MITIGATE

The MITIGATE Methodology – An Overview

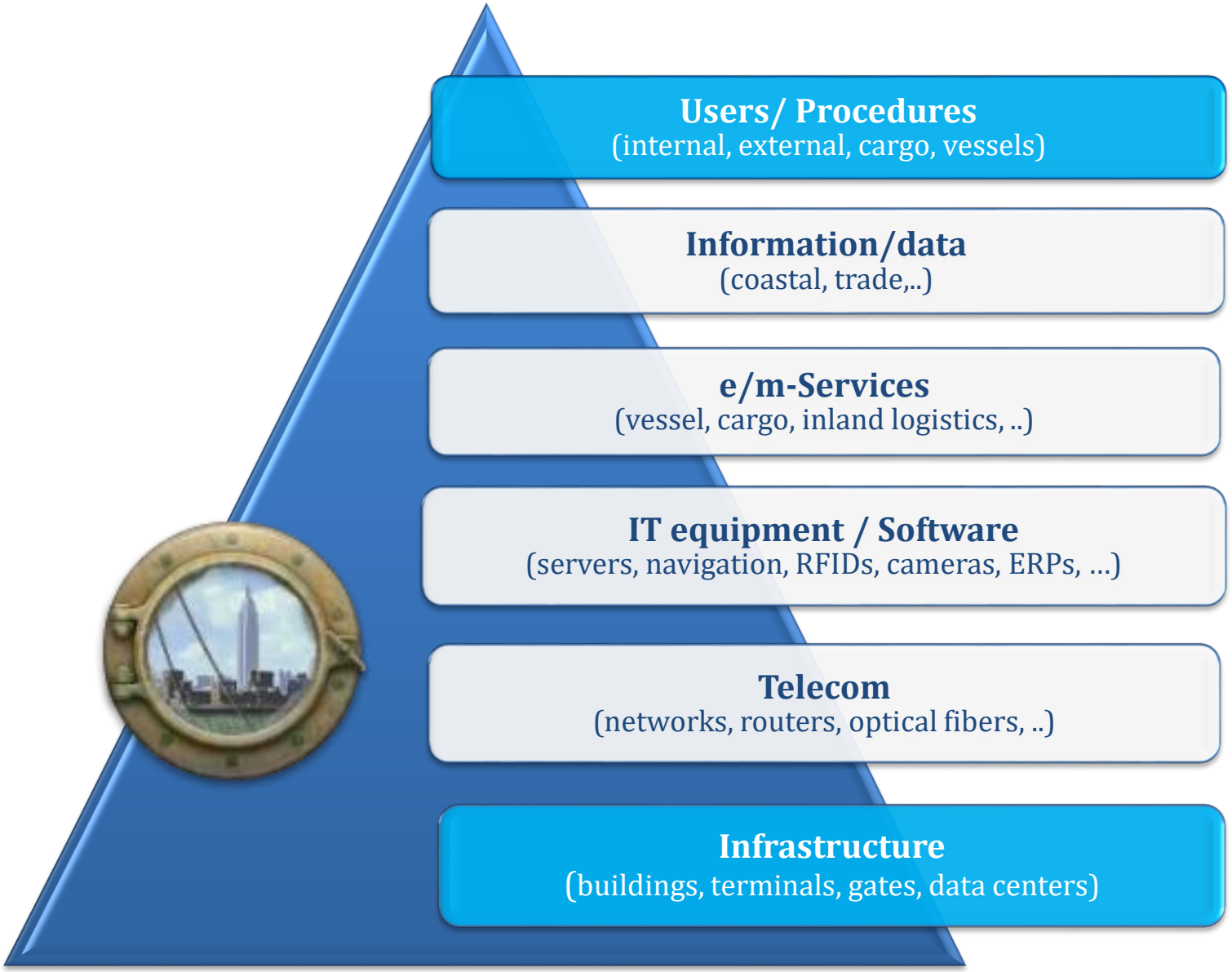
Prof. Christos Douligeris

University of Piraeus, Greece, cdoulig@unipi.gr

in cooperation with

Assoc. Prof. N. Polemi, Dr. S. Papastergiou,
PhD (C.) E.-M. Kalogeraki

ICT Systems


Users/ Procedures
(internal, external, cargo, vessels)
Information/data
(coastal, trade,..)
e/m-Services
(vessel, cargo, inland logistics, ..)
IT equipment / Software
(servers, navigation, RFIDs, cameras, ERPs, …)
Telecom
(networks, routers, optical fibers, ..)
Infrastructure
(buildings, terminals, gates, data centers)

Security is defined

as the preservation of:

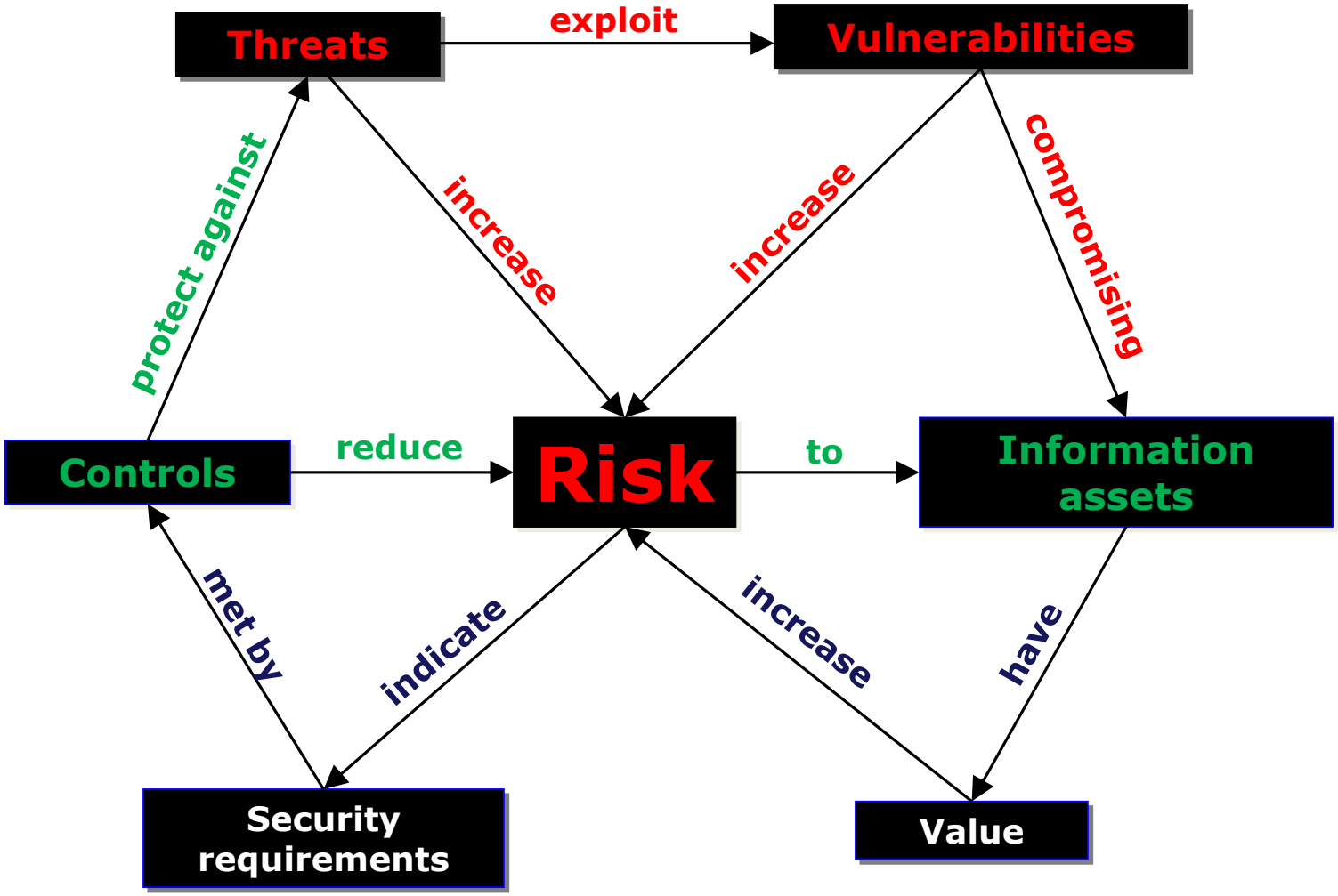
Confidentiality — Making asset accessible only to those authorized to use it

Integrity — Safeguarding accuracy, identity, completeness of asset + processing methods

Availability — Ensuring that asset is available when required and it is not denied

