

Collaborative Security Management Services for Port Information Systems

Ημερίδα Λιμενικού Σώματος
- Ελληνικής Ακτοφυλακής

Athens, Greece
December 2015



ΟΠΑ
AUEB

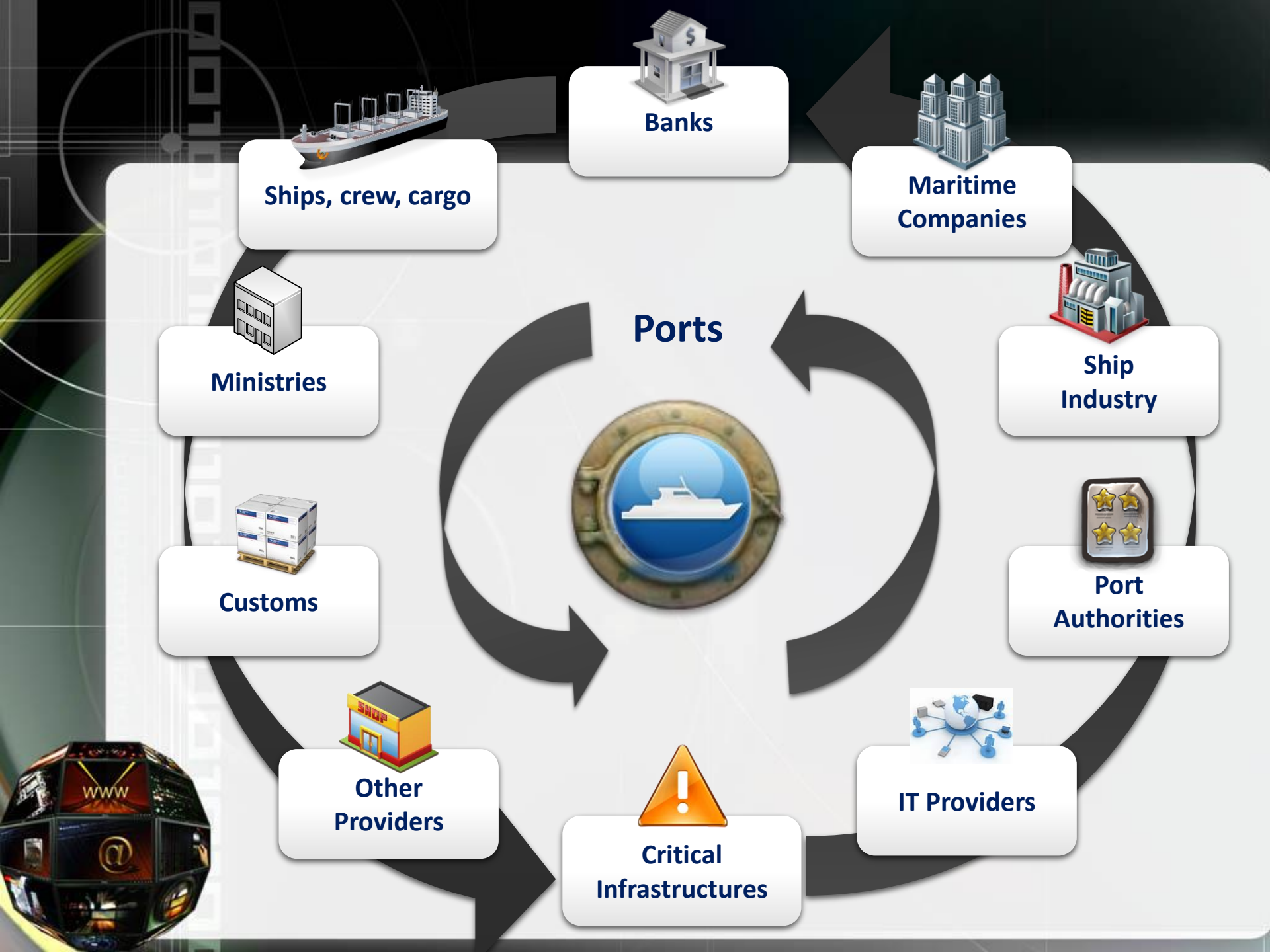
Theodoros Ntouskas & Dimitris Gritzalis

Information Security & Critical Infrastructure Protection Laboratory
Dept. of Informatics | Athens University of Economics & Business

