

# Innovative Security Management Services for Maritime Environment



**ΟΠΑ**  
AUEB

**Theodoros Ntouskas, Dimitris Gritzalis**

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

# Innovative Security Management Services for Maritime Environment

NMIOTC Cyber Security Conference

Chania, Greece  
October 2016



**ΟΠΑ**  
AUEB

**Theodoros Ntouskas & Dimitris Gritzalis**

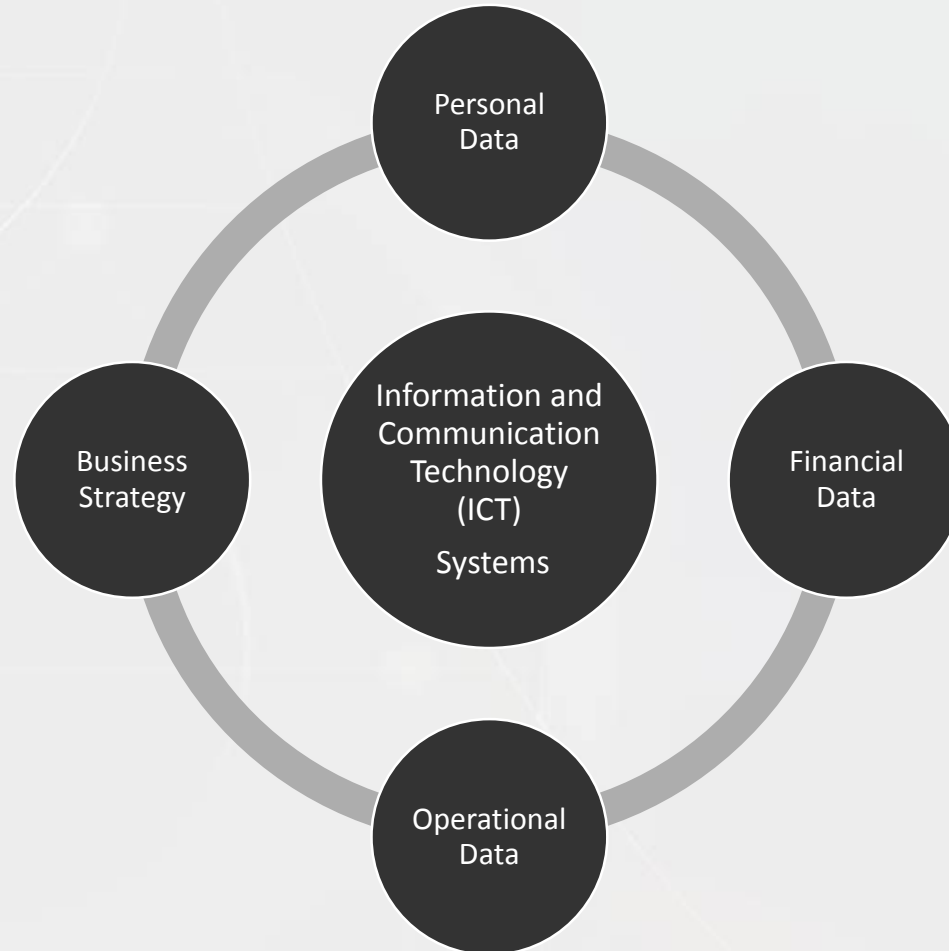
Information Security & Critical Infrastructure Protection Laboratory  
Dept. of Informatics | Athens University of Economics & Business