ISO 27001 security

Risk relationships



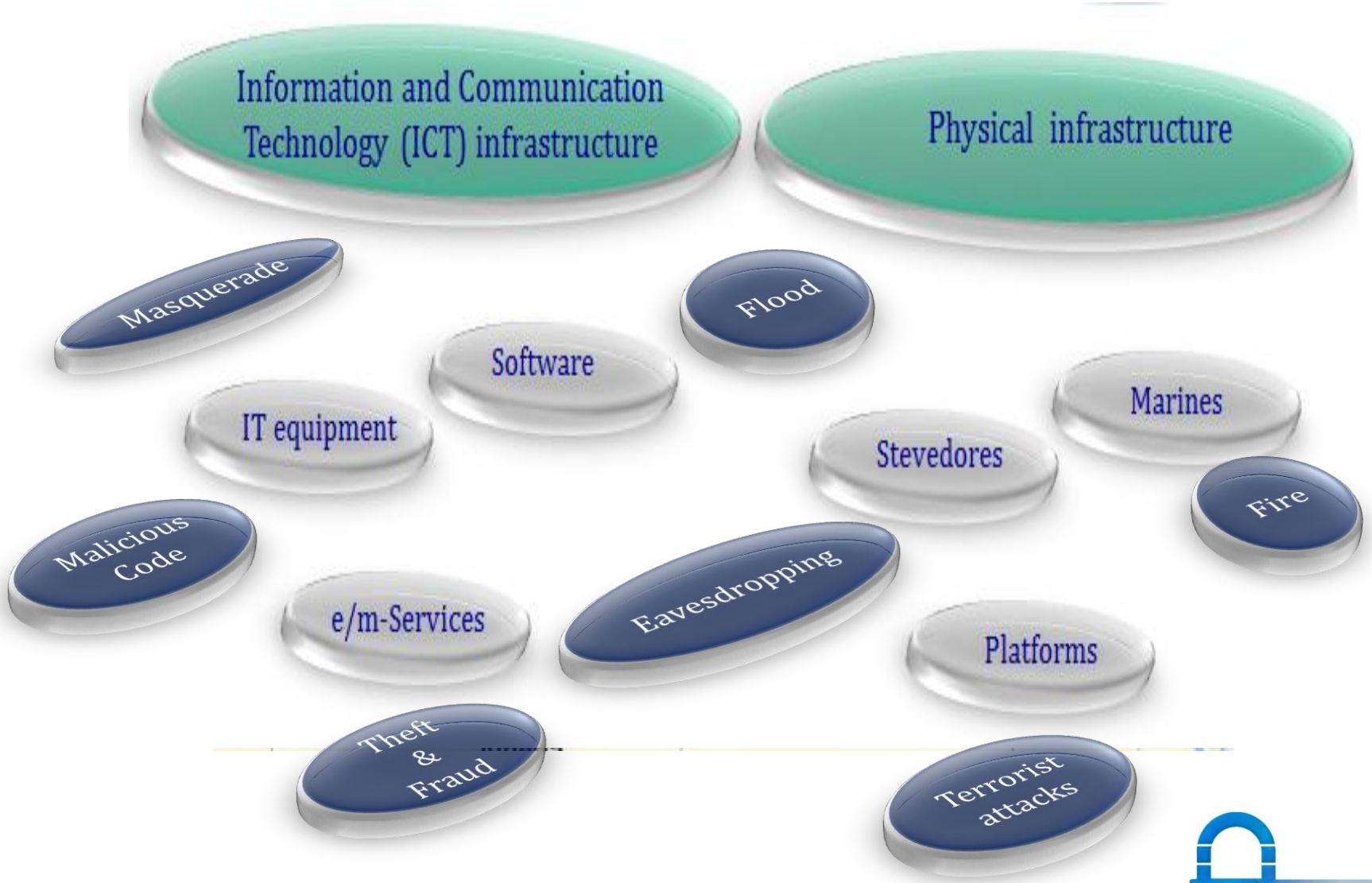
Security & Safety

- **Security (cyber security)**: Ensure the Confidentiality, Integrity and Availability of the ICT systems.
- **Safety (physical security)**: Ensure the access control and availability of the physical assets

- ISO/IEC 27001:2005
  followed by draft ISO/IEC 27001:2013 (building a SM system)
- ISO/IEC 27005:2011 (security risk management)
- NIST SP 800-128, 2011
  Guide for Security-Focused Configuration Management of Information Systems
- ISO 31000:2009 Principles and Guidelines on Implementation
- ISO/IEC 31010:2009 RM- RA Techniques
- ISO/IEC 27002:2005 (best practice recommendations)
- AS/NZS 4360:2004 (Australian/New Zealand standard for RM)

Standards

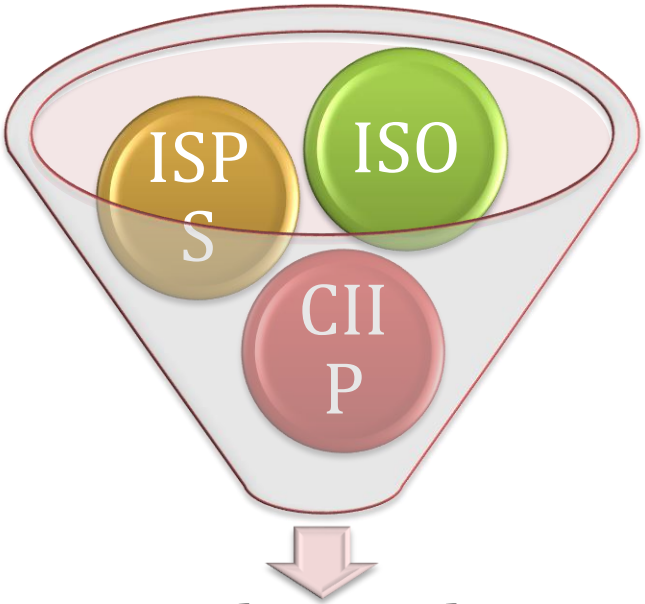
Maritime Sector



CYSM
COLLABORATIVE CYBER/PHYSICAL SECURITY MANAGEMENT SYSTEM

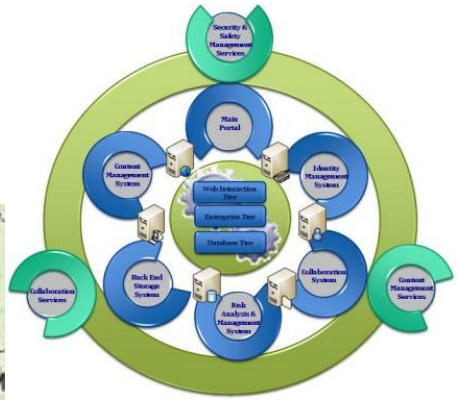
CYSM - Collaborative Cyber/Physical Security Management System (cysm.eu)

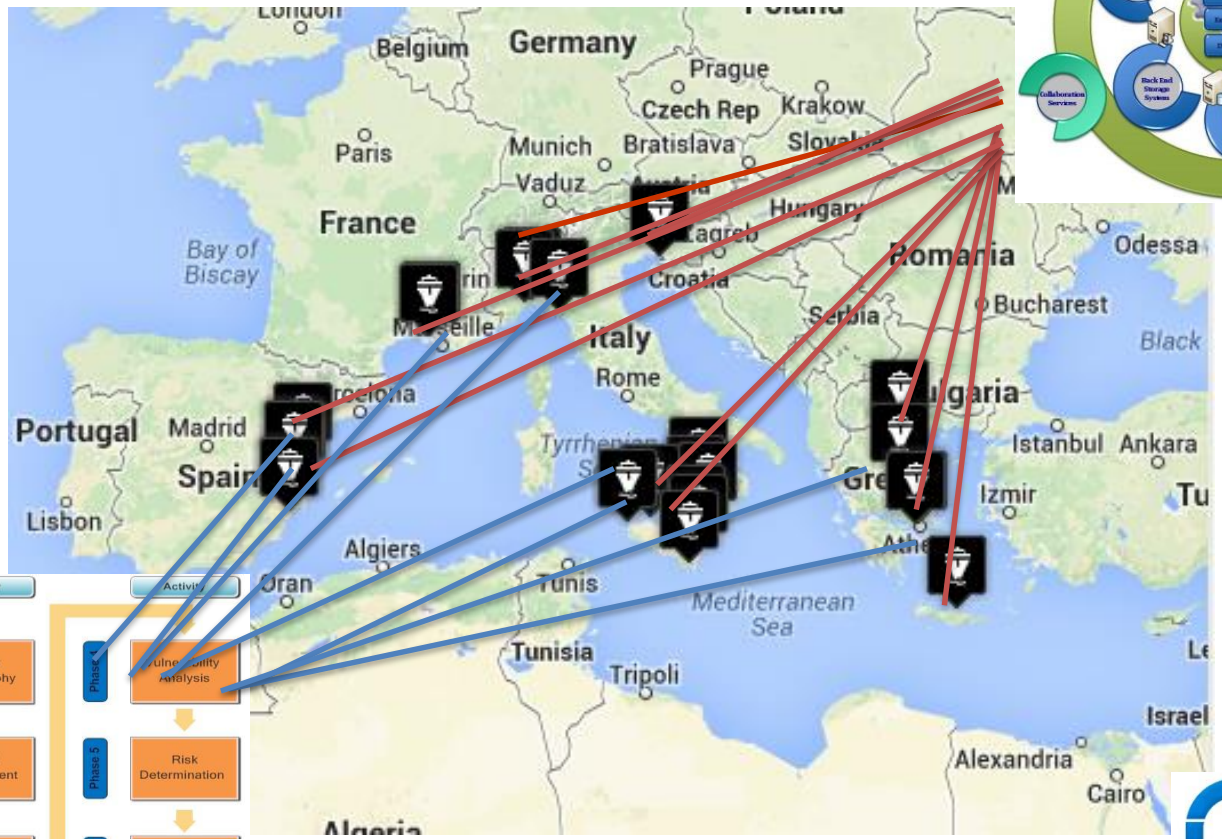
QUESTION A: How can we estimate risks of ports' cyber and physical assets ???

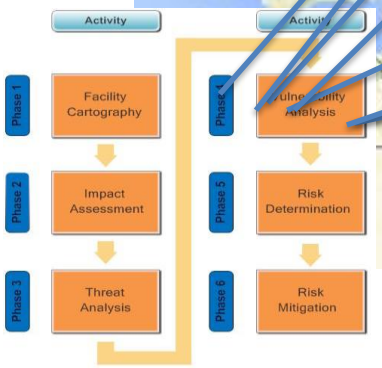


CYSM Outputs (cysm.eu)

- CYSM risk assessment (RA) methodology of ports individual ICT assets
- CYSM collaborative tool offering RA services