Critical Infrastructures: Security needs

- **Critical infrastructures:** Large-scale infrastructures that their degradation/interruption/impairment of their ICT has **vital impact** on health, safety or welfare of citizens.
- The normal functionality of critical infrastructures depends largely on the proper operation of **Information and Communication Systems**.
- The **large amount of critical and sensitive data**, the information and services that are managed on a daily basis, the large number of users and citizens called to be served, require effective **Security Management**.





Transportation and Ports

- ✓ **Transportation** is a key economic sector, facilitating the movement of people, food, water, medicines, fuel, etc. **Port Authorities** play an important role in the international trade and economy environment.
- ✓ In EU >50% of the goods traffic (2010) was carried by Maritime Transport and 90% of the EU external trade took place through the Maritime Sector.
- ✓ Transportation infrastructures face **multiple threats**, ranging from physical disasters, sabotage, insider threats, terrorist attacks, etc.
- ✓ Examples are the events in New York and Washington (2001), Madrid (2004), London (2005) and Italy (2012). The common element of these incidents is the use of **transportation infrastructure components**.
- ✓ The increasing need for protecting transport infrastructures is recognized by most countries; the **transportation sector** is among the sectors recognized as **critical**.
- ✓ **Assessing risk in critical infrastructures** requires a novel approach due to the high complexity, multiple interdependencies and heterogeneity of the port environment.



Open issues

Information Security

Physical Security

Users

(internal + all entities in the maritime environment)

Information/data

(traffic monitoring, marine, coastal, trade, lists, trade data...)

Services

(invoicing, navigation, luggage/cargo/vessel management, logistics,...)

Systems and Software

(transmission systems, maritime navigation, ERP, GIS, ticketing, ...)

ICT Infrastructure

(networks, satellites, relay stations ..)

Physical Infrastructure

(buildings, terminals, data centers, platforms, gates, marinas, ..)