# Topics

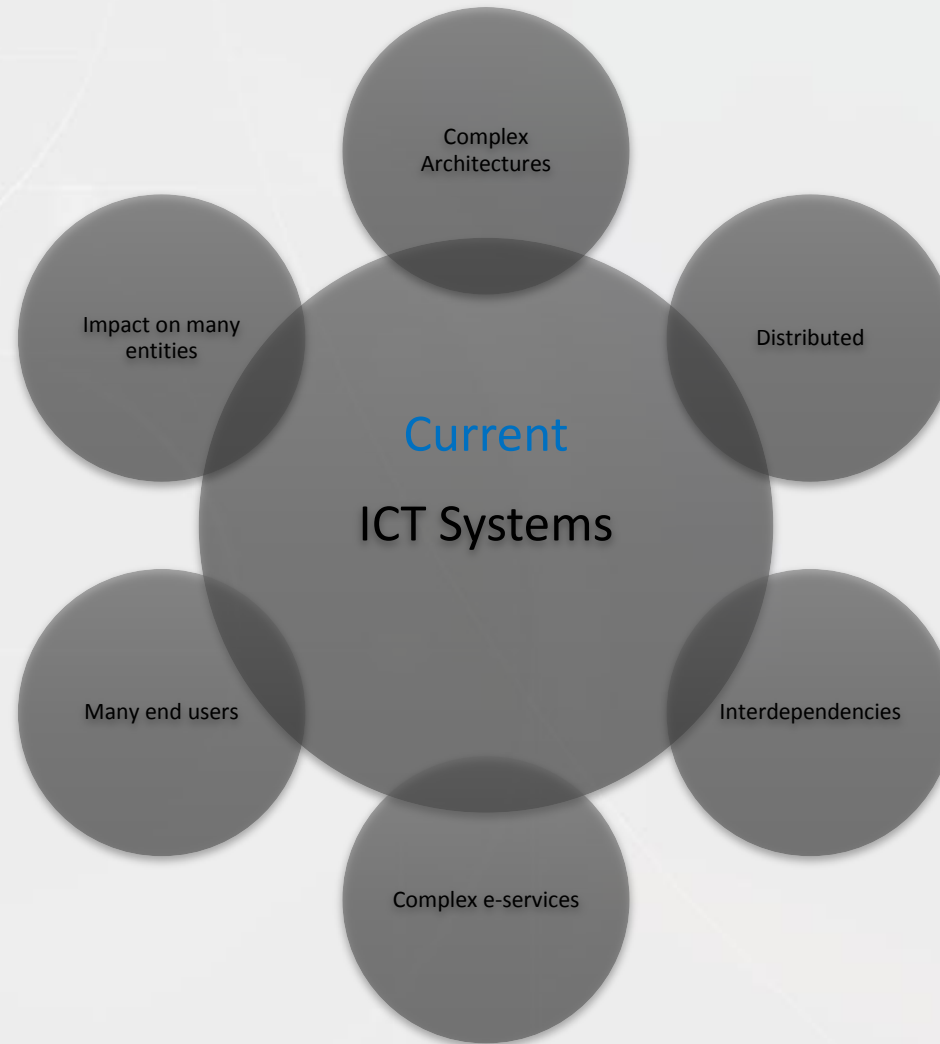
- Introduction
- Open Issues
- STORM Environment
- Case Study A: S-PORT project
- Case Study B: Risk Assessment in Ship Information Systems
- Conclusions



