risk level; however, it does not support any specific technique for this purpose or any computational method to analyze and combine the assessment information. The generic nature of the standard does not include aspects that promote the collaboration among the users.

In this context, more integrated risk management methodologies and methods such as EBIOS, MAGERIT, and MEHARI comply with the rules and obligations defined by the specific standard.

ISO/IEC 27002:2005 is a commercial standard that establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. It provides specifications with guidance for implementation of the ISMS in the organization. This can be used by internal and external analysts with high ICT expertise and experience, to assess an organization's ability to meet its own requirements, as well as any customer or regulatory demands.

The standard provides a list of 10 main control domains (organization of information security; asset management; human resources security; physical and environmental security; communications and operations management; access control; information systems acquisition, development, and maintenance; information security incident management; business continuity management; compliance) comprising 36 control objectives and 127 controls, which are used for the assessment. The standard promotes the adoption of a process approach for establishing, implementing, operating, monitoring, and improving the effectiveness of an organization's ISMS.

It should be noted that ISO/IEC 27002 is not a real method for risk analysis and management, but rather compliance standards, reporting a list of controls for good security practices and the requisites that an existing method should have to be standard compliant. However, although it is neither a method for evaluation nor for management of risks, it includes specific risk handling aspects such as the identification of risk and the creation of an initial risk treatment plan. The standard can cover all types of organizations (e.g., governmental agencies) and all sizes from micro to medium and large size businesses.

SECURITY MANAGEMENT: A HOLISTIC APPROACH

Since an ICT system as defined in Chapter 2 is a six-layer system comprised by physical and cyber layers and assets, a holistic approach to risk assessment is needed to assess the security (confidentiality, integrity, authenticity, availability) level of all assets (physical and cyber) in all layers of the ports' ICT systems. In this section, an overview of security-related legislation and ICT security management standards are provided.

According to the survey [160] the existing methodologies use *four different approaches* to define the risks:

1. The concept of the risk is related to a threat and an asset (or a group of assets), and it comprises the likelihood of the threat, the vulnerability level of the asset(s) to the threat, and the impact of the threat on the asset(s).

$$\text{Risk (Threat, Asset)} = \text{Likelihood (Threat)} \otimes \text{Vulnerability (Threat, Asset)} \otimes \text{Impact (Threat, Asset)}$$

2. The concept of the risk is related to a threat, an asset, and specific security needs. It comprises the vulnerability of the asset and the impact of the threat on the security needs.

$$\text{Risk (Threat, Asset, Needs)} = \text{Impact (Threat, Needs)} \otimes \text{Vulnerability (Threat, Asset)}$$

3. The concept of the risk (defined as annual loss expectancy [ALE]) is related to a threat and an asset, and it comprises the probability of the threat affecting the asset and the average loss of the resulting incident.

$$\begin{aligned}\text{Risk (Threat, Asset)} &= \text{ALE (Threat, Asset)} \\ &= \text{Probability (Threat, Asset)} \otimes \text{Average Loss (Threat, Asset)}\end{aligned}$$

4. The concept of the risk is related to a threat and a critical asset, and it comprises the impact of the threat on the critical asset and the vulnerability of the asset.

$$\text{Risk (Threat, Critical Asset)} = \text{Impact (Threat, Critical Asset)} \otimes \text{Vulnerability (Critical Asset)}$$

5. The concept of the risk is related to an incident (i.e., a threat exploiting vulnerability) and an asset, and it comprises the likelihood of the incident and the consequences of the incident itself.

$$\text{Risk (Incident, Asset)} = \text{Likelihood (Incident)} \otimes \text{Consequences (Incident, Asset)}$$

The **security management process**, i.e., the process in evaluating all risks, consists of the following phases:

- *context establishment*: intends to define the risk management's boundary (e.g., the entire organization, one ICT, one service);
- *asset identification*: identify all assets within the boundary of the assessment;
- *threat analysis*: analyze all threats of the identified assets and the threat levels;
- *risk analysis*: intends to evaluate the risk levels;
- *risk assessment*: used to make decisions and consider the objectives of the organization;
- *risk treatment*: to treat, reduce, retain, avoid, or transfer the risks;
- *risk communication*: to achieve agreement on how to manage risks by exchanging and/or sharing information about risk between the decisionmakers and other stakeholders;
- *risk monitoring and review*: to detect any chances in the context of the organization at an early stage, and to maintain an overview of the complete risk snapshot.

The existing security management methodologies can be evaluated based on the following *assessment criteria* as proposed by the literature [160,33]:

C1. *scope*: the applicability of the method. The following types have been identified: (1) general-purpose method, covering only specialized ICT requirements and (2) targeted-purpose method, covering specific sectoral characteristics, particularities, needs, and requirements;

C2. *target group*: the most appropriate type of organizations the method aims at;

C3. *RA/RM support*: the phases that the method supports (risk analysis or/and risk management);
C4. *evaluation scale*: the approach (quantitative or qualitative) used in the methods to evaluate the risk level;
C5. *impact evaluation*: the approach adopted in the methods to determine the impact level. Each method uses specific scenarios, factors, parameters, and guidelines to define the impact of an event;
C6. *risk evaluation*: the approach used in the methods to calculate risk level;
C7. *collaboration capabilities*: the capacity of the methods to promote the collaboration of the users in the evaluation process;
C8. *computational capabilities*: the capacity of the methods to analyze and combine diverse and distributed corporate knowledge;
C9. *required skills*: the level of skills needed to use and maintain the method;
C10. *cost*: the licensing schema available for the method;
C11. *automated tools*: availability of tools that support the method;
C12. *compliant with standards*: compliance with national or international standards.

The existing security management methodologies are assessed for their suitability to be applied in the ports' ICT CIIs. Because commercial ports are CIs, we also present risk assessment methodologies for CIs. This section concludes that methodologies combining maritime safety, cyber, and CI standards will be most appropriate for the security management of commercial ports CIIs.

For an enriched repository of security risk management methodologies and tools, we refer the reader to the ENISA repository [67]; in this section, we describe only the most well-known ones:

NIST 800-30 [94] is a free guide that provides a foundation for the development of an effective risk management program, containing both the definitions and the practical guidance necessary for assessing and mitigating risks identified within IT systems. The goal is to help mostly large-scale organizations (such as governmental agencies and large companies) to better manage IT-related mission risks. The use of a primitive method for the calculation of the risk level in combination with the lack of an effective computational technique to analyze and correlate the knowledge located in a corporate environment reduce the abilities of the NIST 800-30 for a more integrated approach. In addition, even though the method has adopted and uses extensive technical and operational questionnaires that require the involvement of a variety of users, the concept of collaboration in the determination of the overall results and the formulation of the final treatment

plan is limited. The risk analysis and management process defined in NIST 800-30 is usually executed by a dedicated group of ICT experts.

The method is compliant with the ISO/IEC 27001:2005 addressing all the requirements for the establishment and implementation of an ISMS. Currently, NIST 800-30 is not supported by any freeware or commercial application.