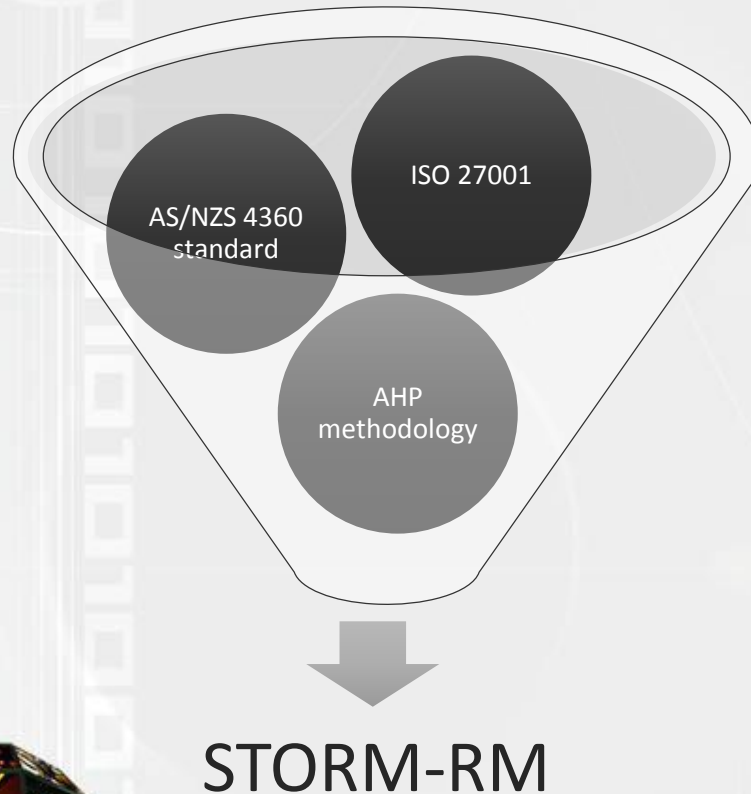


Baseline requirements

- **Compatible with standards:** ISO27001 and sector specific (e.g. CIIP standards and ISPS for maritime sector)
- **Collaboration:** Ensure collaboration among all ICT users
- **Group decision making:** Use group decision making algorithms
- **Interdependencies:** Interdependency analysis
- **Broad analysis:** Analyse interconnected and interdependent threats and evaluate direct and indirect risks
- **Time and resource economical:** Avoid the plethora of questionnaires and frustrating interviews with all participants
- **Easy to implement:** Expert should not need high level of expertise to apply the methodology
- **Open:** Avoid security through obscurity



Ideas and suggestions



STORM-RM methodology

- ❑ Uses multi-criteria collaborative decision making technique: *Analytic Hierarchy Process (AHP)*
- ❑ Takes into account the knowledge of all organizational users
- ❑ Enables all users (internal & external) to evaluate the security impacts
- ❑ It is algorithmic
- ❑ Allows parameterization (change no. of participants, weights, criteria, etc.)



The S-PORT project

➤ Objectives

- ❑ Development of a security management collaborative methodology for critical PIT-systems
- ❑ Collaborative generation, monitor, and update of security management docs in the open source S-Port system

➤ Funded by

General Secretariat for R&D, Ministry of Development

➤ Partners

Univ. of Piraeus (PM)