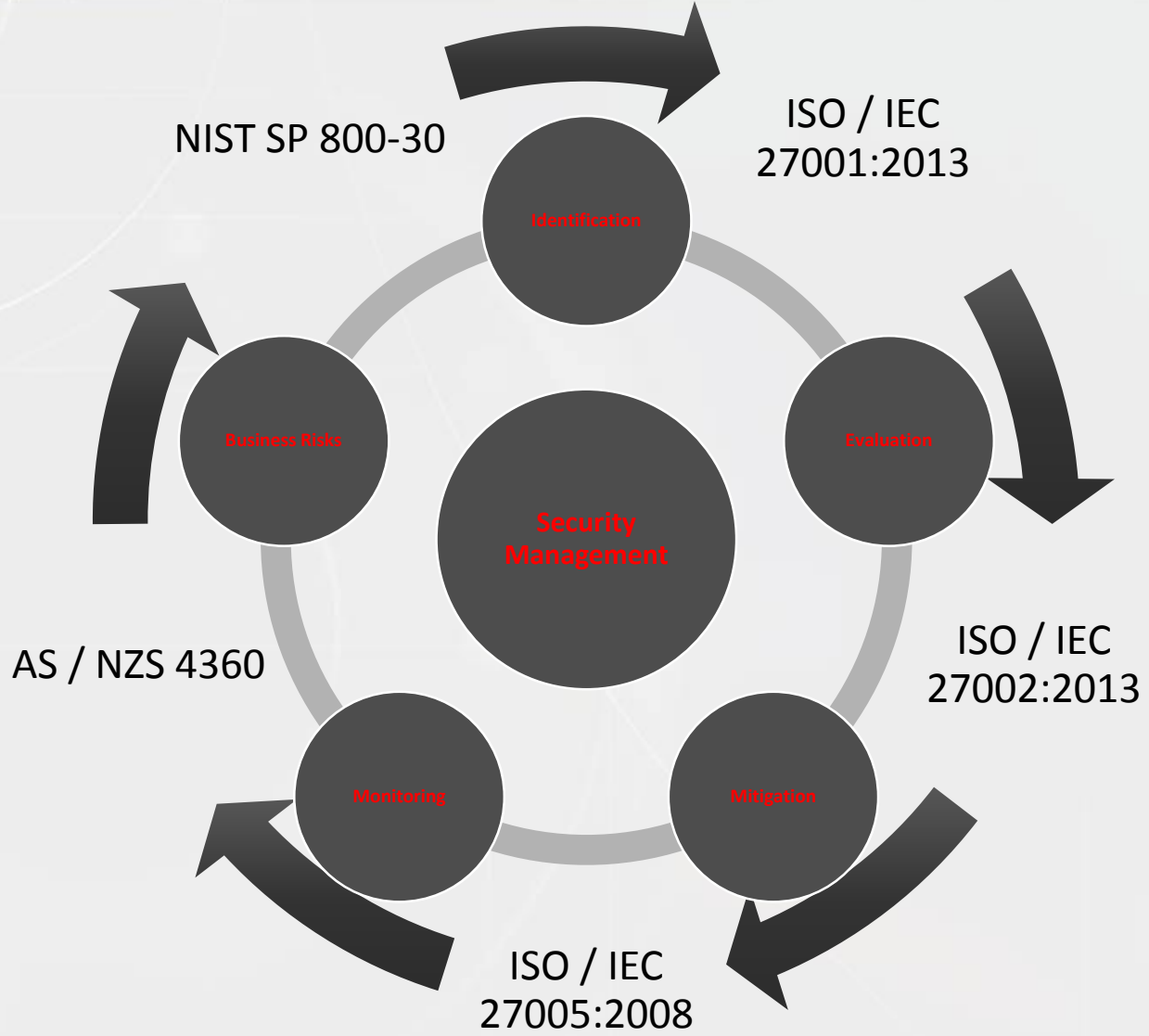
# Introduction



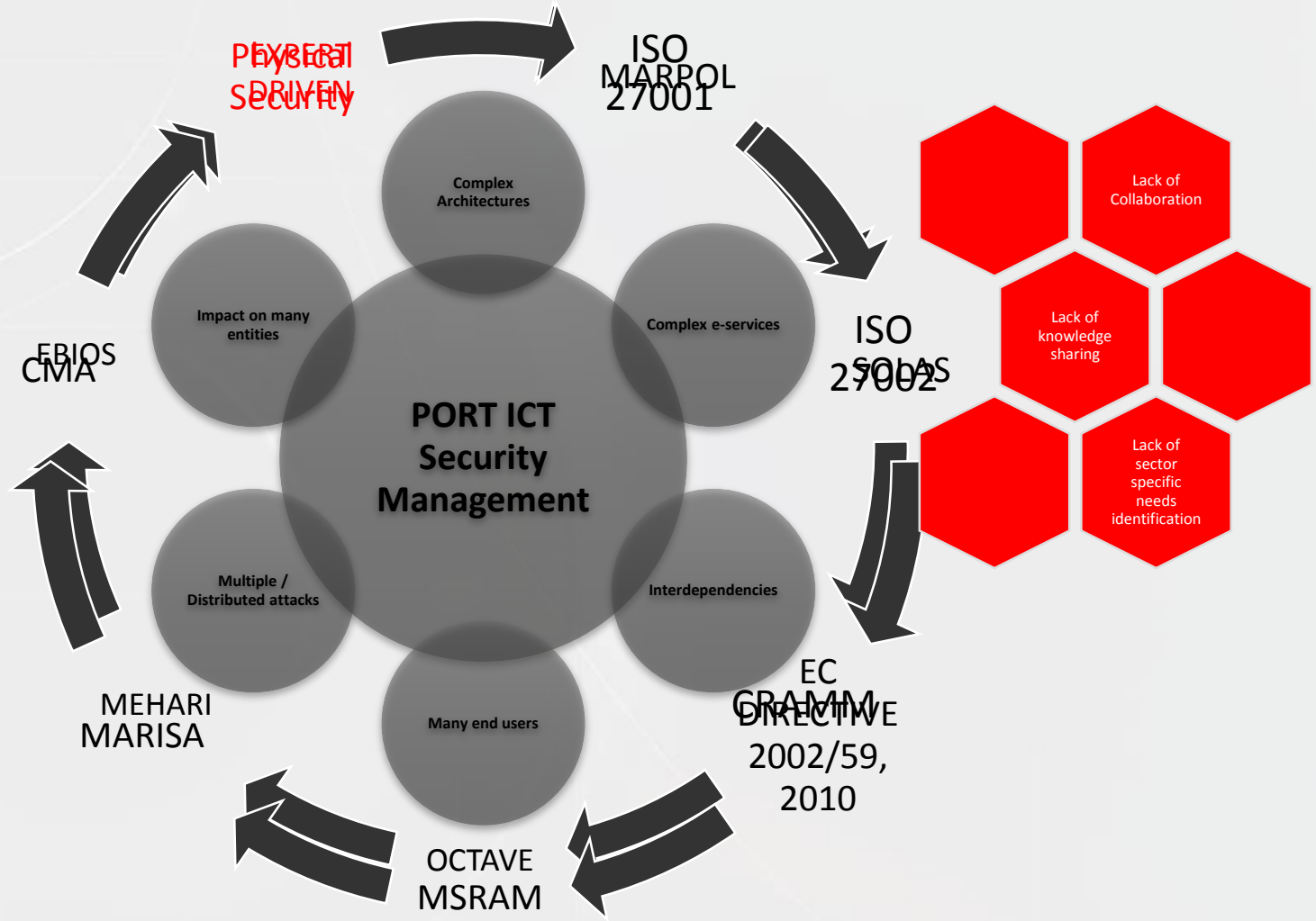