OCTAVE [115] is a free of charge approach to information security risk evaluations that is comprehensive, systematic, context-driven, and self-directed. The approach is embodied in a set of criteria that define the essential elements of an asset-driven information security risk evaluation. Initially, it was designed with larger organizations in mind; however, a targeted method for small organizations has been developed.

The OCTAVE method uses a three-phase approach to examine organizational and technology issues, assembling a comprehensive picture of the organization's information security needs. The method uses workshops to encourage open discussion and exchange of information about assets, security practices, and strategies. In this context, the corporate users participate actively in several parts of the evaluation process. This indicates that the method incorporates specific collaborative abilities.

Each phase consists of several processes, and each process has one or more workshops led or conducted by the analysis team. Some preparation activities are also necessary to establish a good foundation for successfully completing the evaluation. OCTAVE uses for the risk analysis a primitive approach based on a qualitative scale (high, medium, low). In addition, the method does not integrate an advanced technique for the analysis and combination of the knowledge located in the corporate environment. Thus, the information is going through an insufficient process for the determination of the overall results. Finally, OCTAVE method is supported by commercial standalone software, OCTAVE Automated Tool, implemented by Advanced Technology Institute. The tool can assist the user during the data collection phase, organizes collected information, and finally, produces the study reports.

CRAMM [55] is a method developed to assist mostly the large-sized organizations (such as governmental agencies and large companies) to undertake a risk analysis of information systems and networks, to identify security requirements and possible solutions, and to detect contingency requirements and possible solutions. The method is applicable to all types of information systems and networks and can be applied at all stages in the information system lifecycle, from planning and feasibility, through development and implementation, to live operation.

CRAMM consists of three main phases: identification and valuation of assets, risk analysis, and risk management. In this method, an analyst or a group of analysts undertake the responsibility to evaluate the security and risk level of the organization analyzing and combining the diverse knowledge distributed in the corporate environment. The computational method and technique that has been adopted by CRAMM for the correlation and the determination of the results is quite primitive and is based on a qualitative approach. In addition, the involvement of the users of the organizations to the actual assessment can be considered low; thus the collaborative capabilities of the method are characterized as limited. For the analysts to use and execute all the phases of the method (identification and valuation of the assets and risk analysis and management), they should have a high level of skills and experience at gathering and analyzing information to identify threats and vulnerabilities, to infer the risks, and to define the most appropriate countermeasures that fit to the needs of the organizations.

As a method, CRAMM is detailed enough and can cover an extensive range of features at management, operational, and technical levels. Also, CRAMM complies with the rules and obligation imposed by the ISO 27001 and ISO 27005 standards. CRAMM is supported by a commercial standalone tool, developed by Insight Consulting, that provides a way to implement the proposed method.

EBIOS [42] is a risk management approach created under the French General Secrétariat of National Defense. It proposes a methodology and supporting software for assessing and treating risks in the field of information systems security.

EBIOS approach consists of a cycle of the following phases: context analysis in terms of global business process dependency on the information system; threat analysis; and risks estimations. EBIOS methodology is easy to understand and deploy; thus it can be applied by a set of organizations that vary from governmental agencies and large companies to small and medium size enterprises. Its overall philosophy is straightforward and intuitive, and it follows a natural sequence. It consists of formalizing the sensitivities and threats and determining the associated risks for the organization. The methodology possesses collaborative abilities since it gathers and combines the corporate knowledge in a smooth and efficient manner based on a qualitative approach. However, the lack of an advanced computational schema for the correlation and determination of the results can be considered a main disadvantage.

EBIOS has been applied both to basic systems and to complex systems (human resources management system interconnecting several elements), at the predesign stage or on existing systems, to complete information systems or to subsystems. Although, it should be noted that the level of detail of the method is limited to management and operational issues and characteristics.

EBIOS can cover all the requirements, steps, and processes defined by a variety of IT standards such as the ISO/IEC 27001:2005, the ISO/IEC 27002:2005, and the ISO/IEC 27005:2008. The method is supported by an open source tool developed by Central Information Systems Security Division (France) and is a standalone application that is based on Java and XML technologies. The tool integrates all risk analysis and management steps defined by the five EBIOS phases assisting users with low IT expertise and experience to evaluate and mitigate the corporate risks.

IT-Grundschutz [11–13,26] has been developed by the Federal Office for Information Security in Germany, and it provides a configuration for the establishment of an integrated and effective ICT security management.

The method, before starting the risk analysis, does a basic security check to verify implemented security measures. Risk assessment identifies threats, which are not avoided by the measures, such as residual threats. These threats can be eliminated by additional security measures. In this way, risk will be reduced to an acceptable level.

IT-Grundschutz has been designed to apply to organizations with complex underlying infrastructure such as governmental agencies and large companies as well as to small and medium size businesses with basic systems. The method can be deployed by users with standard IT-related expertise and experience that undertake the responsibility to execute the evaluation process. However, the collaborative abilities of the method can be considered low since the corporate users are involved only in specific steps of the risk assessment. The method is compliant to ISO/IEC 27001:2005, addressing the defined requirements, as well as being suitable for the implementation of the ISMS process described by ISO/IEC 27002:2005. In this context, IT-Grundschutz aims at assisting all users with managerial, operational, and technical responsibilities in their efforts to manage the security of information and ICT resources and to reduce the associated risks.

The method is supported by commercial software, GStool, developed by Federal Office for Information Security (BSI). GStool is a standalone application with database support.

MAGERIT is an open methodology developed by the Spanish Higher Council for Electronic Government, offered as a framework and guide to the public administration. It is the answer in the increasing dependency of the public and private organizations on information technologies to fulfill their mission and reach their business objectives. The purpose of MAGERIT is directly related to the generalized use of ICT systems that bring evident benefits for the users but which is also subject to certain risks that must be kept under control by means of security countermeasures that generate confidence in the use of these media.

Various organizations that possess complex IT infrastructure (governmental agencies and large companies) as well as basic systems (small and medium size enterprises) can apply this method to identify and mitigate their security risks. MAGERIT can be used and maintained only by users with high ICT expertise and experience. These users undertake the responsibility to run the risk analysis process via workshops and interviews with specific representatives of the organization that participate only in specific phases of the assessment process. In this context, the method does not support sufficient collaborative capabilities and features.

MAGERIT complies with a set of IT standards. Specifically, it addresses all the rules and obligations imposed by the risk analysis and management standards ISO/IEC 27005:2008, covers all the requirements defined by the ISO/IEC 27001:2005, and conforms with the code of implementation of an ISMS specified by the ISO/IEC 27002:2005.

A commercial software that implements and expands the MAGERIT methodology is the EAR/PILAR. This is a standalone application (based on Java and XML technologies), developed by A. L. H. J. Mañas that has been designed to support and execute the defined risk management process.