Athens Univ. of Economics & Business

INTRASOFT International

MVNS

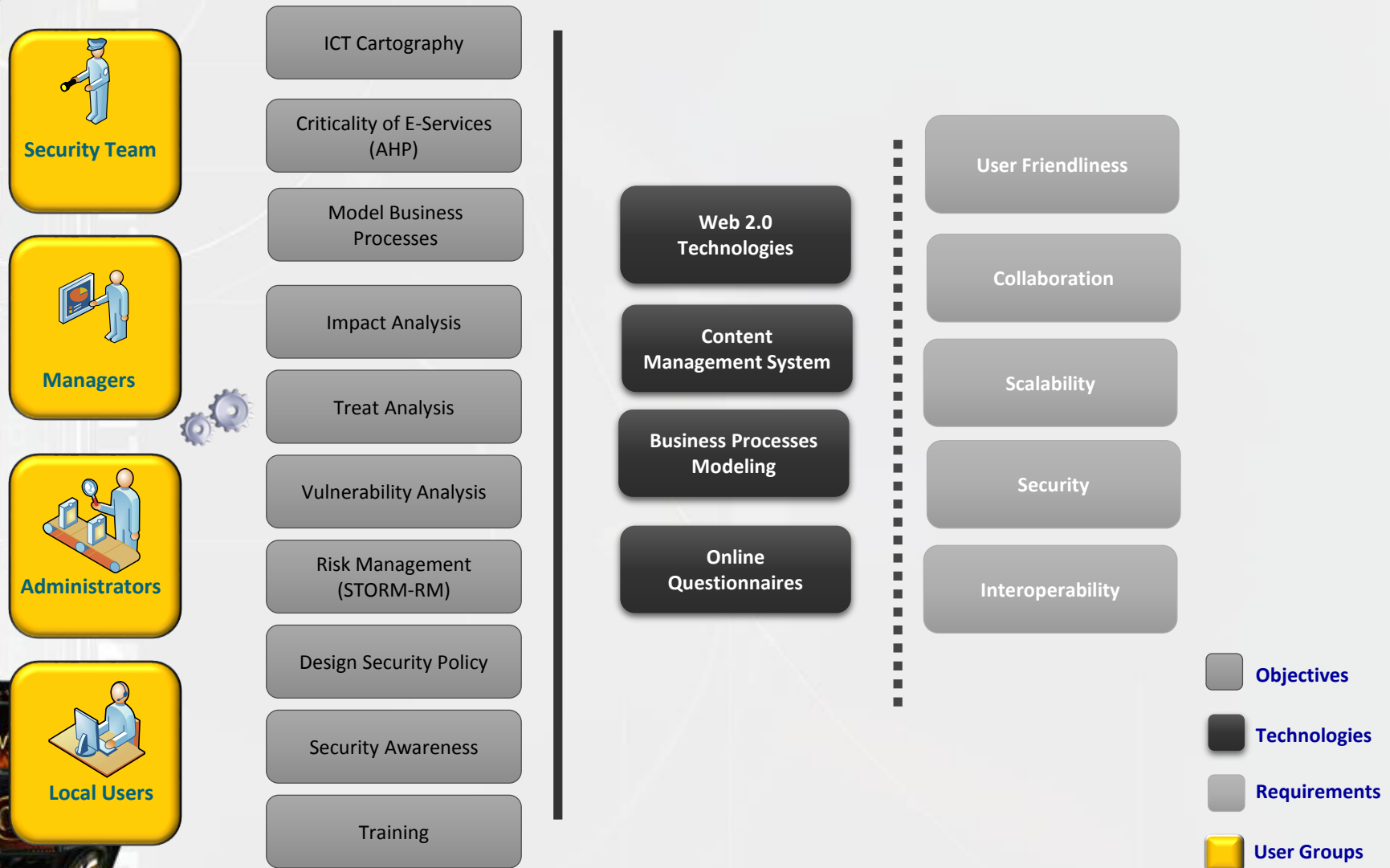
Piraeus Port Authority

Thessaloniki Port Authority

Mykonos Municipal Port Fund



S-PORT: Objectives and requirements



S-PORT: Services



Risk Assessment Services (STORM-RM)

Cartography

Impact Analysis

Threat Analysis

Vulnerability
Analysis

Risk Analysis

Risk Management

Proposed
Countermeasures

Selection of
Countermeasures

Collaborative Services

Forum

Wiki

E-Library

Chat Rooms

Blog

Security Documents

Design Security
Policy

Design DRP



A secure, collaborative environment for the security management of Port Information Systems

[Home](#)[Cartography](#)[Risk Assessment](#)[Risk Management](#)[Security Policy](#)[Collaboration](#)[Library](#)[Logout](#)

Phase 1: Cartography

[Help for Phase 1 Cartography](#)[Infrastructure Identification](#)[E-Services Identification - Assessment](#)[E-Services Identification](#)[E-Services Assessment](#)[Asset Identification](#)

List of E-Services

Code	Name	Description	Manager Name	Manager Last Name	Manager Email	Created at	Updated at	Actions
service1	service1	Description	Manager	Lastame	email1	10 / 24 / 2011	06 / 02 / 2012	
service2	service2	Description	Name	Lastame	email3	10 / 24 / 2011	06 / 02 / 2012	
service3	service3	Description	Name	Lastame	email4	10 / 27 / 2011	06 / 02 / 2012	
service4	service4	Description	Name	Lastame	email	11 / 03 / 2011	06 / 02 / 2012	

[Print the list of E-Services](#)

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ
ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗΣ
ΚΑΙ ΘΡΗΣΚΕΥΜΑΤΩΝ





A secure, collaborative environment for the security management of Port Information Systems

Home Cartography Risk Assessment Risk Management Security Policy Collaboration Library Logout

Risk Assessment

Help for Risk Assessment

service1

Impact Assessment

Threat Assessment

Vulnerability Assessment

service2

service3

service4

Impact Assessment for the assets of SERVICE:

service1

Data Assets

Systems

Results

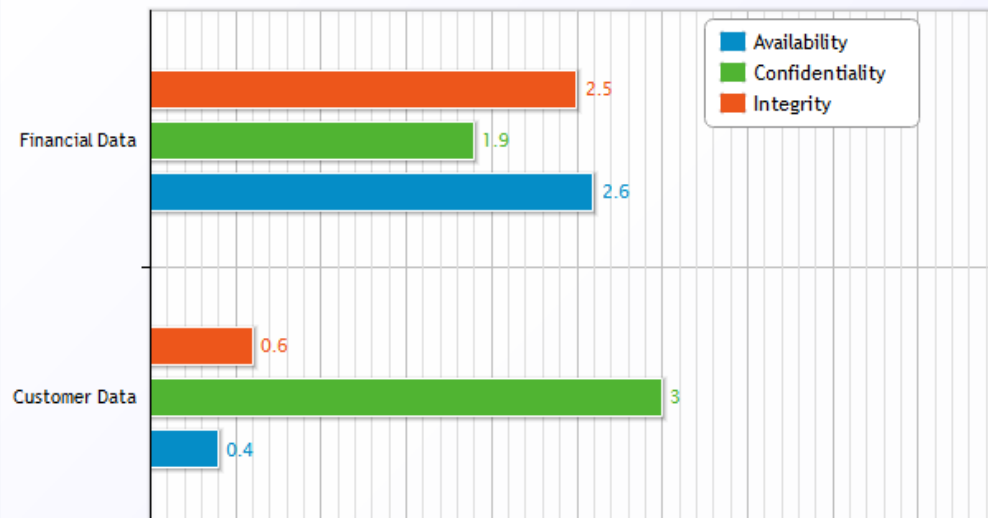
Group Results

Total Results


Final Impact Results

Availability	Confidentiality	Integrity	Total Value	Asset	Port
2.6	1.9	2.5	2.6	Financial Data	Organization 1
0.4	3	0.6	3	Customer Data	Organization 1
0.4	1	1	1	Data2	Organization 1
0.4			0.4	datatritis	Organization 1