# Introduction



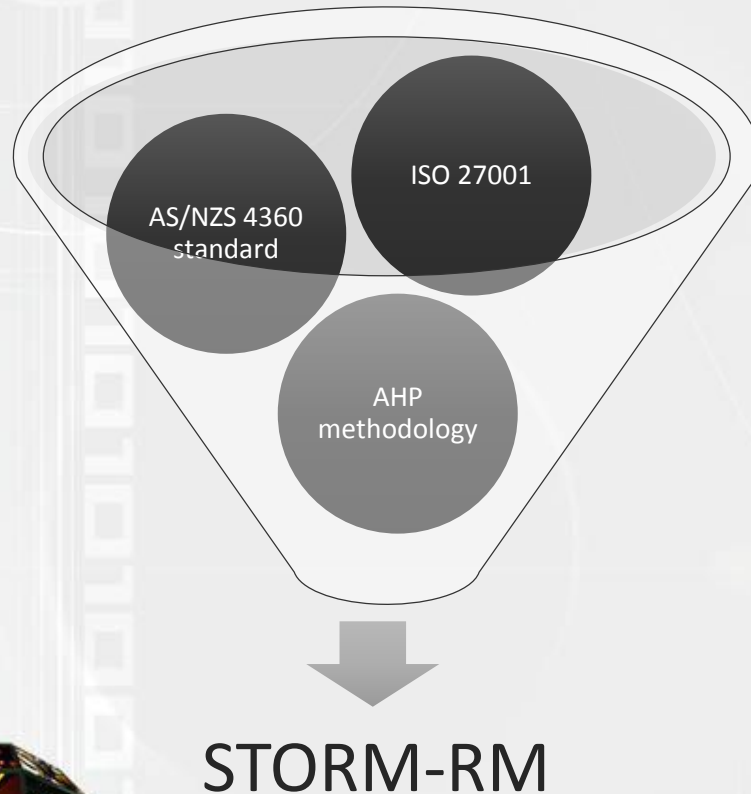
# Security Management: A world of ...acronyms!