MEHARI is a free of charge qualitative risk analysis and management method developed by CLUSIF (CLub for the Security of Information in France or CLub de la Sécurité dde l'Information Français). MEHARI provides a consistent methodology, with appropriate knowledge bases (e.g., manuals and guides that describe the different modules [stakes, risks, vulnerabilities]), that has been designed to assist people implicated in security management (CISOs, risk managers, auditors, CIOs) in their different tasks and actions. Specifically, it is targeted to users with managerial, operational, as well as more technical responsibilities. The methodology is suitable for the implementation of the ISMS process described by ISO/IEC 27001:2005; it is compliant with ISO/IEC 27005:2008 requirements providing the set of tools and elements required for its implementation.

MEHARI is most appropriate for medium- to large-scale organizations such as governmental agencies and medium and large size companies. The corporate users can participate only in specific phases of the methodology related to the identification of assets and vulnerabilities. In this context, the collaborative capabilities of the methods can be considered limited, since the users are not involved directly in the risk calculation and the formulation of the risk treatment plan. In addition, the method uses a primitive computational method to analyze and combine the diversity of the information to deduce the final results.

MEHARI is supported by two standalone toolkits. The first one is commercial software managed by the company Risicare, and the second is a freeware application, [MEHARI2010] basic tool, developed by CLUSIF.

ISAMM [54] is a quantitative type of risk management methodology that can be applied by a variety of organizations such as governmental agencies, large companies, and small and medium size enterprises. In this method, the assessed risks are expressed, through their ALE, in monetary units. ALE is the annual expected loss or cost should a threat or a group of threats be materialized.

$$\text{ALE} = [\text{probability}] \times [\text{average impact}]$$

This formulates the basis for the return on investment–based approach and the economic justification capabilities of ISAMM with respect to the risk treatment plan. ISAMM allows showing and simulating the reducing effect on the risk ALE for each improvement control and to compare this with its cost of implementation.

ISAMM is compliant to ISO/IEC 27002 and provides maximal support of the ISO/IEC 27001 ISMS standard. It is supported by a freeware tool, ISAMM Consultant tool, and a commercial application named ISAMM Client tool.

Table 3.1 provides a summarized overall assessment of the previously mentioned security management methodologies based upon the twelve criteria previously described.

All the methodologies and methods presented describe specific implementation steps for the evaluation of the security level of the organizations. Beside ISO 27001 and ISO 27002 that provide generic requirements of risk assessment and do not include specific risk handling aspects, all the other approaches provide well-defined actions and steps for the execution of the risk analysis and risk management processes. Also, most of the methods are meant to be used with qualitative measurements, and this confirms

Table 3.1 Assessment of Security Management Methods and criteria

Methods	Criteria C1	C2	C3	C4	C5
ISO/IEC 27005:2008	General-purpose	Government, agencies, large companies, SME	RA/RM	Quantitative/Qualitative	Based on the business harm
NIST 800-30	General-purpose	Government, agencies, large companies	RA/RM	Qualitative	Based on open damage scenarios
OCTAVE	General-purpose	Government, agencies, large companies, SME	RA/RM	Qualitative	Based on critical assets
CRAMM	General-purpose	Government, agencies, large companies	RA/RM	Qualitative	Based on open damage scenarios
EBIOS	General-purpose	Government, agencies, large companies, SME	RA/RM	Qualitative	Based on security needs
IT-Grundschutz	General-purpose	Government, agencies, large companies, SME	RA/RM	Qualitative	Based on open damage scenarios
MAGERIT	General-purpose	Government, agencies, large companies	RA/RM	Quantitative/Qualitative	Based on open damage scenarios
MEHARI	General-purpose	Government, agencies, medium to large companies	RA/RM	Qualitative	Based on fixed damage scenarios
ISAMM	General-purpose	Government, agencies, large companies, SME	RA/RM	Qualitative	Based on monetary loss

C6	C7	C8	C9	C10	C11	C12
N/A	Low	Low	Standard	Commercial	No	ISO/IEC 27001:2005, ISO/IEC 27002:2005
Type 1	Low	Low	ITC experts	Free	No	ISO/IEC 27001:2005
Type 4	Medium	Low	Standard	Free	Yes/ Commercial	—
Type 1	Low	Low	ITC experts	Commercial	Yes/ Commercial	ISO/IEC 27002:2005
Type 2	Medium	Low	Standard	Free	Yes/Free	ISO/IEC 27001:2005, ISO/IEC 27002:2005, ISO/IEC 27005:2008
Type 5	Low	Low	Standard	Free	Yes/ Commercial	ISO/IEC 27001:2005, ISO/IEC 27002:2005
Type 5	Low	Low	ITC experts	Free	Yes/ Commercial	ISO/IEC 27001:2005, ISO/IEC 27002:2005, ISO/IEC 27005:2008
Type 1	Low	Low	ITC experts	Commercial	Yes/ Commercial/ Free	ISO/IEC 27001:2005, ISO/IEC 27005:2008
Type 3	Low	Low	Standard	N/A	Yes/ Commercial/ Free	ISO/IEC 27002:2005

the fact that most risk assessments today are carried out in a qualitative way, mainly due to lack of reliable quantitative data or to time constraints.

We have identified the following pitfalls of the described methodologies:

Only a part of them are supported by software (in some cases freeware) tools. The general characteristics of these tools are:

- not easy to use without high security expertise;
- monolithic and standalone, thus failing to address advanced requirements of the modern information systems;
- the use of advanced and interactive Web-based graphical user interfaces and the collaboration aspect are two notable requirements that the existing tools and applications do not satisfy. For this reason, most solutions fail to facilitate the distribution and sharing of the information, experience, and expertise within an enterprise and encourage the users to jointly work for the implementation of the phases of the risk analysis and risk management in an effective and smooth manner.

Regarding impact level evaluation [160], the ISO 27005 and ISO 27002 impose that the impact of a security event is assessed in terms of the business harm caused to the organization. In MEHARI, the analysts involved in the risk analysis process measure the impact level based on a "fixed" impact scenario. On the other hand, CRAMM, IT-Grundshutz, NIST SP 800-30, STORM, and MAGERIT give the opportunity to the analysts to specify different impact scenarios (e.g., from catastrophic to marginal) that depict the negative effects of an event (e.g., threat, attack) on the organization. In this context, these approaches adopt the concept of damage scenarios. OCTAVE measures impact based on how "hard" a security event affects a critical asset. In EBIOS, the impact level of an event is measured considering the security needs that the specific event violates. Similarly, in ISAMM the impact is assessed in terms of financial losses the organization has suffered because of an event. The impact level evaluation approach needs to be standardized to achieve uniform evaluations for the EU ports.

They fail to capture the complexity of infrastructure interconnections, cross-sector impacts, dependencies with other systems, or infrastructures and cascading effects within a sector or across sectors. Therefore, various modifications are required to be applied in the security management of the ports' ICT systems since these systems interact with many maritime external entities (interdependencies analysis).