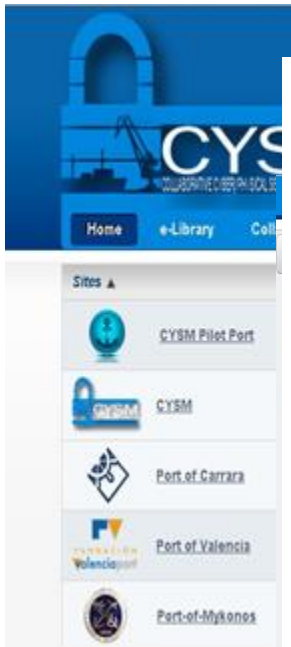


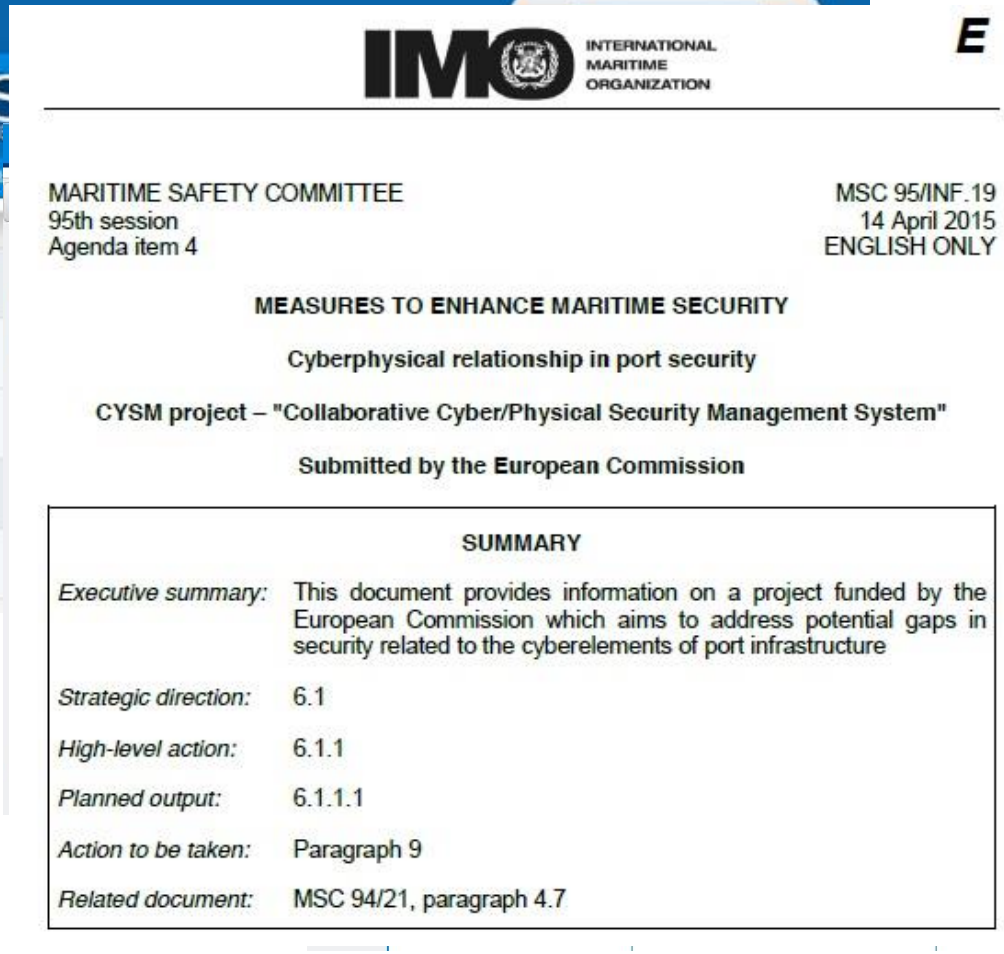


CYSM
COLLABORATIVE CYBER/PHYSICAL SECURITY MANAGEMENT SYSTEM

Cysm Security Management System

http://cysm.cs.unipi.gr/





IMO INTERNATIONAL MARITIME ORGANIZATION

E

MARITIME SAFETY COMMITTEE
95th session
Agenda item 4

MSC 95/INF.19
14 April 2015
ENGLISH ONLY

MEASURES TO ENHANCE MARITIME SECURITY

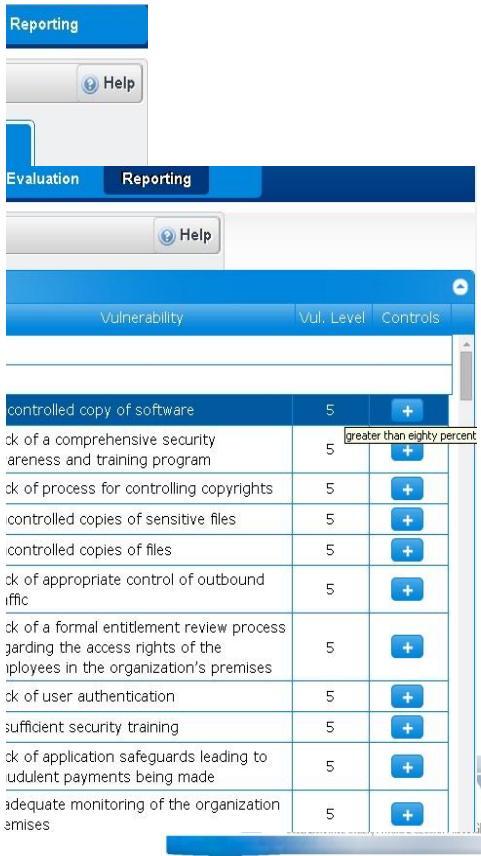
Cyberphysical relationship in port security

CYSM project – "Collaborative Cyber/Physical Security Management System"

Submitted by the European Commission

SUMMARY

Executive summary:	This document provides information on a project funded by the European Commission which aims to address potential gaps in security related to the cyberelements of port infrastructure
Strategic direction:	6.1
High-level action:	6.1.1
Planned output:	6.1.1.1
Action to be taken:	Paragraph 9
Related document:	MSC 94/21, paragraph 4.7



CYSM Consortium

FEPORTS

UNIVERSITY OF PIRAEUS RESEARCH CENTER

FUNDACIÓN valenciaport

ΟΛΠ PIRAEUS PORT AUTHORITY S.A.