service1 Impact Assessment



Risk Management

 Help

S-PORT RM Results

Impact Assessment Results


Threat Assessment Results


Vulnerability Assessment Results


Risk Assessment Results


Proposed Countermeasures

Risk Assessment Results: June 2, 2012 10:36:58 AM EEST

 Risk Matrix

 Risk Evaluation Matrix

 Risk Scale

 Print Results



Data Assets

S/W - H/W

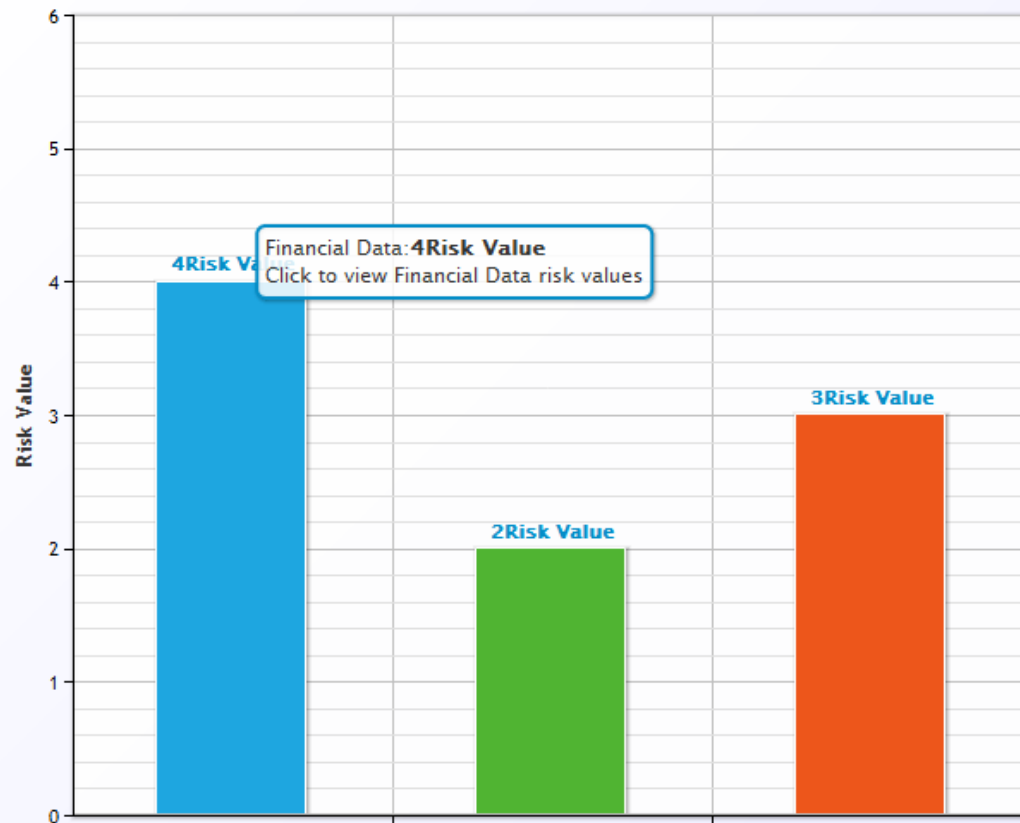
Per Threat

Per Asset

Overall Risk Assessment Results - Per Asset

Risk Assessment Results

Click the columns to view the risk values. Click again to view max values of assets.





A secure, collaborative environment for the security management of Port Information Systems

[Home](#) [Cartography](#) [Risk Assessment](#) [Risk Management](#) [Security Policy](#) [Collaboration](#) [Library](#) [Logout](#)

Forums

[New topic](#)

2 topics, 3 messages

Forum	Topics	Messages	Last Message
Public Boards			
Cartography	1	2	test no222 4 days ago by demo
Risk Assessment Survey help	1	1	test2 4 months ago by teo
Disaster Recovery Plan			



ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ
ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗΣ
ΚΑΙ ΘΡΗΣΚΕΥΜΑΤΩΝ





A secure, collaborative environment for the security management of Port Information Systems

Home Cartography Risk Assessment Risk Management Security Policy Collaboration Library Logout

Security Policy

Help

Security Policy

Disaster Recovery Plan

Disaster Recovery Managers

Disaster Recovery Logistics Team

Recovery Site Managers

Disaster Recovery Hardware Team

Disaster Recovery Software Team

Disaster Recovery Network Team

Disaster Recovery Helpdesk Team

Disaster Recovery Operations Team

Disaster Recovery Applications Team

Disaster Recovery Managers

DRP Phase	Responsibilities
Development	<ul style="list-style-type: none">Oversee the documenting, publishing and dissemination of DRPUpdate the DRP manual when infrastructure, operations or organisation changes in Computer Centre impact the DRP.
Testing	<ul style="list-style-type: none">Schedule, organise and staff DR tests in collaboration with Disaster Recovery teams, on fixed schedule or when need arises
Normal Operation	<ul style="list-style-type: none">Update DRP and DR Handbook via Change Management procedures when infrastructure, operations or organization changes in Computer Centre impact the DRPEnsure DRP terms and policies are applied at all levels in Computer CentreEscalate issues to DR Steering Committee, when its intervention is needed. Issues may involve policy or technical aspectsMeet DR team members at regular intervals for update on issues potentially impacting the viability of the DRP

Role	Name	Address	Cell Phone	R/S Desk Loc
DR Coordinator	Theodore Ntouskas	karaoli 2	25252525	main site

Update

PDF



ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ
ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗΣ
ΚΑΙ ΘΡΗΣΚΕΥΜΑΤΩΝ





A secure, collaborative environment for the security management of Port Information Systems

[Home](#) [Cartography](#) [Risk Assessment](#) [Risk Management](#) [Security Policy](#) [Collaboration](#) [Library](#) [Logout](#)

[View](#) [Edit](#) [History](#) [Index](#)

🏠 [index](#)

[wiki](#)
[forum](#)
[blog](#)
[chat](#)

index

1. Introduction

This section provides an introduction to the principles of risk management. The vocabulary of risk management is defined in ISO Guide 73, "Risk management. Vocabulary." [2] [home](#)

In ideal risk management, a prioritization process is followed whereby the risks with the greatest loss and the greatest probability of occurring are handled first, and risks with lower probability of occurrence and lower loss are handled in descending order. In practice the process can be very difficult, and balancing between risks with a high probability of occurrence but lower loss versus a risk with high loss but lower probability of occurrence can often be mishandled.