The methodologies try to cover the obligations imposed by the ISO family of standards (ISO/IEC 27001:2005, ISO/IEC 27002:2005, ISO/IEC 27005:2008). However, only EBIOS and MAGERIT achieve full

compliance with their rules and procedures. CRAMM, ISAMM, and IT-Grundschutz follow the code of implementation of an ISMS as described by the ISO/IEC 27002:2005, while NIST 800-30, IT-Grundschutz, and MEHARI satisfy the requirements defined by the ISO/IEC 27001:2005. They are very generic, failing to provide targeted technical solutions that address specific sectoral (e.g., maritime) problems and threats, such as interdependent threats rising from associated entities, sector-specific threats (e.g., weather conditions, strikes), and sector-specific legislation (e.g., ISPS in maritime environment). However, these methods and standards provide an insight for the security management of the ports' ICT systems.

All the methods rely on interviews and workshops to aggregate and accumulate the information of the security assessment. However, most of them present limited collaborative capabilities since they do not promote the extensive and efficient collaboration among the involved stakeholders, the effective discussion and exchange of information, ideas, and thoughts, as well as the active involvement of the corporate representatives. This is a major drawback if we want to apply them in the ports' ICT systems since there are many users and the required face-to-face interviews will require time, effort, and resources. Only OCTAVE and EBIOS provide basic collaboration abilities containing specific features that allow the users to participate actively in several parts of the evaluation process.

Regarding risk level evaluation, the following conclusions can be deduced. CRAMM, MEHARI, STORM, and NIST SP 800-30 share the same common view on risk, i.e., they all consider risk as a combination of the likelihood and the impact of a threat to hit a group of assets and the vulnerability level of this group of assets. Similarly, IT-Grundshutz and MAGERIT consider risk as the combination of the likelihood of an incident (i.e., a threat exploiting some vulnerabilities) and the consequences (positive or negative) of this incident happening. On the other hand, Type 2, Type 3, and Type 4 profiles are intrinsically tied to a particular approach to risk analysis, since Type 2 and Type 4 rely on qualitative concepts for defining risk (e.g., critical assets, security needs) and Type 3 relies on the quantitative concepts of probability and average monetary loss. Finally, the methods of the ISO family do not adopt any risk analysis profile. This is because ISO 27005 is a very general guideline to set up a risk management framework, while ISO 27002 and ISO 27001 are not real methods for risk management, but rather compliance standards, reporting a list of controls for good security practices and the requisites that an existing method should have to be standard-compliant, respectively. Another important drawback of

the risk analysis approaches is the lack of efficient and advanced computational techniques. They usually rely on primitive methods to evaluate, determine, and mitigate the corporate risks and use ineffective procedures and techniques to analyze and combine the diverse knowledge located in the organizations. The adoption of more advanced approaches (using new techniques, e.g., fuzzy logic, graph theory, group decision-making) that enhance the inherent capabilities of the risk analysis solutions will increase the accuracy of their conclusions.

CIIP METHODOLOGIES

Several standards and methodologies exist for ensuring the critical information infrastructure protection (CIIP). Most of them contain procedures, definitions, and explanations of techniques used to collect and analyze information in CIIP.

Most the CIIP standards and methodologies are from the energy sector and more specifically from the US Department of Energy and North American Reliability Corporation. From its 83 standards a group of specific standards (CIP-002-3 and CIP-003-3) address the protection of critical infrastructures, but only for the electrical energy systems in a very abstract manner. However, since they are very generic, they can provide an insight for the ports. Various national risk assessment methodologies for CIs exist that use various ways in estimating the criticality of an infrastructure even at national level (e.g., in the Netherlands). There is not a standardized way in examining the criticality of an infrastructure or/and addressing cyber threats. A short description of these CIIP methodologies is presented in Table 3.2.

The CIIP methodologies and standards have been evaluated [159] according to the following criteria:

- **availability**: availability of supported applications (under research (R) and/or development (D), or already available for use by the public with commercial purposes (C) or by a limited or restricted group, normally the military (L));
- **CI affected**: The CI sectors that are covered based on [NIPP2009] and Directive 114/08 11 include electricity (1); natural gas (2); oil and pipelines (3); drinking water (4); sewage and wastewater (5); industrial control (6); telecommunications (7); computer networks and information systems (8); railways (9); highways and roads (10); human activities including services and emergency evacuation (11); banking and finance (12); also, the policies and regulations features (13);

Table 3.2 CIIP methodologies short description

	Nature	Description
ATHENA	Software tool	Provides a model for vulnerability analysis of interdependent infrastructure networks
Critical infrastructures interdependencies integrator (CI3)	Software tool	Estimates service's restoration time and cost
Critical infrastructure protection decision support system (CIP/DSS)	Software tool	Provides decision support for CIIP comparing the effectiveness of strategies to reduce the probability of a risk
Critical infrastructure protection modeling and analysis (CIPMA)	Software tool	Evaluates the effects on the operation disruption of CII services within and across sectors
Agent-based simulation model of the US economy (COMM-ASPEN)	Software tool	Provides simulations of the effects of both market decisions and interruptions of telecom infrastructure in the economy based on an agent-based approach
DUTCH NRA	Working methodology	Provides a multicriteria decision-making approach for the risk evaluation considering political and societal issues
Procedimiento informá tico-ló gico para el aná lisis de riesgos (EAR-PILAR)	Software tool	Supports a comprehensive risk analysis method
Electricity market complex adaptive system (EMCAS)	Software tool	Provides an in-depth investigation of the operational and economic impacts on the electrical system, as affected by various external events, based on an agent-simulation approach
Fast analysis infrastructure tool (FAIT)	Software tool	Provides a framework for conducting economic impact assessment across multiple sectors
Financial system infrastructure (FINSIM)	Software tool	It applies to scenarios of crisis affecting the banking payment system, the use of plastic money, the federal funds market, and the interactions between these entities

Continued

Table 3.2 CIIP methodologies short description—cont'd

	Nature	Description
Failure modes and effects analysis (FMEA-FMECA)	Working methodology	Provides a procedural approach for identifying and analyzing possible failures in the design, development and maintenance of a system, based upon the severity or the effect of system failures
FORT-FUTURE	Software tool	Provides a framework that enables decisionmakers to virtually test potential solutions running multiple dynamic simulations
Fault tree analysis (FTA)	Working methodology	Provides a method to failure analysis, identifying the causes leading to the manifestation of a risk within a system
Interoperability (GIS)	Working methodology	Using geographic information systems in emergency coordination and support for decision-making
GORAF	Software tool	Provides a framework for the identification and analysis of the most critical resources within an infrastructure
Hazardous operations (HAZOP)	Working methodology	Support a range of techniques for the identification of potentially hazardous conditions and risks based on assumptions
Inoperability input–output model (IIM)	Software tool	Provides a comprehensive framework based on analytical models to identify and address the risks come from the intra- and interconnectedness of economic sectors
INTEPOINT VU	Software tool	Adopts a decision support model to analyze planning responses to intentional and unintentional events
LUND	Working methodology	Provides a method for the representation of a system of roads or rail interconnected transport infrastructure