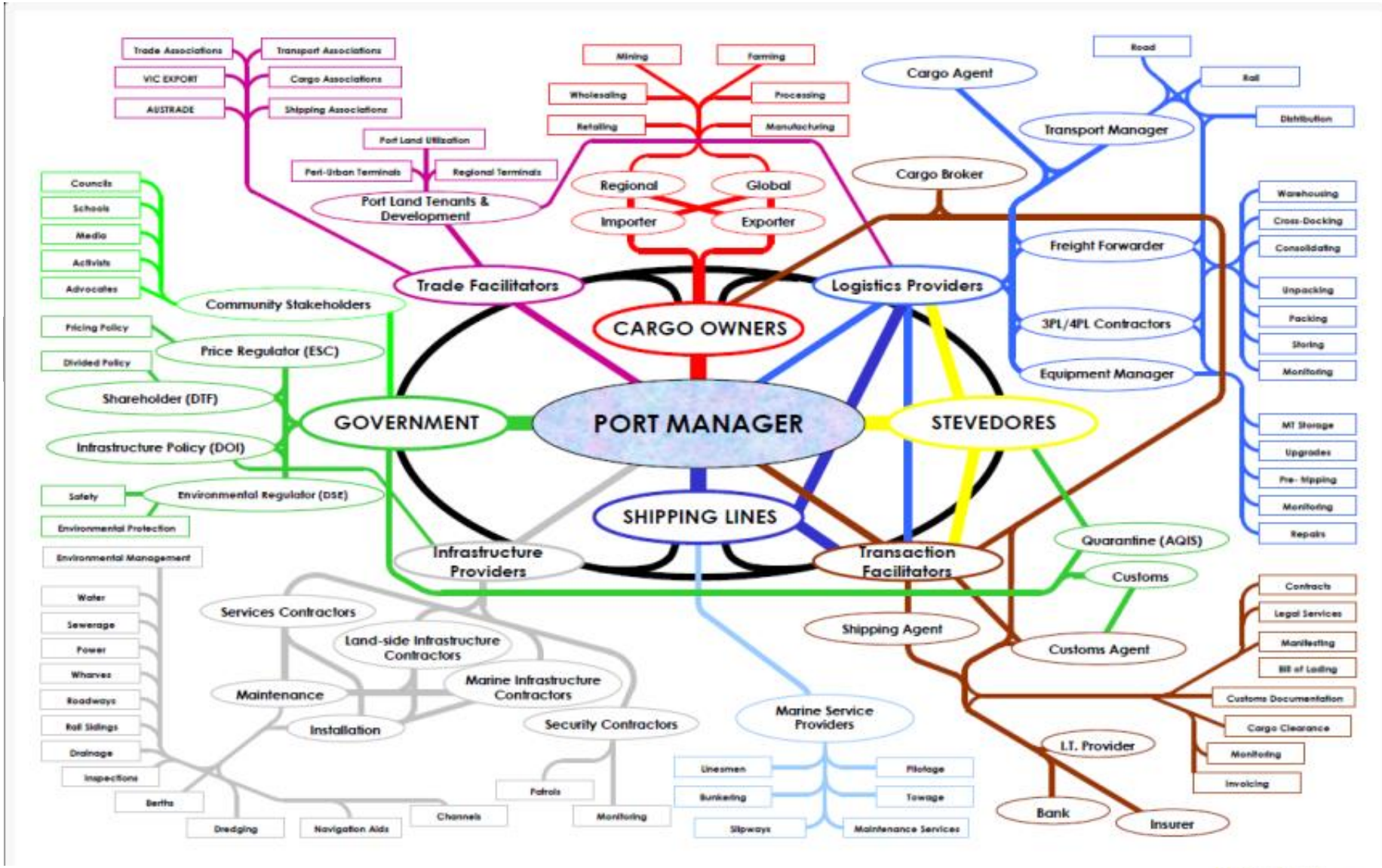
UNIVERSITÀ DEGLI STUDI DI GENOVA

2003

SingularLogic Innovation at your doorstep

CYSM COLLABORATIVE CYBER/PHYSICAL SECURITY MANAGEMENT SYSTEM

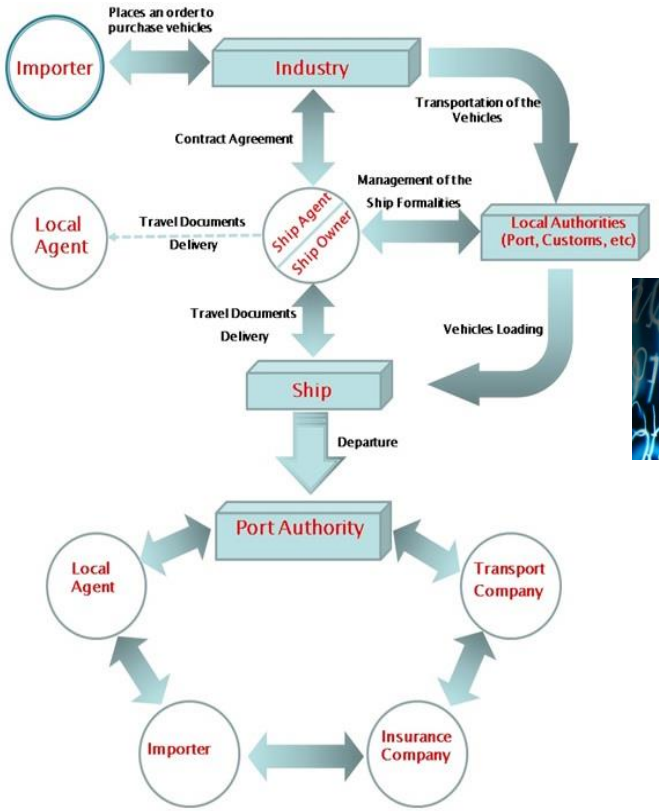
Ports Ecosystem

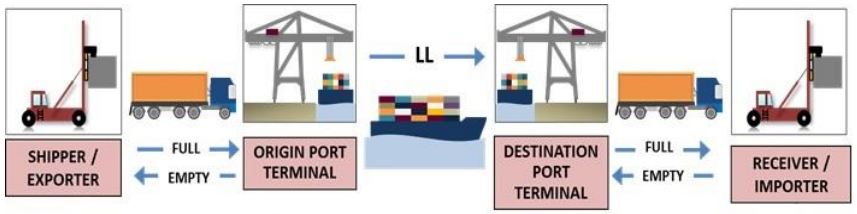


Medusa

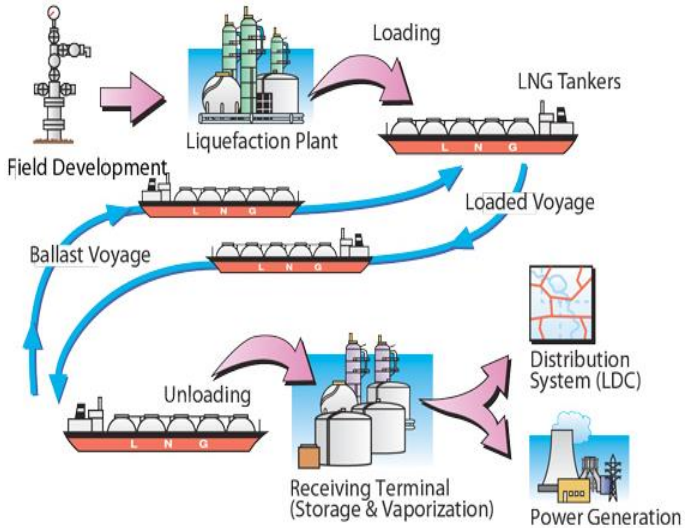
Maritime Supply Chain Service

Vehicle Transport Supply Chain Service





Container Transport Supply Chain Service



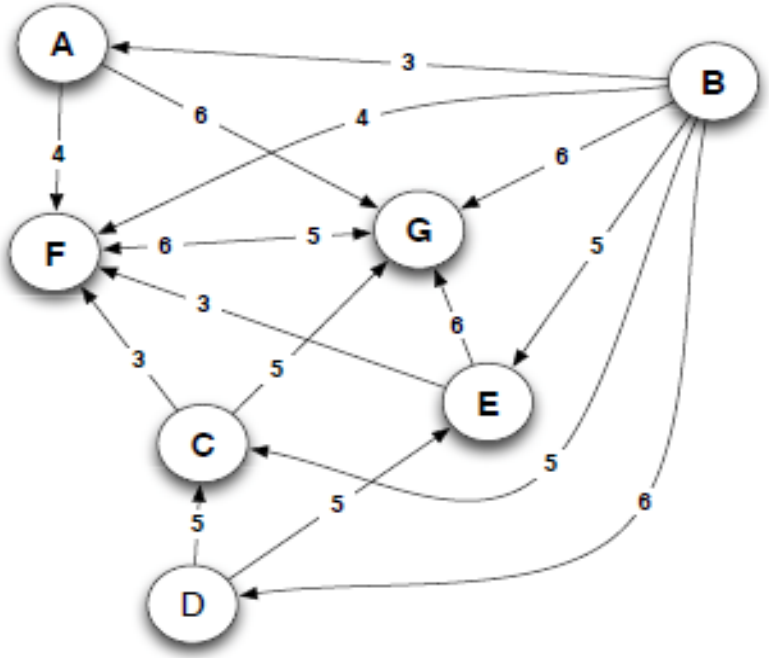
LNG Transport Supply Chain Service

Medusa

Identifying dependencies: Dependency graphs

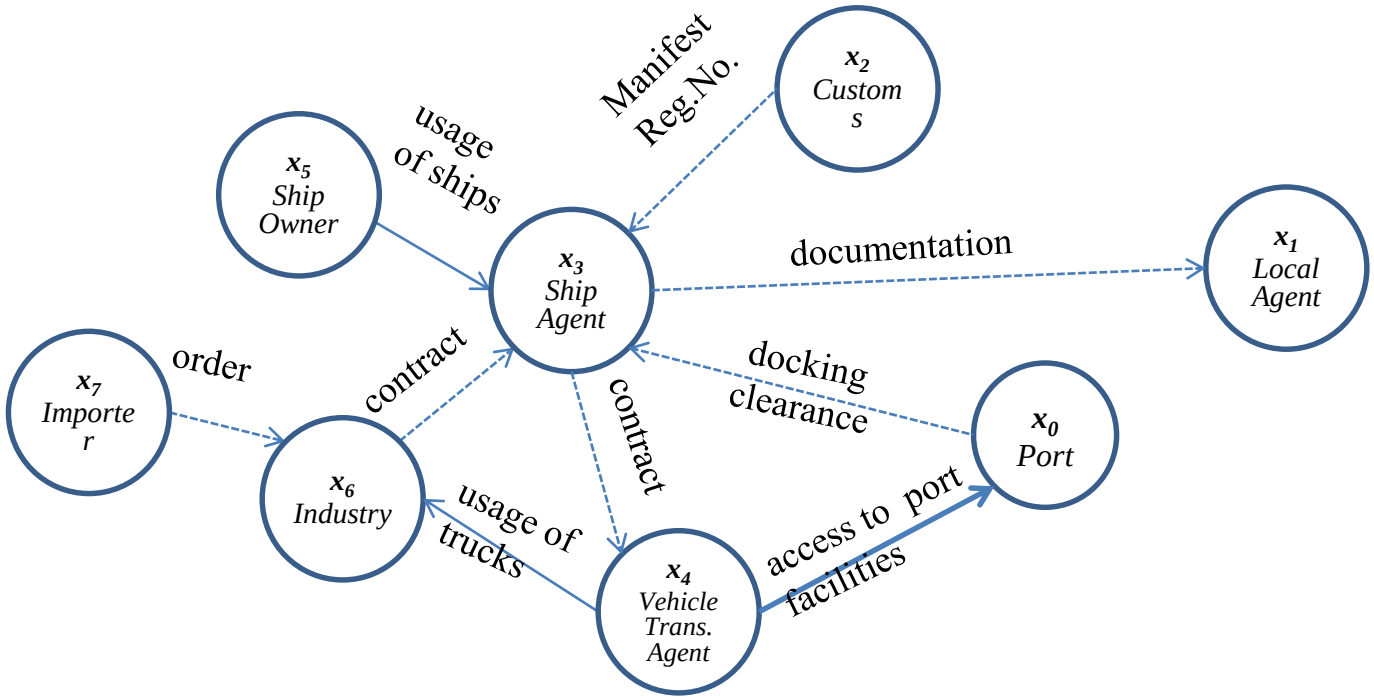
Dependent CIs	Dep. Type	Description	SImp	IImp	IImp Type	Scale $I_{j,s}$	LH $L_{j,s}$	Risk $R_{j,s}$
	CI_A (Finance Sector)							
CI_F	C	Provides payment services	UA	UA	Public Confidence	L	L	4
CI_G	C	Provides payment Services	UA	UA	Public Confidence	H	L	6
	CI_B (Energy Sector)							
CI_A	P	Depends for power	UA	UA	Economic Impact	VL	L	3
CI_C	P	Depends for power	UA	UA	Public Confidence	H	VL	5
CI_D	P	Depends for power	UA	UA	Economic Impact	VH	VL	6
CI_E	P	Depends for power	UA	UA	Economic Impact	H	VL	5
CI_F	P	Depends for power	UA	UA	Public Confidence	L	L	4
CI_G	P	Depends for power	UA	UA	Public Confidence	H	L	6
	CI_G (Government Sector)							
CI_F	S	Industrial action	UA	UA	Economic Impact	M	M	6

Dependency. P: Physical, C: Cyber, G: Geographic, Log: Logical, S: Social
Source/Incoming Impact (SImp/IImp). UA: Unavailability, DS: Disclosure, MD: Modification
Scale/Likelihood. VH: Very High, H: High, M: Medium, L: Low, VL: Very Low



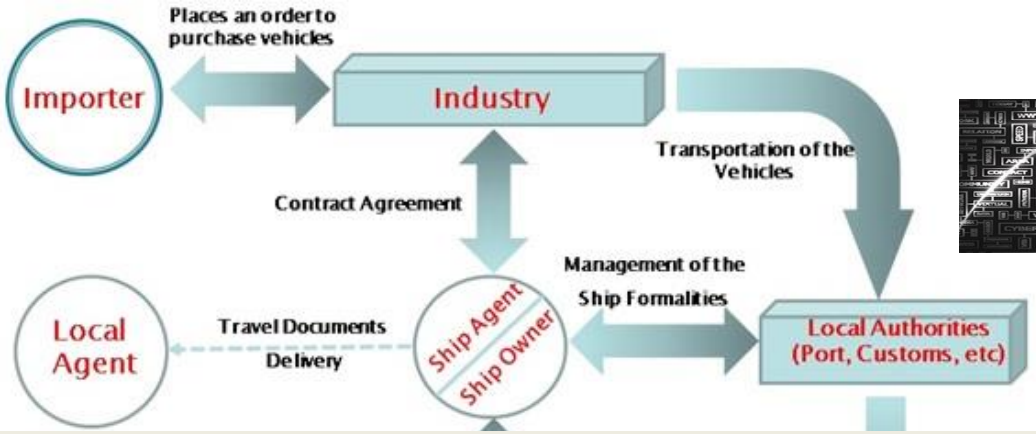
Medusa

Graph Representation: Vehicle Transport Service

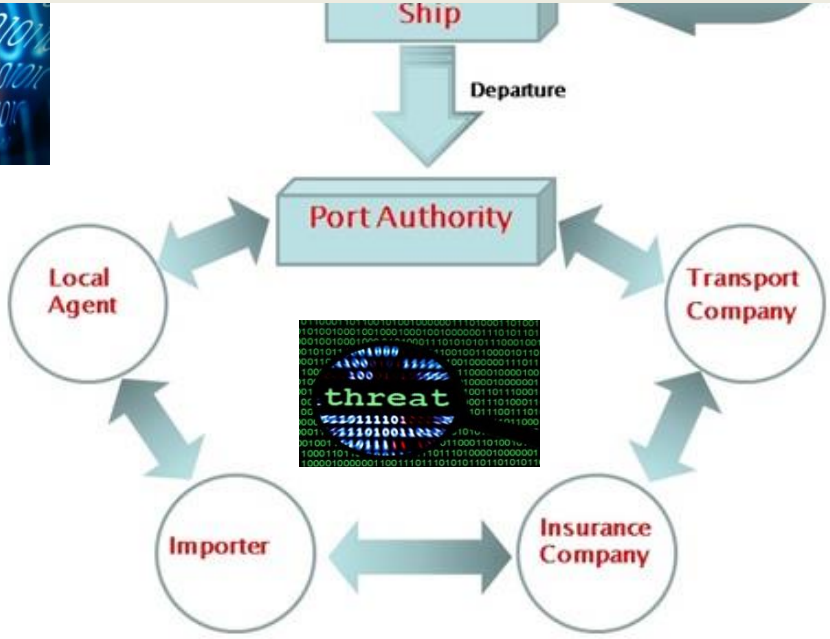


Medusa

Risks of Port's Supply Chain Services



QUESTION B: How can we estimate risks of a supply chain at the entity level ???