Intangible risk management identifies a new type of a risk that has a 100% probability of occurring but is ignored by the organization due to a lack of identification ability. For example, when deficient knowledge is applied to a situation, a knowledge risk materializes. Relationship risk appears when ineffective collaboration occurs. Process-engagement risk may be an issue when ineffective operational procedures are applied. These risks directly reduce the productivity of knowledge workers, decrease cost effectiveness, profitability, service, quality, reputation, brand value, and earnings quality. Intangible risk management allows risk management to create immediate value from the identification and reduction of risks that reduce productivity.

Risk management also faces difficulties allocating resources. This is the idea of opportunity cost. Resources spent on risk management could have been spent on more profitable activities. Again, ideal risk management minimizes spending and minimizes the negative effects of risks.

Method

For the most part, these methods consist of the following elements, performed, more or less, in the following order.

1. identify, characterize, and assess threats
2. assess the vulnerability of critical assets to specific threats
3. determine the risk (i.e. the expected consequences of specific types of attacks on specific assets)
4. identify ways to reduce those risks
5. prioritize risk reduction measures based on a strategy

Table of contents

- [1. Introduction](#)
 - [Method](#)
 - [Principles of risk management](#)
- [2. Process](#)
 - [Establishing the context](#)
 - [Identification](#)
 - [Assessment](#)



A secure, collaborative environment for the security management of Port Information Systems

Home Cartography Risk Assessment Risk Management Security Policy Collaboration Library Logout

S-Port Taxonomy

- ✓ S-Port Digital Library
 - ✓ European Level
 - ✓ Directives
 - ✓ Good Practices
 - ✓ Other
 - ✓ Programmes & Initiatives
 - ✓ Regulations
 - ✓ Relevant Organisations & Authorities
 - ✓ Research & Studies
 - ✓ Statistics
 - ☐ Greece
 - ☐ Good Practices
 - ☐ Legislation
 - ☐ National Policies & Practices
 - ☐ Other
 - ☐ Programmes & Initiatives
 - ☐ Relevant Organisations & Authorities
 - ☐ Research & Studies
 - ☐ Statistics
 - ☐ ISPS Code
 - ☐ ISPS Best Practices
 - ☐ ISPS Code & Revisions
 - ☐ Other Relevant Information
 - ☐ International Level
 - ☐ Good Practices
 - ☐ Programmes & Initiatives
 - ☐ Relevant Organisations & Authorities
 - ☐ Research & Studies
 - ☐ Statistics
 - ☐ Other Information
 - ☐ Other Relevant Information About
 - ☐ Other Useful Security Standards
 - ☐ Security Tools Manuals

S-PORT Library - Upload File

Document Title*:	<input type="text"/>
Description*:	<input type="text"/>
Select File*:	<input type="button" value="Choose File"/> No file chosen
Selected Tags*:	Europe,EU_Directives,EU_GoodPractices,EU_Other,EU_ProgrammesInitiatives,EU_Regulations,EU_OrganisationsAuthorities,EU_ResearchStudies,EU_Statistics
<input type="button" value="Save"/>	

Generic conclusions and some proposals

- S-Port is a useful asset for the security management of the PIS, providing continuity and rendering of services
- With S-Port, Port Authorities and their IS will adopt all the rules and procedures of the ISPS Code, thus reducing possibility of threats and maximizing their productivity
- Collaborative Risk Management methodologies need to be further developed
- Maritime interoperable Security Management Tools (MSMT) (like S-Port) should be developed so as to:
 - Implement the MSMM as collaborative friendly interoperable services (based on open standards)
 - Be cost effective (open source)
 - Enable collaboration among users in the maritime environment