Metodología de análisis y gestión de riesgos de los sistemas de información (MARGERIT)	Working methodology	Provides an approach that gives emphasis on the protection of the ICT infrastructure
Methodology for interdependencies assessment (MIA)	Working methodology	Aims to identify and evaluate the interdependencies among critical ICT components
Multilayer infrastructure (MIN)	Software tool	Provides a dynamic game theoretic model to analyze multilayer infrastructure networks
Multinetwork interdependent critical infrastructure programme for analysis of lifelines (MUNICIPAL)	Software tool	Provides a framework for identifying, analyzing, and responding to events that affect the interdependence of civil infrastructure
National agent-based laboratory for economics (N-ABLE)	Software tool	Identifies and analyzes economic factors, feedbacks, and downstream effects of road transport infrastructure and electricity markets
Net-centric effects-based operations model (NEMO)	Software tool	Provides an environment to support decision-making in the area of planning an infrastructure system
Network security risk assessment model (NSRAM)	Software tool	Analyses interconnected multiinfrastructure networks in order to determine the system behavior to various kinds of negative events
Risk maps	Working methodology	Supports a method for identifying and recording of risks in a systematic and effective manner
Transportation routing analysis geographic information system (TRAGIS)	Software tool	Provides a method for the optimization of transportation routes
Urban infrastructure suite (UIS)	Software tool	Provides a simulation-based approach to represent urban infrastructures and populations
Virtual interacting network community (VINCI)	Working methodology	Provides virtualization of the network architecture for critical infrastructures

- **stage**: the functionality provided in each of the stages of risk management programs: identification of assets (a); risk assessment (b); prioritization of actions (c); implementation programs (d); and effectiveness measurement (e).

  Based upon these criteria, an overall ranking is described in Table 3.3.

CIIP methodologies mostly address safety threats; over two-thirds of them are implemented in software tools, and the rest are analytical and generic methodologies. About half of the applications have resulted in the development of computer platforms, whether commercial or of restricted use, e.g., corporate, institutional, private, or military. One-quarter of the

Table 3.3 Assessment of suitable CIIP methods

CIIP methodologies	Availability	CI sector	Stage
ATHENA	L	1,2,3,4,5,6,**7**,**8**,**9**,**10**,11,12,13	b
CI3	L	1,2,4,5,6,**7**	c
CIP/DSS	L	1,2,3,4,5,6,**7**,**9**,**10**,11,12,13	a,c,d,e
CIPMA	L	1,2,3,**7**,**8**,12,13	d,e
DUTCH NRA	L	1,3,4,**10**,11,13	a,b,c
EAR/PILAR	C	**8**,11,13	a,b,c,d
EMCAS	C	1,**7**,12	a,b,c
FAIT	L	1,2,5,**9**	a,b
FINSIM	R	**7,12**	a,b
FMEA/FMECA	C	6,**7**,11,12	a,b,c
FORT-FUTURE	L	1,2,3,4,5,6,**7**,**9**,**10**,11,12,13	a,b,c,e
FTA	C	6,**7**,11,12	a,b,c
GIS interoperability	R	9,1	c,e
GoRAF	R	1,4,6,**8**,11	b,c,d
HAZOP	C	1,2,3,**7**,11,13	a,b,c
IIM	R	1,4,**7**,**8**,**10**,13	a,c,d
INTEPOINT VU	C	1,**7**,**9**,**10**,11	c
LUND	R	1,**9**,**10**	a,b
MARGERIT V2	C	**8**,11,12,13	a,b,d
MIA	R	**7,8**,13	a,b
MIN	R	**10,11**	a
MUNICIPAL	R	1,**7**,**8**	a,c
N-ABLE	L	1,**9**,12	a,c,d,e
NEMO	L	1,2,4,**9**,13	c,d,e
NSRAM	R	1,7	c,d,e
Risk maps	R	1,2,3,4,5,6,**7**,**9**,**10**,11,12,13	A
TRAGIS	L	**9,1**	A
UIS	L	4,5,**7**,**10**,11	a,b,c,d
VINCI	R	**8**	d

The bold describe the methodologies that can be applied in the transport sector that host information systems.

applications have limited availability and are mostly addressed at military and governmental segments. This could be explained due the leadership taken by some US laboratories, which in turn are sponsored by both the Department of Homeland Security and the Department of Energy. Another quarter of the applications have commercial purposes (computer platform licensing, consulting, etc.). These are extensively used in the energy sector, cybersecurity, and in the definition of emergency response strategies.

Regarding the deployed CI sector, nearly one-quarter of the applications are involved with energy infrastructure (electricity, natural gas, oil, and pipelines). Other infrastructures receiving attention are those related to information technologies and communication and control systems (21%), water (13%), transportation (10%), and banking (8%). About 11% of the methodologies are related to human activities queries and responses checking into CI, which establishes responses to human users' system under emergencies, industrial security, policy recommendations on assets protection, and/or human life protection. Finally, implementation of policies and regulations has attracted special consideration in 12% of the reviewed platforms.

Regarding the risk stage, over two-thirds of the approaches cover the first three steps of a complete risk management process. These steps concern the identification of the corporate assets developing an inventory, the risk assessment process focusing on the evaluation of the security level, and the prioritization of actions establishing priorities for risk assessments, to identify where risk reduction is more compelling and then to determine protective measures that need to be taken. Nearly half of the solutions implement a protection program that includes the deployment of specific protection measures, while only a limited number of the applications apply the stage of measuring effectiveness establishing indicators to provide information on achieving specific security goals.

CYSM RISK ASSESSMENT TOOL AS A BEST PRACTICE

A proposed solution to better address the ports' security is to combine the ISPS with common ICT security management and CIIP standards. However, the well-known security management standards described before will need further modifications to adapt to the port ICT security, so they can address specific sectoral threats, i.e., interdependent threats rising from all entities in the maritime environment, specific threats (e.g., weather conditions, strikes), and maritime legislation (e.g., ISPS).

A targeted security management methodology for the ports' CIs should address the following general requirements:

- *Compatibility with standards*: The methodology needs to comply and implement the ISO 27001, CIIP standards, and the ISPS to address all aspects of the security requirements of the ports' ICT systems that are hosted in the ports CIIs.
- *Collaboration*: Ensure collaboration among all ICT port users (e.g., operators, administrators, collaborators, suppliers, providers).
- *Interdependencies*: All interconnections of the ports' CIIs with all other entities in the maritime ecosystem need to be identified.
- *Broad threat analysis*: Analyze interconnected and interdependent threats.
- *Time and resource economical*: Avoid the plethora of paper-based questionnaires and frustrating interviews imposed by the existing methodologies that are resource (time, personnel) efforts.
- *Easy to implement*: The expert should not need a high level of expertise to apply the methodology.
- *Open*: Avoid security through obscurity.
- *Holistic*: Secure all layers and all assets of the ports' ICT systems.
- *User centric*: Collect and value the opinions and experience of all port users regarding the security of the ports' ICT system.
- *Automation*: Implement the methodology in a user-friendly, open source, collaborative tool.