Medusa

ISO Supply Chain (SC) standards

ISO 28000 family of standards: designed to protect people, goods, infrastructure and equipment, including means of transport, against security incidents and to prevent their potentially devastating effects.

1. ISO 20858:2007 on Ships and marine technology –to assist in the uniform implementation of ISPS;
2. ISO 28000:2007 on Specification for security management systems for the SC;
3. ISO 28001:2007 on Security management systems for SC– Best practices for implementing SC security);
4. ISO 28003:2007 on Security management systems for the SC- Requirements for auditors of SC security management systems;
5. ISO 28004:2007 on Security management systems for the SC– Guidelines for the implementation of ISO 28000.

Medusa

Research gaps in SC security

ISO 28001 is a guide for SC security management

- …but not a specific methodology
- …or tool to assist the risk assessor

Supply Chains are inherently (inter)dependent systems, however:

- ISO28001 (or any existing RA methodology) does not define ways to assess dependencies within SCs
- … and eventually assess the *cascading risks* within a Supply Chain

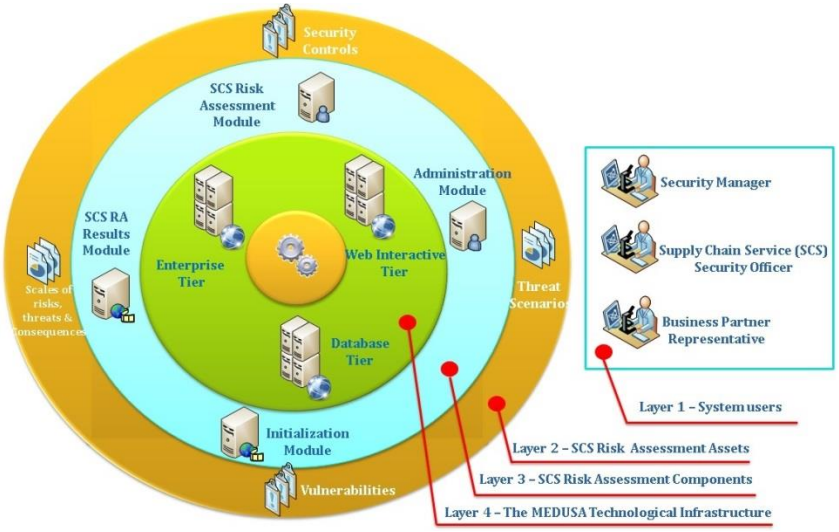
Medusa

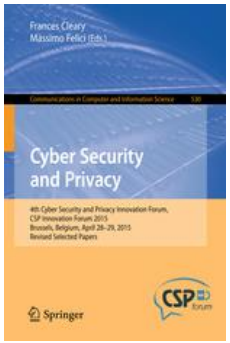
Medusa (medusa.cs.unipi.gr)

Obj. 1: techniques for capturing multi-order dependencies of security incidents and risks

Obj. 2: algorithms for identifying and assessing the critical path of the inter-dependencies across the global supply chain

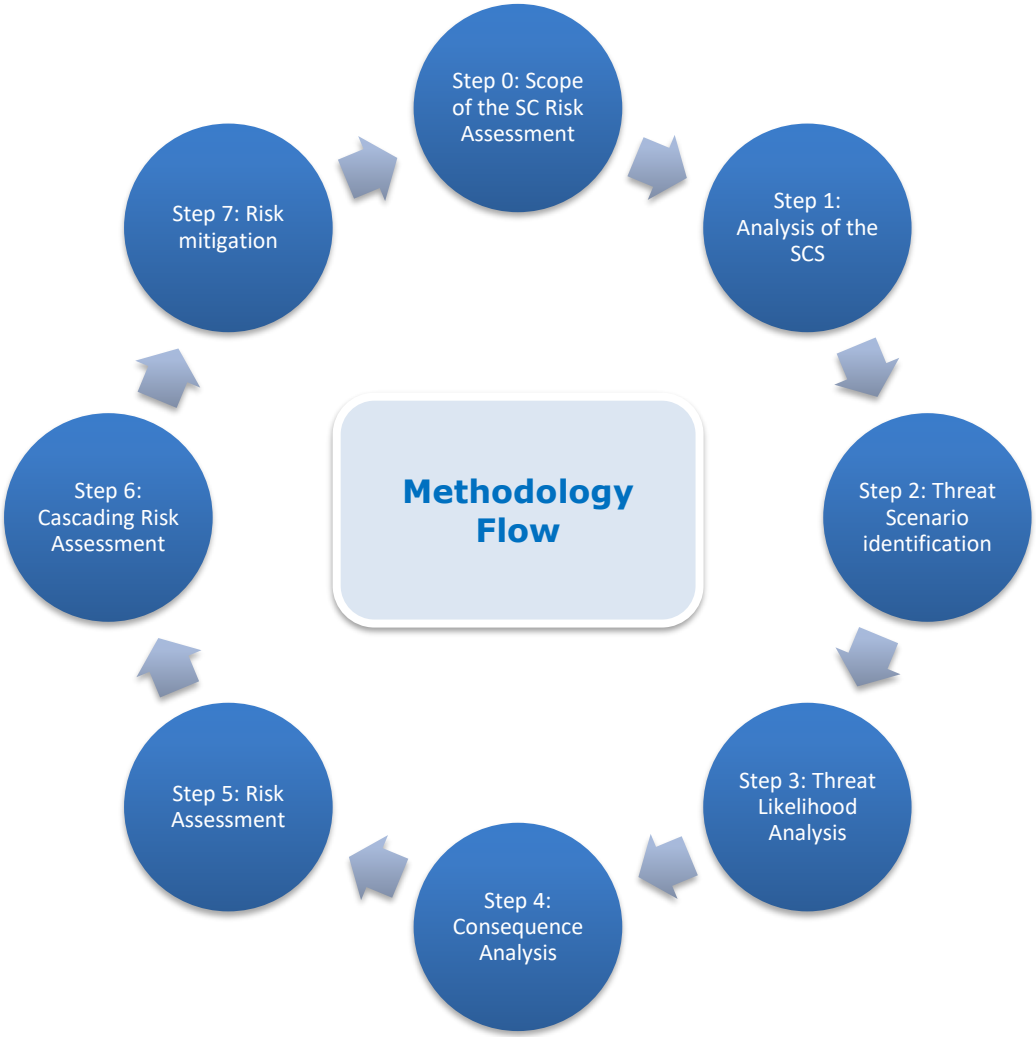
Obj. 3: A risk assessment (RA) methodology for identifying and analyzing the cascading effects of security incidents on port infrastructures, given their various dependencies





Medusa

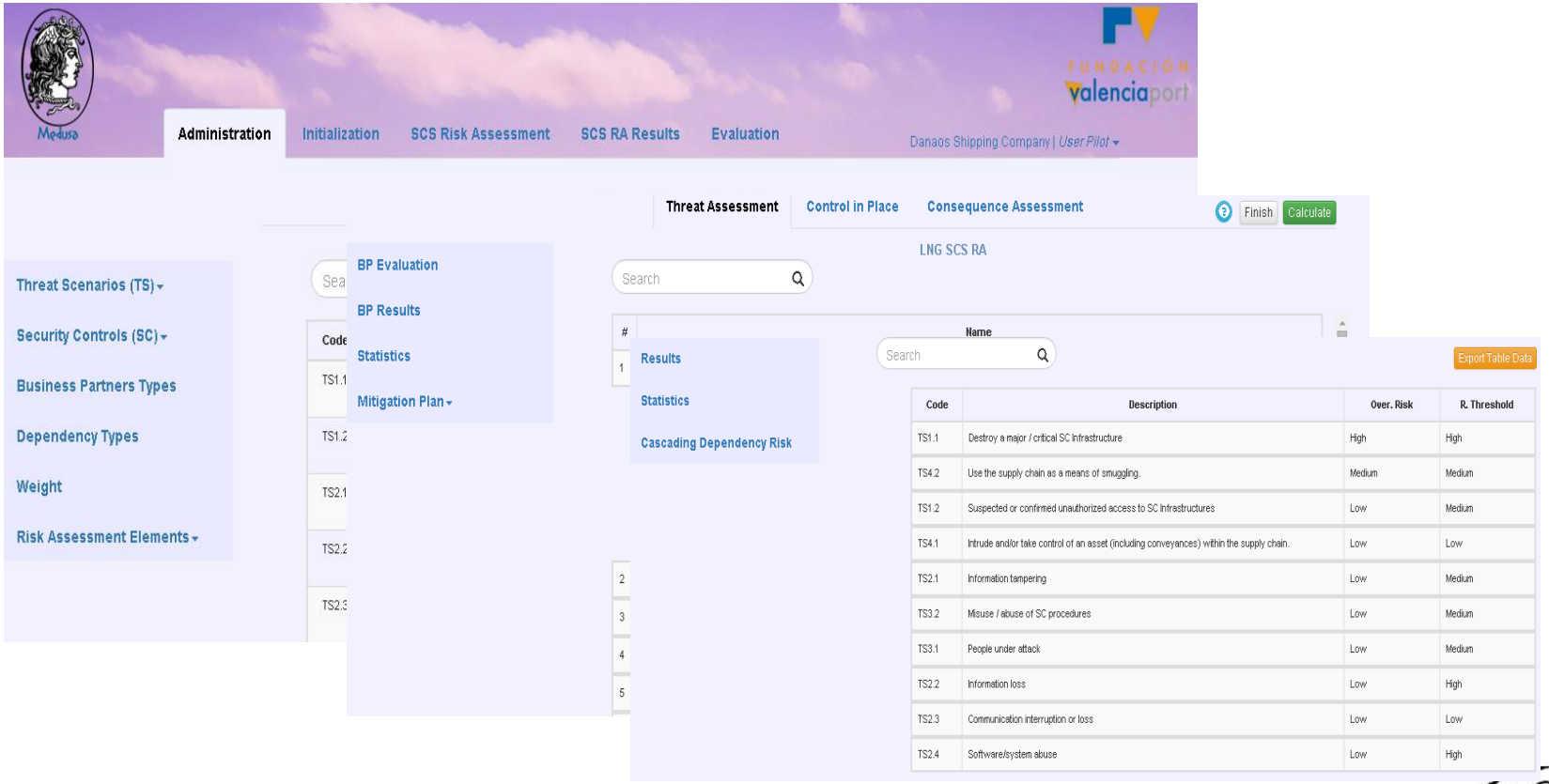
MEDUSA Integrated Risk Management Assessment Framework