# Open issues



# Ideas and suggestions

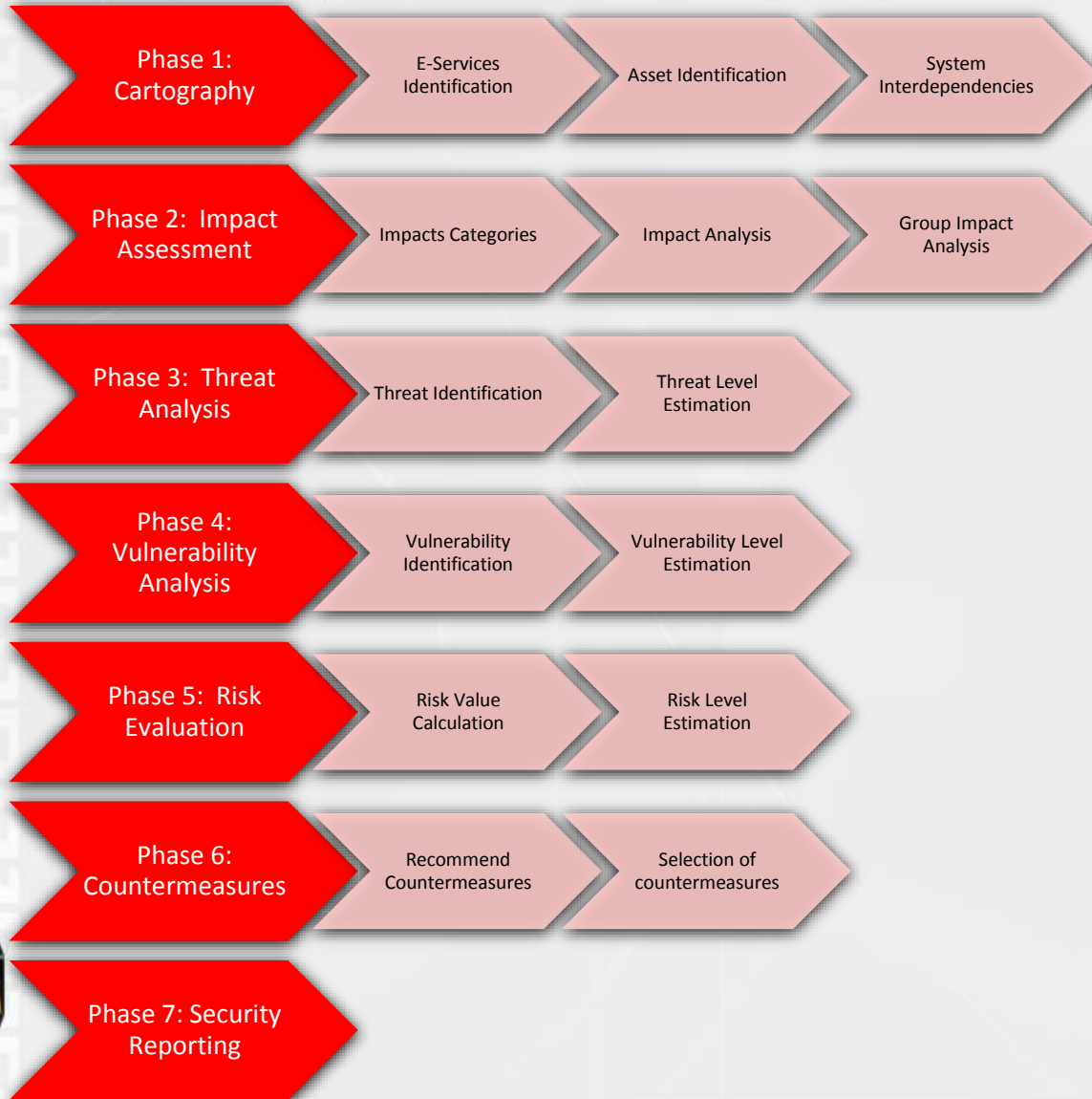


## STORM-RM methodology

- ❑ 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.)

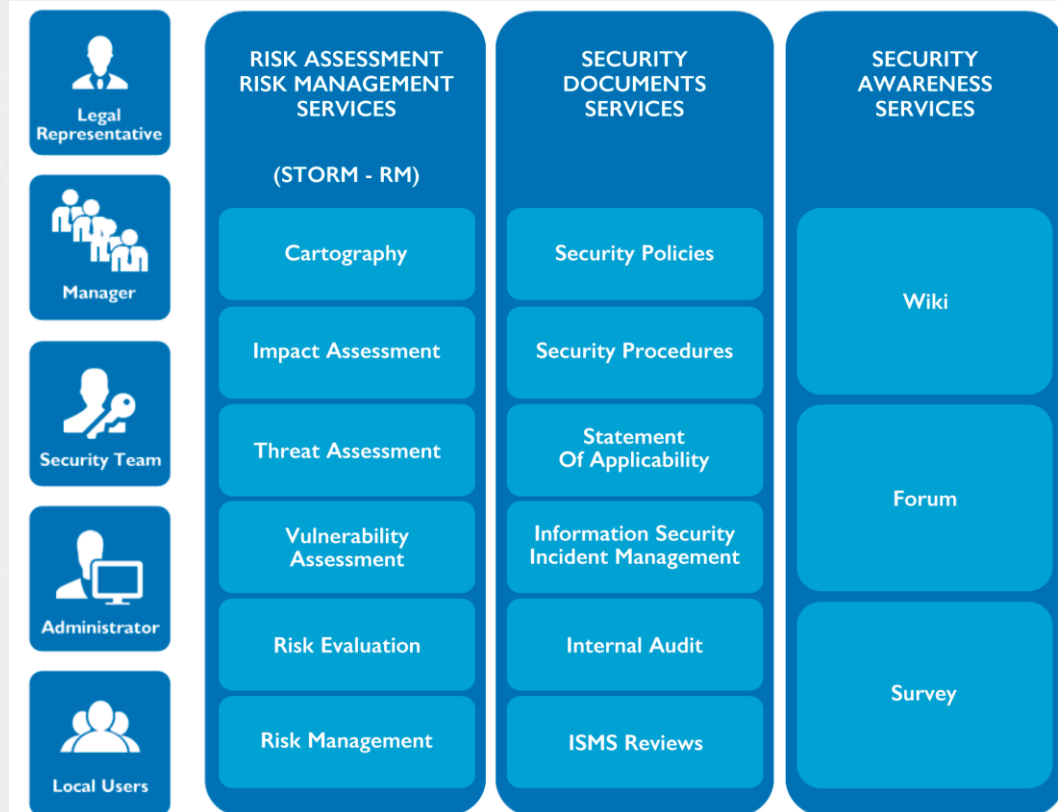


# STORM-RM Methodology



# STORM - Secure TOol for Risk Management

- Innovative, collaborative, cost effective and user friendly security consultancy environment.
- Can be used by different type of organizations in order to collaboratively manage their information security.
- Offers a bundle of targeted services to the ICT users in order to guide them to securely manage their ICT systems.
- Based on the PDCA model of the ISO27001 security standard.