Any targeted security management methodology needs to be supported by a tool. This tool will be used by the port security team to easily manage their security. Such a tool needs to address the following general requirements:

- *Knowledge codification*: Participants should be able to find relevant risk management knowledge. A codification strategy probably works best for certain types of knowledge that are not expected to change frequently. Participants can then easily retrieve methods and best practices that have proven themselves in the past, and reuse them accordingly.
- *Personalization*: Security management decisions need to reach consensus with all ports' users; knowledge is not always immediately "stable" enough to codify. For such knowledge, a personalization strategy could prove useful to enable participants to find who knows what. Furthermore, personalization techniques should also be valuable to support the discussions and negotiations between ports' users and stakeholders.

- *Collaboration*: Because security management is consensus decision-making, a knowledge-sharing tool should explicitly support collaboration between different users. This property enables the active involvement of all important stakeholders in the decision-making process.
- *Role-specific content views*: Since the security management includes three modes (practicing, criticizing, and reviewing) in which usually different participants' roles are involved, the tool must support specialized views on the available content, such as open issues or approved decisions.
- *Descriptive approach*: Since the security management process is highly creative, the knowledge-sharing tool should not be prescriptive in nature. A more descriptive approach toward the knowledge management would best facilitate the creativity of the participants.
- *Service-oriented*: All steps involved in the security management methodology (boundary specification, asset identification, threat analysis, impact analysis, vulnerability estimation, risk estimation, and mitigation strategy) should be provided as collaborative services.

Cyber/physical security management (CYSM) can serve as a best practice meeting the aforementioned requirements, identifying, classifying, assessing, and mitigating risks associated with port infrastructures and security and safety incidents. CYSM risk management tool has been developed in the EU CIPS Project CYSM under the Horizon2020 program. It has been developed based on several 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 proposed Collaborative CYSM system, presenting the supported functionality and the adopted processes.

The CYSM system is an innovative, scalable Risk Assessment Toolkit that 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 that constitute the conceptual pillars for building a solution that assists ports to improve their current cyber and physical level. In this context, for CYSM to support sound decision-making, it does the following:

- 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;

- incorporates a collaborative, multiattribute, 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 semiautomated risk assessment routines and processes to (1) determine the value of the information assets; (2) identify the applicable threats and vulnerabilities that exist (or could exist); (3) identify the existing controls and their effect on the risk identified; (4) determine the potential consequences; and (5) 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 will facilitate and encourage 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 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, i.e., Cyber Risk Assessment Services, Physical Risk Assessment Services, and the Security Framework Service. 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 (Fig. 3.1).

CYSM System Components

For the proposed system to meet its objectives, it integrates a set of primary components. From a conceptual perspective, the main components are the following:

- *Community Portal*: This area is accessible by all users of the involved ports in the CYSM community and comprises the following:
  - Community 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

Figure 3.1 Collaborative cyber/physical security management (CYSM) system.

opinions, thoughts and contributions, and sharing information, experience, and expertise;
- Community 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 own port infrastructure. This area executes the risk assessment processes and routines integrated in the system and consist of the following modules:
  - 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., that is valuable, private knowledge for the port;
  - 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.

These components 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.

Showcase Scenario

The scope of this section is to describe a use case to illustrate the functionality of the CYSM system. The scenario involves a commercial port, Piraeus Port Authority (PPA), that supports several business operations including the transport and accommodation of people, freight, natural gas, oil, cargos, 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 cargos) facilities. According to the scenario, the security officer (SeOf) of the PPA utilizes the CYSM system 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 SeOf via dynamic, interactive, and evolutionary interfaces to perform the evaluation process (Fig. 3.2). This process can be divided into the following five phases:

Customization Phase

Initially, the SeOf, authenticates himself (using his credentials) into the CYSM system. Upon approval the SeOf gains access to the Community

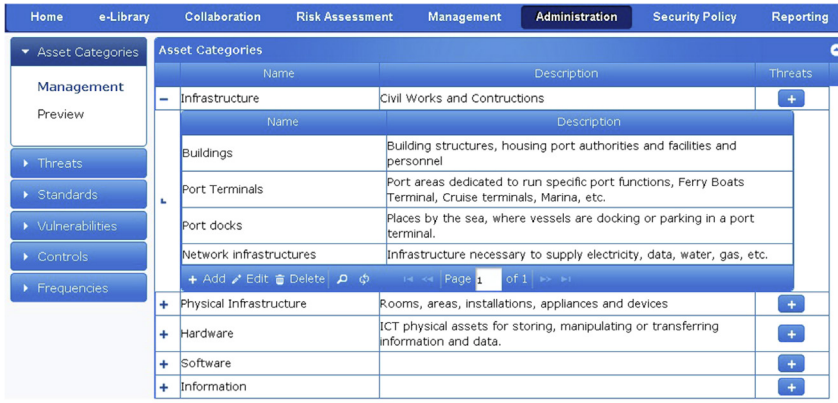

Figure 3.2 CYSM Administration module.

Portal and is directed to the PPA Private Portal where he accesses the Administration module. This module allows the SeOf to set various boundaries and constraints:

- to manage the list of threats that is facing the port;
- to manage the list of vulnerabilities;
- to manage the list of controls that are deployed or can be applied from the organization to mitigate the risks and deal with their defined threats and weaknesses;
- to define the correlation among controls, vulnerabilities, and threats;
- to manage the list of the assets categories and asset subcategories based on which cyber and physical assets will be classified and to define the threats that are applicable to each asset category;
- to manage the standards against which the port's cyber and physical facilities will be assessed;
- to define the correlation between the controls that can be applied from a port and the requirements imposed by the standards;
- to 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).

The SeOf should update the content 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.

Risk Assessment Initiation Phase

After the successful customization of the system, the SeOf accesses the Management module where he can initiate a risk assessment (Fig. 3.3). For the definition of a new assessment, the SeOf should specify: (1) the basic information (e.g., name, the start and end date, and a short description); (2) the boundaries of the risk assessment (the physical or ICT port facility that will be assessed); (3) the departments that will be involved and the role and weight of each department to the risk procedure; and finally (4) the standards or the areas of the standards (ISO27001 and ISPS code) against which the defined area will be evaluated.