Medusa

MEDUSA Supply Chain Risk Management System

http://medusascsra.cs.unipi.gr



Medusa

Medusa Consortium

EUROPHAR

University of Cyprus

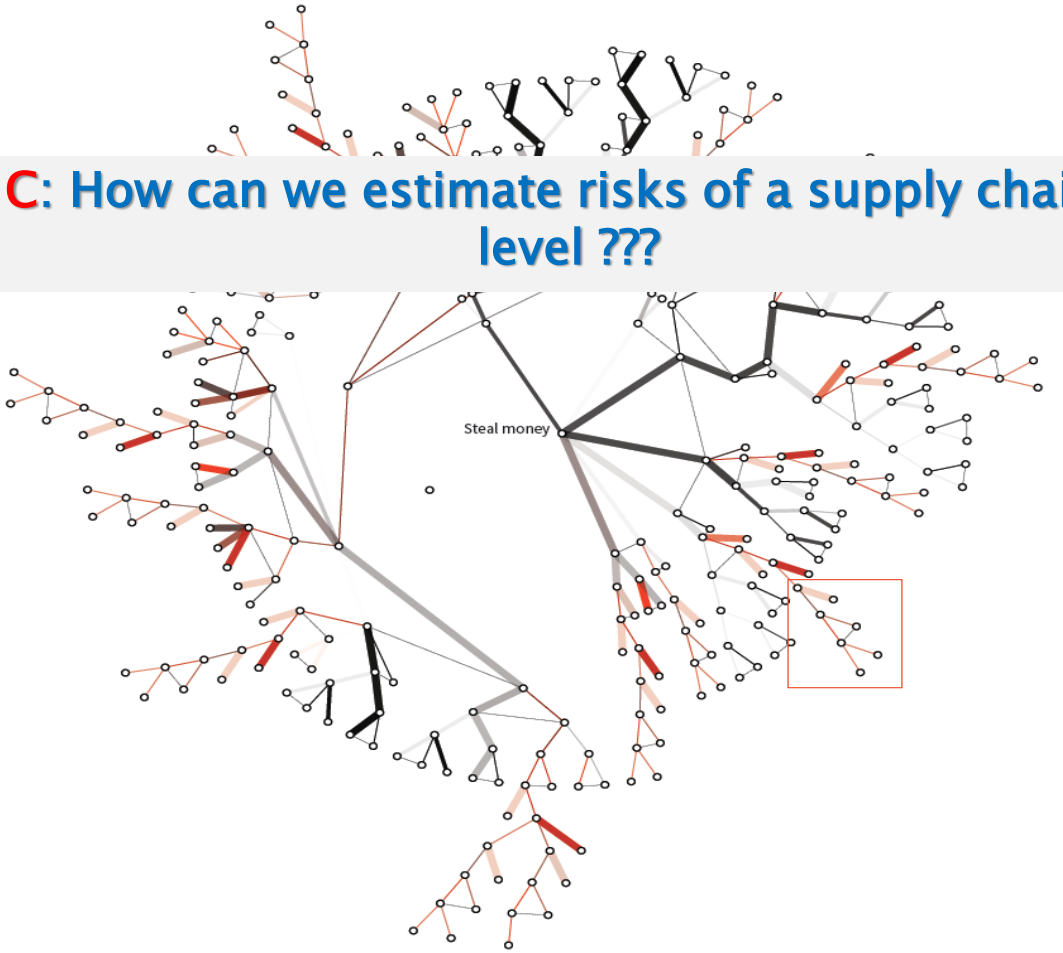
UNIVERSITY OF PIRAEUS RESEARCH CENTER

SingularLogic
Innovation at your doorstep

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

Medusa

ICT-empowered Supply Chain Services



QUESTION C: How can we estimate risks of a supply chain at the asset level ???

MITIGATE

ICT Maritime Supply Chain Service

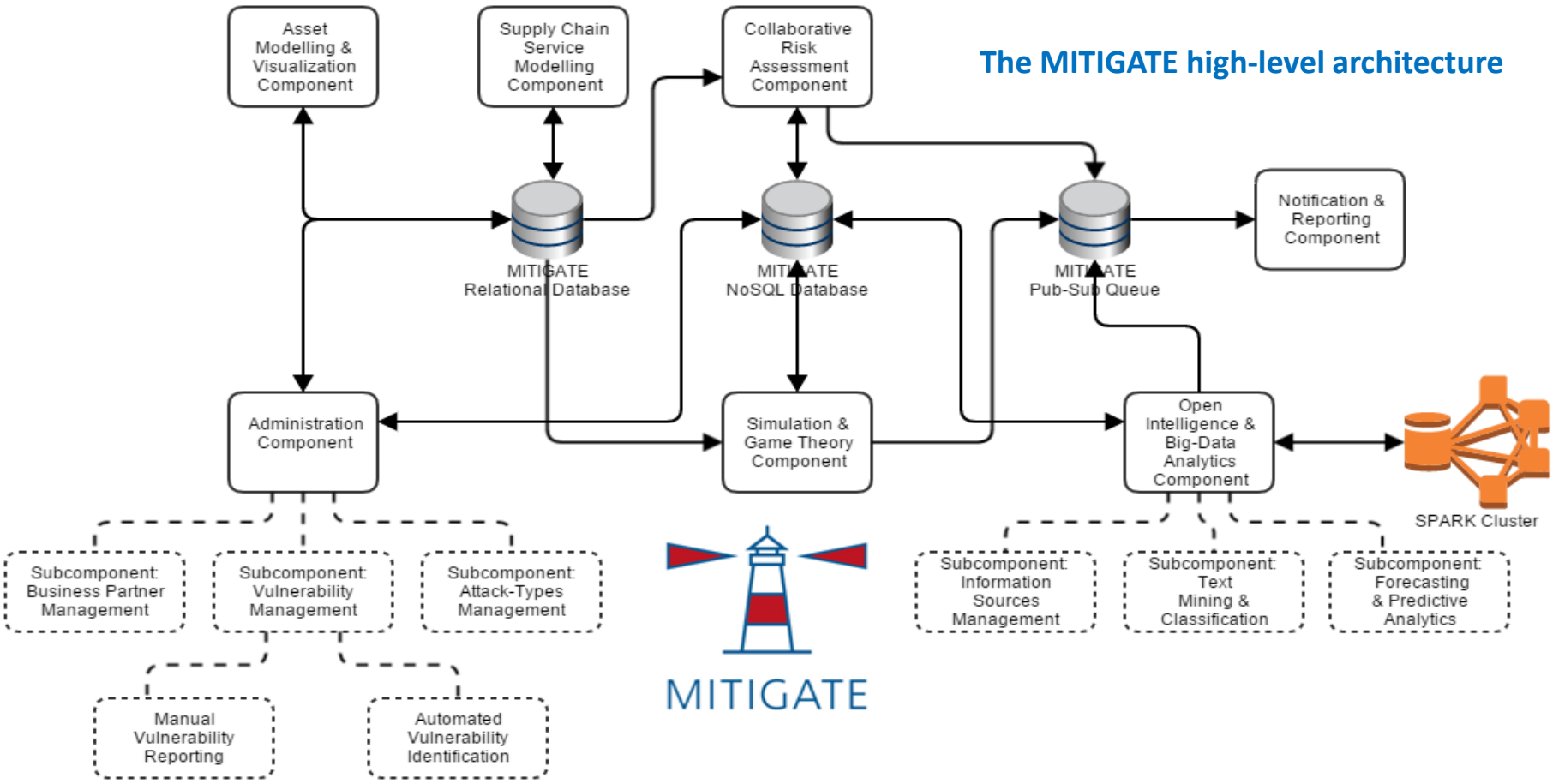
Port Authority
Data Store
Web Server
Application Server
Redundant Client Server
Port's OS (PPA)
Corporate Domain Controller (CDC)
Printer
Workstation
Switch hub
Wireless Modem
Firewall
Enterprise Level
MPLS
WAN
Leased Line
Communication Routers
Control Center
HMI
Engineering Workstation
Virtual Workstation
Switch hub
Wireless Modem
Firewall
Data Historian
DataBase Server
SCADA Host Server (MTU)
WLAN
Supervision Level
Remote Control Station-1
Remote Control Station-2
RTUs
PLCs
Controller Equipment
Actuator
Sensors
Wireless Modem
Microprocessor
Mobile Device
Process Recorder
Software Communicator
Firewall
Distribution Level
Field Level
External Agent user: Transport Company, Carrier Agents
AIS receiver
Automatic Identification System (AIS)
switch
Router
Wireless Modem
Web Client Server
IPsec VPN Client Server
AIS Server
Database Server
Satellite extension Network
Ground Station
VTS Center
AIS Base
Vehicles Loading/Unloading
RoRos & Liner Vessels
Transponder
Amplifier