# 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



# 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.
- ✓ A Eurostat survey shows that **3.8 billion gross weight of goods** handled in all **EU ports** during 2014
- ✓ 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.



# 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**.



# Current Status

- The **current maritime legislation, methodologies and tools** :
  - **MARPOL** (e.g. MEPC.: 189(60), 190(60))
  - **SOLAS** (e.g. MSc.: 286(86), 256(84), 46(66), 291(87), 216(82), 282(86), 291(87), 290(87)) for the safety of passengers, ships and cargo, the ISPS Code
  - **Methodologies / Tools:** MSRAM , MARISA, CMA, SafeSeaNet
- Concentrate only on the **Safety**
- **Security management standards** (e.g. Cobit, Val IT, ISO 27001, ISO 27005; NIST) **methodologies** (e.g. CRAMM, EBIOS, OCTAVE, MAGERIT, Dutch A&K Analysis) and **tools** (e.g. CRAMM, COBRA):
  - Are expert driven
  - They do not address sector specific needs
  - They do not allow collaboration





# 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 Improvements

- A new cartography service (i.e. System Modeling service), based on BPMN was introduced enabling users to design the business processes and identify the related PCIT assets.
- Opinion weights of the risk management methodology were appropriately parameterized in order to adapt to the organizational structure of ports.
- ISPS code specific impacts were embedded into the S-Port environment.
- Physical and environmental threats, particular to a port environment, were considered.
- A new taxonomy was introduced, so as to allow the contents of the digital library to take into consideration all the important maritime areas.



# S-PORT Evaluation

- **Piraeus Port Authority**

- participated in the pilot, with 3 users:
  - (a) an administrator, (b) a security officer, and (c) an end-user.
- *Car Terminal Service*: one of the main business processes of this port.

- **Thessaloniki Port Authority**

- participated with 8 users: (a) 1 security officer, (b) 1 manager, (c) 3 system administrators, and (d) 3 end-users.
- Users created the asset-model and assessed the *Container Terminal Service*

- **Municipal Port Fund of the Island of Mykonos**

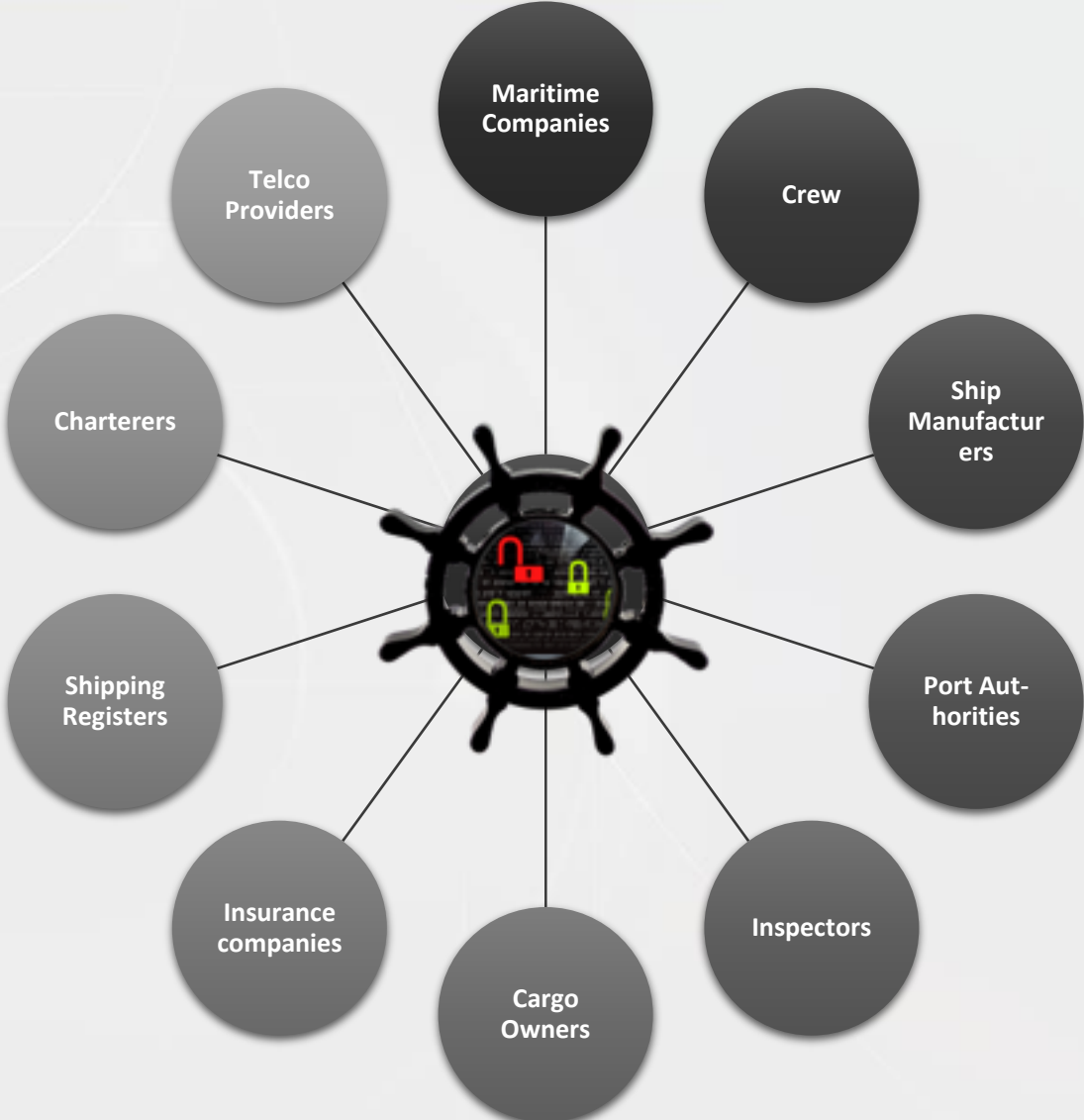
- participated in the pilot with 3 end-users and 1 security officer
- Two services: (a) the *Cruise Management service*, and (b) the *Ferry Management service*.