Evaluation Phase

Having initiated the risk assessment, all the members (participants) of the departments are invited to participate in the risk assessment process, login to the CYSM system using their accounts, and access the Risk Assessment

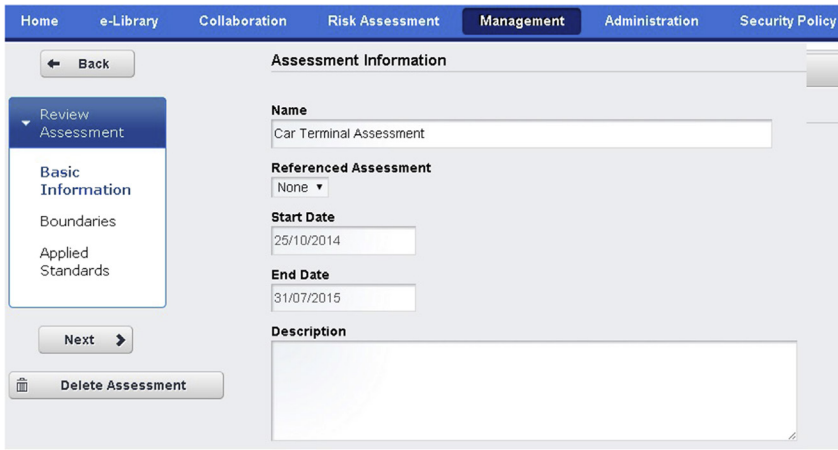

Figure 3.3 CYSM Management module.

Figure 3.4 CYSM Risk Assessment module.

module of the PPA Private Portal (Fig. 3.4). In this module, a list of the available assessments appears, and the participants select the assessment related to the evaluation of the Cruising Facility to complete the following steps:

1. *Assets Identification*: Define the assets that comprise the Cruising Facility and categorize them in the main categories and subcategories defined in the Administration module.
2. *Impact Assessment*: Determine the value of each of them to the organization. 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.

Figure 3.5 CYSM Risk Assessment Results module.

3. *Control Identification*: Define the controls applied to each asset.
4. *Threat Assessment*: Estimate the likelihood of occurrence of a predefined list of threats to each asset.

Risk Assessment Results Calculation and Review Phase

Once all the participants completed the evaluation phase, the SeOf accesses the Risk Assessment Results module (Fig. 3.5) to produce and review the results of the risk assessment. More specifically, the SeOf 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 who completed the evaluation. Now, the SeOf can review the produced results based on those he can select and prioritize the countermeasures that should be adopted in the PPA to handle and mitigate the identified risks. In this way, the SeOf can formulate an effective and efficient risk mitigation plan.

Security Policy Reporting Phase

Finally, the SeOf accesses the Security Policy Reporting module (Fig. 3.6) 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 system is a security management revolutionary consultation environment that is oriented to the special requirements of ports and is in

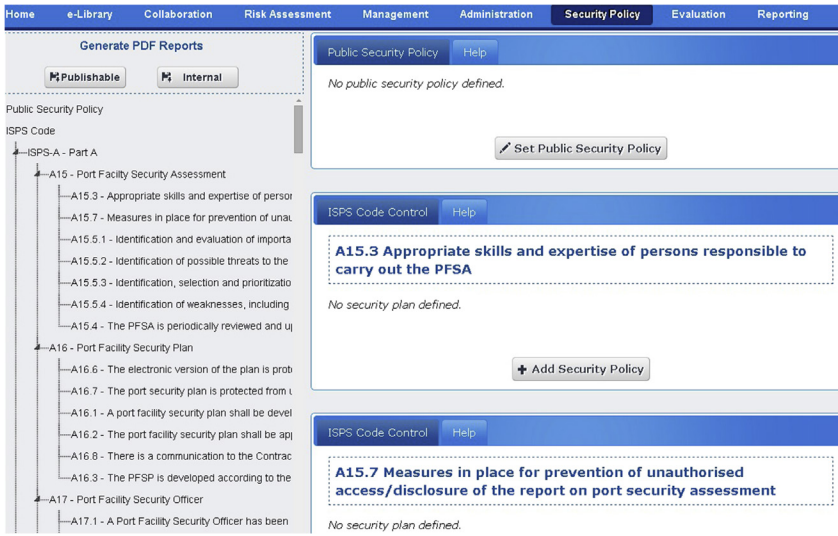

Figure 3.6 CYSM Security Policy Reporting module.

accordance to the basic principles and the business goals of existing risk assessment standards and methodologies. The nature of the system is associated with a high degree of 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.

CYSM Architecture

The CYSM Risk Assessment Toolkit adopts and implements the functions and procedures presented in the previous sections. For the CYSM Risk Assessment Toolkit to meet its objectives, it incorporates and merges a set of integrated and interconnected subsystems (Fig. 3.7). From a conceptual perspective, the required subsystems are the following:

The **Web Interactive component** provides an intuitive, interactive, and graphic way (e.g., dynamic forms) to represent the information and content (e.g., requirements, rules, obligations, recommendations, and advices of the legal, regulatory, and standardization framework and regime as well as security and safety content required for automating technical control compliance, vulnerability checking, and security measurement activities) of the risk assessment services. It is designed to be a single environment where all the applications a user needs can run, and these are integrated together in a consistent and systematic way.

Figure 3.7 CYSM Risk Assessment Toolkit architecture.

If an application lives outside of the main CYSM portal, the portal should be able to consume some resource of the application (such as an RSS feed or a subset of functionality in a "dashboard" application), so the end user will be able to see everything he/she interacts with at a glance.

To achieve this, all the application functionality within **CYSM Web Interactive component** is in fragments of the page, called portlets. Portlets are Web applications that run in a portion of a Web page. Within the proposed platform, the portlet container is the most important architectural bone. The container's job is to aggregate the set of portlets that are to appear on any page and display them properly to the user. In this way, one or many applications reside on a page, and the user can (at the administrator's discretion) arrange them in the way that works best for the user.

Portlet applications, like servlet applications, have become a Java standard, which various portal server vendors have implemented. The Java standard defines the portlet specification. A JSR-168 or JSR-286 standard portlet is deployable on any portlet container, which supports those standards. Portlets are placed on the page in a certain order by the end user and are served up dynamically by the portal server.

Portal applications come generally in two flavors:

1. multiple portlets written to provide small amounts of functionality and aggregated by the portal server into a larger application;
2. whole applications written to reside in only one or a few portlet windows.

Portlets are not difficult to build, and Java standard portlets can be written by any Java developer with experience in writing Web applications.

CYSM platform provides a Plugins Software Development Kit that makes the creating of portlet projects easy.

Platform administrators can use the Dockbar, which is the primary tool logged in that users have for navigating the portal and accessing administrative functions from anywhere on the Web site. Depending on the logged-in user's roles and what section of the CYSM portal the user is viewing, all or only some of the options are available in the Dockbar.

Moreover, administrators can use the Manage menu in which they are able to access various settings for the current page and any of its subpages. The items available are Page, Page Layout Sitemap, and Settings. With Page Layout a user can choose the layout template to use for the current page. The other settings are the same as their counterparts in the Control Panel, which is also an important option for configuring appropriately the portal and its functionality.

With the usage of the Toggle Edit Controls a user can turn on and off the edit controls of the portlet windows. This is helpful for administrators who want to look at a page they are working on and see it the way a regular user would.

Additionally, in the Dockbar a user can be informed of all the places in the portal to which he has access. CYSM platform allows for various configurations of pages for end users: configure it so that some or all users have their own pages, public and private (or both), upon which they can place the portlets they need to use. The administrator account by default has its own pages.