MITIGATE

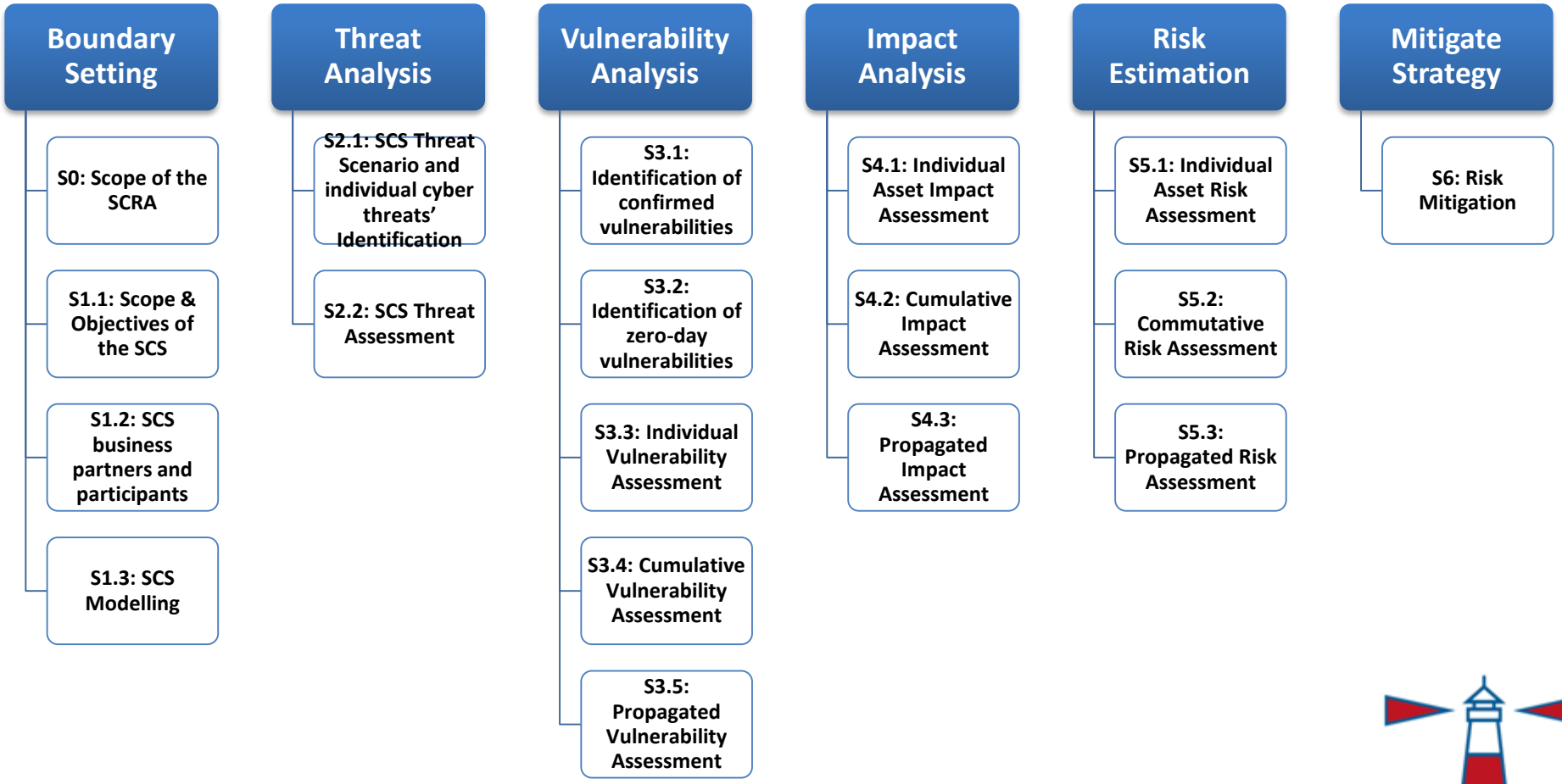
MITIGATE Objectives (mitigateproject.eu)

Goal of MITIGATE is to realize a **radical shift** in risk management methodologies for the maritime sector towards a ***dynamic*** **evidence-driven Maritime Supply Chain Risk Assessment (g-MSRA)** approach that alleviates the limitations of state-of-the-art risk management frameworks.

The MITIGATE high-level architecture



MITIGATE evidence-driven Maritime Supply Chain Risk Assessment (g-MSRA)



MITIGATE

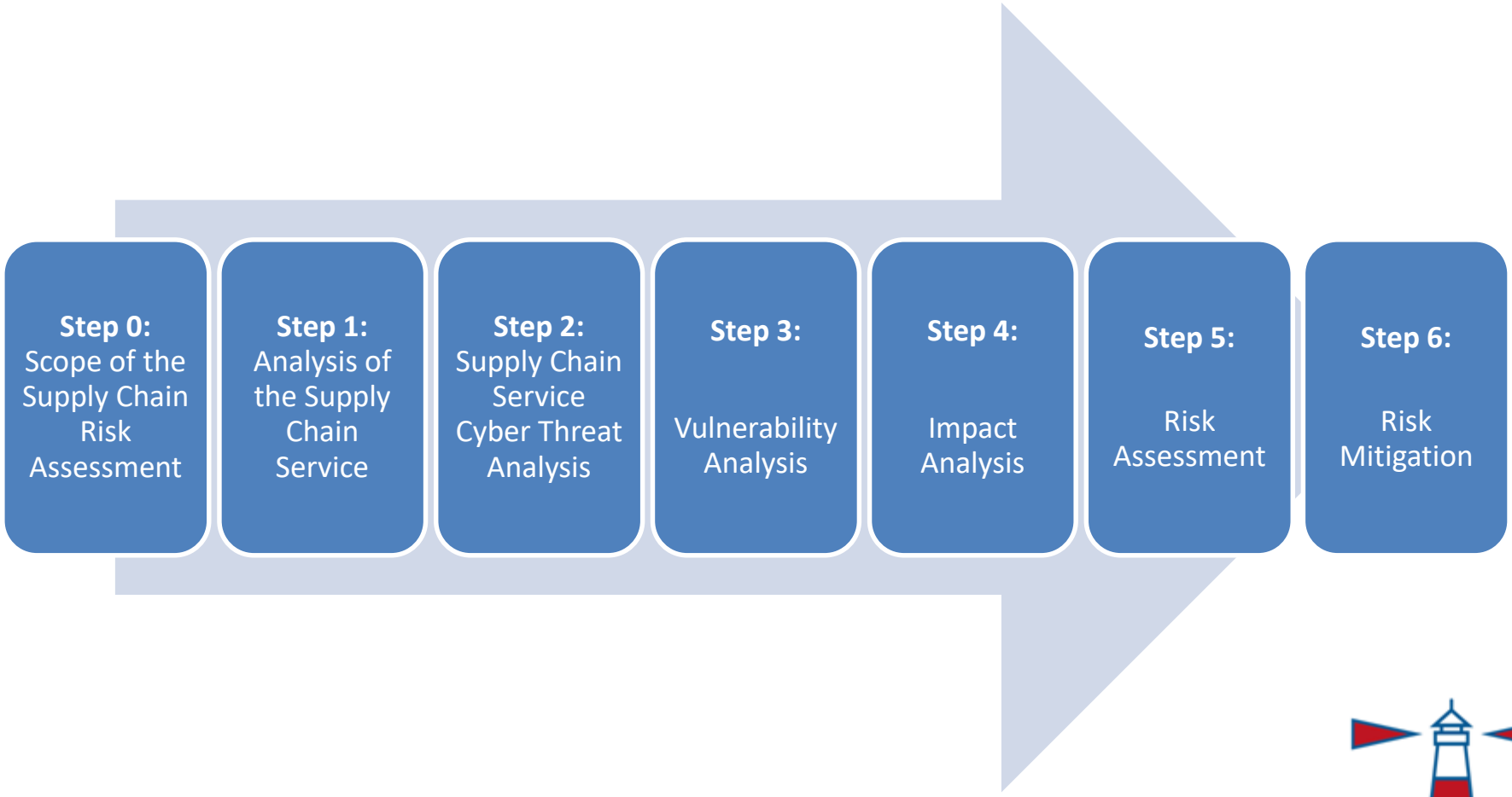
General Idea

- Seven step methodology
  - Based on the risk management process in the standards **ISO 28001** and **ISO 31000**
  - Covers the main activities from **context definition** to **risk identification and analysis** up to **mitigation actions**

- Main objectives of the methodology are tp:
  - identify and measure all relevant **cyber threats**
  - predict potential **attacks/threats paths and patterns**
  - estimate the existence of **zero-day exploitable vulnerabilities**
  - evaluate the **individual**, **cumulative** and **propagated vulnerabilities**
  - assess the potential **impacts**
  - derive and prioritize the corresponding **risks**
  - formulate a proper **mitigation strategy**

MITIGATE

Steps of the Methodology



MITIGATE

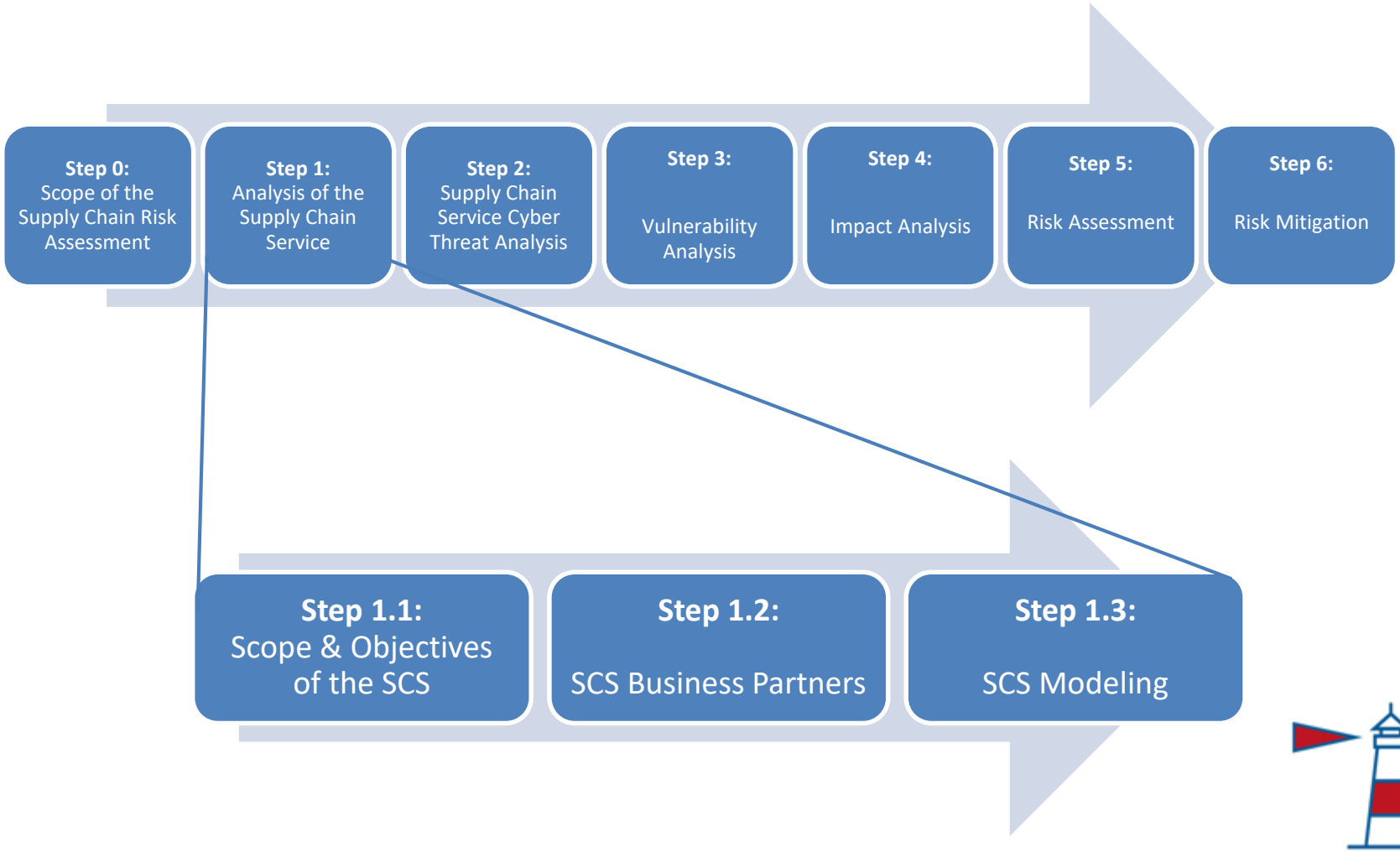
Step 0:
Scope of the SC Risk Assessment

- **Scope:**
  - Selection of the Supply Chain Service (SCS)
  - Definition of the **boundaries** for the assessment (overall scope, main goals, expected outcome)
- **Outcome:**
  - Specification of the boundaries for the SC risk assessment
- **Example:**