References

1. Gritzalis D., "Insider threat prevention through Open Source Intelligence based on Online Social Networks", Keynote address, *13th European Conference on Cyber Warfare and Security* (ECCWS-2014), Greece, 2014.
2. Kotzanikolaou P., Theoharidou M., Gritzalis D., "Risk assessment of multi-order interdependencies between critical information and communication infrastructures", *Critical Information Infrastructure Protection and Resilience in the ICT Sector*, pp. 151-170, IGI Global, 2013.
3. Kotzanikolaou P., Theoharidou M., Gritzalis D., "Accessing n-order dependencies between critical infrastructures", *International Journal of Critical Infrastructure Protection*, Vol. 9, Nos. 1-2, pp. 93-110, 2013.
4. Kotzanikolaou P., Theoharidou M., Gritzalis D., "Cascading effects of common-cause failures on Critical Infrastructures, in *Proc. of the 7th IFIP International Conference on Critical Infrastructure Protection*, pp. 171-182, Springer (AICT 417), USA, March 2013.
5. Kotzanikolaou P., Theoharidou M., Gritzalis D., "Interdependencies between Critical Infrastructures: Analyzing the Risk of Cascading Effects", in *Proc. of the 6th International Workshop on Critical Infrastructure Security*, pp. 107-118, Springer (LNCS 6983), Switzerland, September 2011.
6. Ntouskas, T., Pentafronimos G., Papastergiou, S., "STORM - Collaborative Security Management Environment", in *Proc. of WISTP-2011*, Springer, LNCS 6633, pp. 320-335, 2011.
7. Ntouskas, T., Polemi, N., "STORM-RM: a collaborative and multicriteria risk management methodology", *Int. Journal of Multicriteria Decision Making*, Vol. 2, No. 2, pp. 159-177, 2012.
8. Ntouskas T., Kotzanikolaou P., Polemi N., "Impact Assessment through Collaborative Asset Modeling: The STORM-RM approach", in *Proc. of the 1st International Symposium & 10th Balkan Conference on Operational Research*, Thessaloniki, Greece, 2011.
9. Polemi D., Ntouskas T., Georgakakis E., Douligeris C., Theoharidou M., Gritzalis D., "S-Port: Collaborative security management of Port Information Systems", in *Proc. of the 4th International Conference on Information, Intelligence, Systems and Applications*, IEEE Press, Greece, 2013.
10. Theoharidou M., Kotzanikolaou P., Gritzalis D., "Risk-based Criticality Analysis", in *Proc. of the 3rd IFIP International Conference on Critical Infrastructure Protection*, Springer, USA, March 2009.
11. Theoharidou M., Kotzanikolaou P., Gritzalis D., "A multi-layer criticality assessment methodology based on interdependencies", *Computers & Security*, Vol. 29, No. 6, pp. 643-658, 2010.
12. Theoharidou M., Kotzanikolaou P., Gritzalis D., "Risk assessment methodology for interdependent Critical Infrastructures", *International Journal of Risk Assessment and Management*, Vol. 15, Nos. 2/3, pp. 128-148, 2011.
13. Theoharidou M., Kandias M., Gritzalis D., "Securing Transportation-Critical Infrastructures: Trends and Perspectives", in *Proc. of the 7th IEEE International Conference in Global Security, Safety and Sustainability*, pp. 171-178, Springer (LNICST 99), Greece, 2012.
14. Stergiopoulos G., Theoharidou M., Kotzanikolaou P., Gritzalis D., "Using centrality measures in dependency risk graphs for efficient risk mitigation", in *Critical Infrastructure Protection IX*, pp. 25-40, Springer, 2015.
15. Stergiopoulos G., Kotzanikolaou P., Theoharidou M., Gritzalis D., "Risk mitigation strategies for Critical Infrastructures based on graph centrality analysis", *International Journal of Critical Infrastructure Protection*, September 2015.
16. Stergiopoulos G., Theoharidou M., Gritzalis D., "Using logical error detection in remote-terminal units to predict initiating events of Critical Infrastructures failures", *Proc. of the 3rd International Conference on Human Aspects of Information Security, Privacy & Trust*, Springer, USA, 2015.