One of the most important tools CYSM platform offers for managing the portal is the Control Panel. The Control Panel is composed of administrative portlets that a user can use to manage various aspects of the portal.

The **Semantic Modeling component**, on the other hand, integrates a collection of semantic structures (notably ontologies/taxonomies) modeling:

- the security and safety posture of the ports;
- the employees of ports based on their cognitive state and behavior regarding their role and responsibilities in their enterprise, existing background knowledge about security and safety, and level of their interaction with the port infrastructure;
- all the cyber and physical aspects (e.g., security and safety-related legal, regulatory and standardization framework and tools, etc.);
- their semantic relationships providing a modularization of knowledge.

This module is responsible for the content categories that are defined by someone with administrative access to the content. They are hierarchical, tree-like structures that users can use to find content. Categories are different from tags in that they are never created by end users. Instead, categories define how the content is organized from the point of view of the owner of the content (e.g., ports). A good example of categories might be the organization of a port: it shows the hierarchical structure and organization for all the departments within that port.

The **Execution Engine component** incorporates an automated workflow tool that executes all the underlying complex processes and routines defined by the proposed CYSM Risk Management Methodology (CYSM-RM) of the services, providing a high degree of automation and transparency. Also, this component undertakes the responsibility using elements of the Web Interactive component (e.g., online forms) to guide and direct the users to perform the required activities and actions.

CYSM workflows are essentially a predetermined sequence of connected steps. In a CYSM system, each workflow is designed to manage the creation, modification, and publication of Web content. An administrator can set up a workflow so that content cannot be published without going through an approval process designed. In this way, content goes up on the site only after it has been reviewed and approved.

The CYSM system's workflow engine allows a privileged user to define any number of simple to complex business processes/workflows, deploy them, and manage them through a portal interface (Web Interactive Tier). Those processes have knowledge of users, groups, and roles without writing a single line of code; it only requires the creation of a single XML document. This document is executed by the end users on the portal. Administrators can create as many different workflow definitions as they need to manage the work done on their portal.

The key parts of the workflow definition are the asset, states, transitions, and tasks. The asset is whatever piece of content is being reviewed and approved in the workflow. States represent stages of the workflow, for example, created, rejected, or approved. Transitions occur between states, and indicate what the next state should be. Tasks are steps in the workflow that require user action.

The **Interaction component** embodies mechanisms and interfaces that implement a set of standards and languages to encapsulate information from other services and automated tools in an automated and transparent

way. This component integrates all the characteristics of an enterprise service bus, which is a software architecture construct that lives between the (business) applications, enabling communication among them. Ideally, it replaces all direct contact with the applications on the component itself, so all communication takes place via it.

The Interaction component provides its fundamental services via an event-driven and standards-based messaging engine (the bus). Through its utilization, integration architects can exploit the value of messaging without writing code. Developers can use technologies found in a category of middleware infrastructure products, usually based on recognized standards.

With this component, a potential author such as the CYSM technical team can filter, transform, route, and manipulate SOAP, binary, plain XML, and text messages that pass through his business systems by HTTP, HTTPS, JMS, mail, etc.

Finally, the **Advanced Security Intelligence Engine** delivers analysis of all activity observed within the ports' environment in an effective and efficient manner. The component incorporates the proposed CYSM Risk Management Methodology (CYSM-RM) and a set of technologies for enumerating, describing, measuring/quantifying, and encapsulating data (e.g., findings, threats and vulnerabilities metrics, and prioritization of countermeasures). With a practical combination of flexibility, usability, and comprehensive data analysis, the proposed engine delivers visibility to risks, threats, and critical operations issues. Also, it provides a full lifecycle of security and safety management by incorporating the following components:

- The Asset Identification component encompasses the mechanisms required to collect and gather the critical information and physical assets of the evaluated ports' facilities. These aspects are not confined only to technical issues, but they are also concerned with the business and physical processes in which the systems are embedded.
- The Evaluation component integrates the appropriate means to assess the security and safety of ports' operational environment. This component conducts an analysis to pinpoint threats and vulnerabilities and assigns a rank to each based on the risk potential verses consequences. Finally, it can make recommendations on how best to minimize against these consequences.

The Asset Identification component plays an important role in all integrated CYSM services and especially in the Risk Assessment service. It is

required from each port to quickly correlate different sets of information about its assets. The CYSM platform provides the necessary constructs to uniquely identify assets based on known identifiers and/or known information about the assets. Within the CYSM platform for the asset identification, different categories of assets have been already defined and properly integrated. These are as follows:

- infrastructures (e.g., buildings, terminals)
- physical assets (lockers, cabinets, etc.)
- hardware assets (e.g., servers, routers, switches)
- software assets (operating systems, applications, etc.)
- data assets (e.g., electronic data, paper-based/printed data)

The Evaluation component, on the other hand, refers to the risk treatment plan, which is part of the risk management plan for each port. It outlines how risks will be managed whether they are low, high, or acceptable risks according to the management decision of each port.

The CYSM system serves as a best practice example of a targeted (physical and cyber) risk management tool for ports' operators. It adopts a simplified and optimized approach as a response to the transitional time-consuming risk assessment procedures. The proposed approach is represented through several customized and specialized self-risk assessment processes that are modeled and implemented in the system in a graphic approach using visualization tools, automated routines, processes, and structured content that encapsulate several simplifications and incorporate automated steps. CYSM offers open source "easy to use" tools enabling the security and safety management in intuitive and graphic way. In a nutshell, the basic design principles of all the related functions developed within CYSM include these:

- *Easy to use for nonexperts*. Simplification and automation of the supported risk assessment procedures and activities makes it 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 workflows and routines and online intuitive and interactive graphic representations (e.g., dynamic questionnaires) to use the provided functionality.
- *Collaborative*. The risk assessment process is treated as a participatory challenge among various user groups with a different vision angle for each one and different standards, respectively. In this context, CYSM calculates the actual risk factor based on the opinion of all involved users and not only to persons that are involved with security and safety,

considering their experience and expertise and the different points of observations. CYSM raises the security awareness and consciousness of all port operators and users.

The CYSM system has been tested and evaluated by several commercial ports (including Port of Piraeus, Valencia Port Authority, and Port of Mykonos) during the CYSM project (in the pilot operation phase). 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 online services of the CYSM system.

Finally, CYSM promotes a holistic approach to the security and safety management for ports. This approach is based on flexible semantic infrastructure and tagging mechanisms for security policies and other relative security and safety data. The provision of such structured knowledge enables ports to handle their cyber and physical issues in an effective and unified manner and facilitates their cooperation, encouraging working together on issues of mutual concern.

CYSM is not a product but a research initiative that can serve as a best practice in the development of new ICT security management tools that are compliant with the ISO 27001, CIIP, and ISPS, helping the port operators to better manage their physical and cyber risks within their CIIs.