# Case Study B: Risk Assessment in SIS



# Commercial Ships



# Floating digital offices

- **Cargo Management Systems:** For the management and control of cargo which may interact with a variety of systems ashore. Such systems may include shipment-tracking tools available to shippers via the internet.
- **Bridge Systems:** Networked Navigation systems with interfaces to shore-side networks for update and provision of services (including ECDIS, GNSS, AIS, VDR, etc.).
- **Machinery, propulsion and power control systems:** for monitoring and controlling onboard machinery, propulsion and steering.
- **Access Control Systems:** For supporting access control to ensure physical security and safety of a ship and its cargo (including surveillance, shipboard security alarm, and electronic “personnel-on-board” system).
- **Passenger servicing systems:** For property management, boarding and access control of passengers.
- **Passenger public networks:** For the passenger entertainment (including WiFi networks)
- **Administration and crew welfare systems:** For administration of the ship or the welfare of the crew.
- **Communication systems:** For the internet connectivity via satellite and/or other wireless communication.



# Risk Assessment in SIS

- So, modern ships **cannot** be viewed as an **isolated** units since:
  - **depend** on different and plethora information systems,
  - **interact** with different entities
  - any potential threats could have **significant impact** at the proper operation of **all interconnected entities**.
- **Existing best practices and maritime regulation** have recently identified these security needs and they have proposed general guidelines in order to effectively address cyber-threats
  - BIMCO, *Guidelines on Cyber Security Onboard Ships* (2016)
  - AMMITEC, *Cyber Security Awareness* (2016)
  - IMO, *Measures to Enhance Maritime Security* (2015)
- Indicative Risk Assessment scenario with the STORM security management tool, so as to evaluate the security gaps and identify the importance of the SIS security management.



## Common e-services (on board..)

- Navigation Service: Responsible for the proper ship navigation, such as Automatic Identification System (AIS), Global Positioning System (GPS), Global Maritime Distress and Safety System (GMDSS)
- Operational Service: Responsible for the proper operation of the ship
- ECDIS (Electronic Chart Display and Information System): Responsible for the position data, electronic maps
- Planned Maintenance Service (PMS): Responsible for the warehouse, supplier and maintenance management.
- Email Service: Data that are transferred via email such as ships' route, cargo information, charterers information
- ERP Service: Responsible for monitoring of suppliers, vessel operations, crew, maritime company etc.



# Main User Groups

- Bridge Officers: they have access at all onboard systems and they are responsible mainly for the Navigation System, Email and ERP Service.
- Crew: They have access mainly at the Operational Service, Email Service and ERP Service
- Maritime Company Users: They have access at some of the onboard systems via remote connection in order to support the crew and bridge officers or maintain the systems.



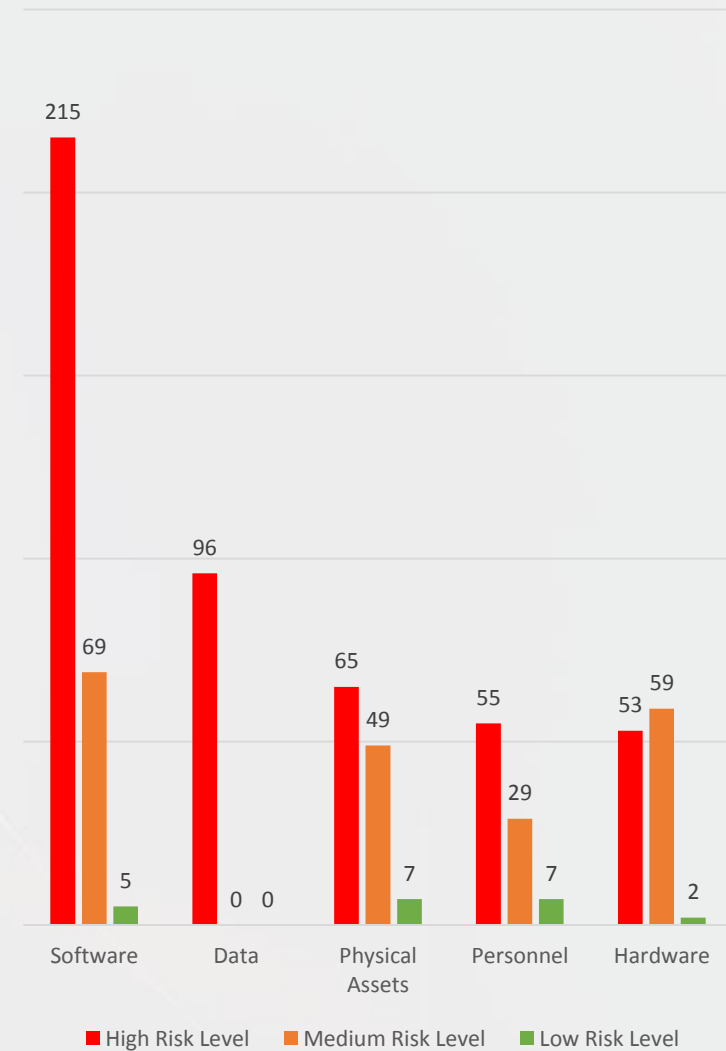
# Assets examined

- 6 Data Assets: (including Navigation Data, Operational Data, ECDIS Data, PMS Data, email, etc.)
- 8 Computer Systems: (including ECDIS System, File Server, Navigation Equipment, PMS Company Client, PMS server, Email Server, ERP Server, Vessel Workstations etc.)
- 2 Networks: Main Vessel Network, Satellite Network
- 8 Hardware Assets: (including main server, main network and satellite equipment)
- 21 Software Assets: (including all operating systems, ECDIS SW, PMS software, etc.)
- 3 Physical Assets: (including the Vessel Bridge, Vessel Control Room and Maritime Company Computer Room)
- More than 100 threats were examined, different for each asset category, in order to identify the potential risks.



# Risk Assessment Results

- **Criticality of the data** that are hosted onboard or transferred via communication services to all involved entities of the maritime environment
- **Indicative important threats:**
  - destruction, disclosure or falsification of data,
  - interruption of business processes,
  - unauthorized access or weak authentication
- **The main vulnerabilities:**
  - lack of security awareness programs
  - lack of backup systems
  - existence of several «single point of failure» assets
  - weak protection of the physical access to the Ship Information systems.



# Generic conclusions and some proposals

- With the **rapid growth** and adoption of technology in maritime environment, **SIS** and **PICT** are increasingly exposed against cyber risks.
- These cyber risks could be exploited either by **satellite networks**, either by **the traditional communication channels** and could have **significant impact** on all **maritime entities** affecting **international economy**.
- A **holistic and common approach** (enabling the collaboration among all involved entities) should be adopted for the security management of both SIS and PICT systems in order to:
  - continuously monitor security and privacy risks,
  - improve their ICT-based business processes,
  - provide continuity and rendering of services for all entities of the maritime environment



# Acknowledgement

- We would like to thank all port authorities involved in the S-PORT project:
  - Piraeus Port Authority,
  - Thessaloniki Port Authority
  - Municipal Port Fund of the Island of Mykonos
- We would also like to thank **Mr. Konstantinos Bonatsos** (AMC college, postgraduate student) for his contribution to the ship case-study



## References

1. Gritzalis D., "Insider threat prevention through Open Source Intelligence based on Online Social Networks", Keynote address, *13<sup>th</sup> 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 7<sup>th</sup> 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 6<sup>th</sup> 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 1<sup>st</sup> International Symposium & 10<sup>th</sup> 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 4<sup>th</sup> 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 3<sup>rd</sup> 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 7<sup>th</sup> 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 3<sup>rd</sup> International Conference on Human Aspects of Information Security, Privacy & Trust, Springer, USA, 2015.