Supply Chain Risk Assessment (SCRA): Vehicles Transport Service Risk Assessment	
Scope of the SC RA	All ICT assets and components required for the provision of the Vehicles Transport Service
Goal of the SC RA	Identification, analysis, assessment and migration of all ICT-related Threat Scenario, vulnerabilities and risks associated with the Vehicles Transport Service.
Expected output	Evaluation of the ICT-related element of the Vehicles Transport Service

MITIGATE

Step 1:
Analysis of the SCS



MITIGATE

Step 1:
Analysis of the SCS

- **Scope:**
  - Description of the SCS
  - Identification of the **business partners**, $\mathrm{bp_n}$, participating in the SCS
  - Identification and modeling of the **main processes** involved in the SCS

- **Outcome:**
  - Textual description of the SCS
  - List of **business partners and participants** involved in the SCS risk assessment
  - List of **Supply Chain Service's Business Processes** (SCSBPs)
- Set of **SCS cyber assets** as well as their **interconnections** and **interdependencies (**hosting, exchange data/information, storing, controlling, processing, accessing, installing, trusted)

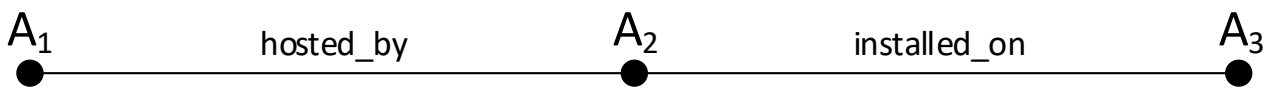
MITIGATE

- **Example:**

Supply Chain Service	Purchase & shipment of the Vehicles Transport Service
Description:	The Vehicles Transport Chain Service is a massively complex system with numerous players, including shippers, transport operators aiming at the shipment and receipt of various types of vehicles and equipment such as trucks, vans, truck trailers, threshing machines etc. This Service is a relatively long and complicated process that involves domestic and international transportation, warehouse management, order and inventory control, materials handling, import/export facilitation, and information technology.
Goal of the SCS	Deliver the Vehicles to the Source Port and complete all the required preparations for shipping.
Expected output	Delivery of vehicles to source port

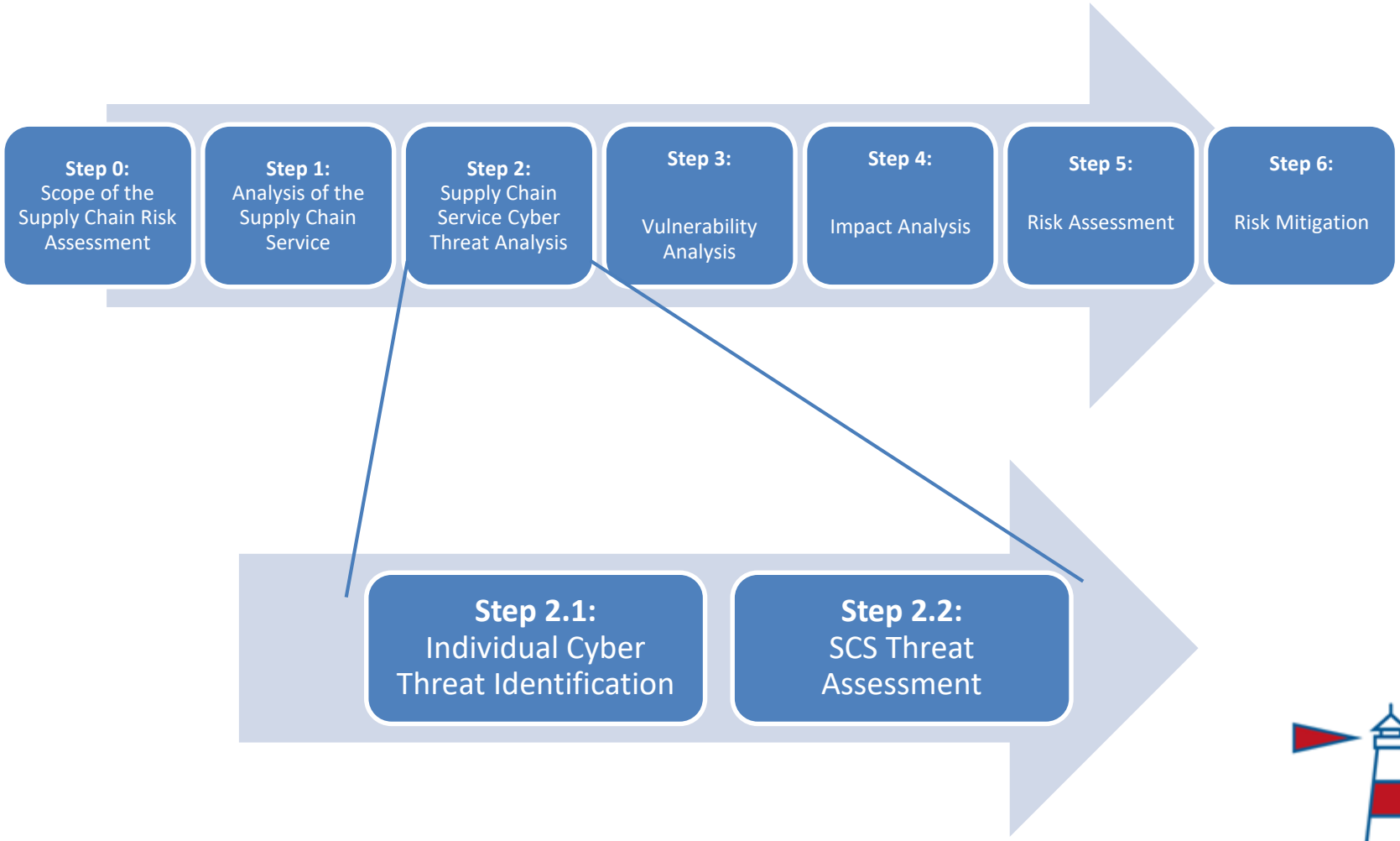
Node ID (x_i)	Asset Code	Name	Category	Product Name	Version	Vendor
bp_0	A_1	Port Community System	Web Application	Custom Application	Oracle Supply Chain Products Suite 12.0.6	Custom Application
	A_2	PCS Application Server	Web Server	Apache HTTP Server	Apache HTTP Server 2.0.37	Apache
	A_3	PCS Operating System	Operating system	Microsoft Windows Server 2012	Windows 2012 (Version 1, Release 4)	Microsoft

Node ID (x_i)	Asset Source	Asset Destination	Dependency Type	Dependency Access Vector
bp_0	A_1	A_3	1. hosting	Local (L)
	A_2	A_3	7. installing	Local (L)



MITIGATE

Step 2:
SCS Cyber Threat Analysis



MITIGATE

Step 2.1: Ind. Cyber Threat Identification

- **Scope:**
  - Identification of all individual cyber threats against the cyber assets within the SCS
  - Information can come from
    - **business partners** (based on their expertise),
    - existing **repositories** of cyber threats,
    - from **crowdsourcing** (a community of online users/security experts/stakeholders) or
    - from **social media** (discussion groups or forums)
- **Outcome:**
  - List of individual cyber threats applicable to the SCS cyber assets
  - Set of correspondences of individual cyber threats to the cyber assets within the SCS
- **Example:**

Code	Cyber Threats Name
$T_{1,A_{0,1}}$	Information tampering
$T_{2,A_{0,1}}$	Information loss
$T_{3,A_{0,1}}$	Communication interruption or loss

MITIGATE

WASC Threat Classification 2.0 and CAPEC

Authentication Issues	CWE-287	When an actor claims to have a given identity, the software does not prove or insufficiently proves that the claim is correct.
Buffer Errors	CWE-119	The software performs operations on a memory buffer, but it can read from or write to a memory location that is outside of the intended boundary of the buffer.
Code	CWE-17	Weaknesses in this category are typically introduced during code development, including specification, design, and implementation.
Code Injection	CWE-94	The software constructs all or part of a code segment using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the syntax or behavior of the intended code segment.
Command Injection	CWE-77	The software constructs all or part of a command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended command when it is sent to a downstream component.
Configuration	CWE-16	Weaknesses in this category are typically introduced during the configuration of the software.
Credentials Management	CWE-255	Weaknesses in this category are related to the management of credentials.
Cross-Site Request Forgery (CSRF)	CWE-352	The web application does not, or cannot, sufficiently verify whether a well-formed, valid, consistent request was intentionally provided by the user who submitted the request.
Cross-Site Scripting (XSS)	CWE-79	The software does not neutralize or incorrectly neutralizes user-controllable input before it is placed in output that is used as a web page that is served to other users.
Cryptographic Issues	CWE-310	Weaknesses in this category are related to the use of cryptography.
Data Handling	CWE-19	Weaknesses in this category are typically found in functionality that processes data.
Format String Vulnerability	CWE-134	The software uses externally-controlled format strings in printf-style functions, which can lead to buffer overflows or data representation problems.
Improper Access Control	CWE-284	The software does not restrict or incorrectly restricts access to a resource from an unauthorized actor.
Indicator of Poor Code Quality	CWE-398	The code has features that do not directly introduce a weakness or vulnerability, but indicate that the product has not been carefully developed or maintained.

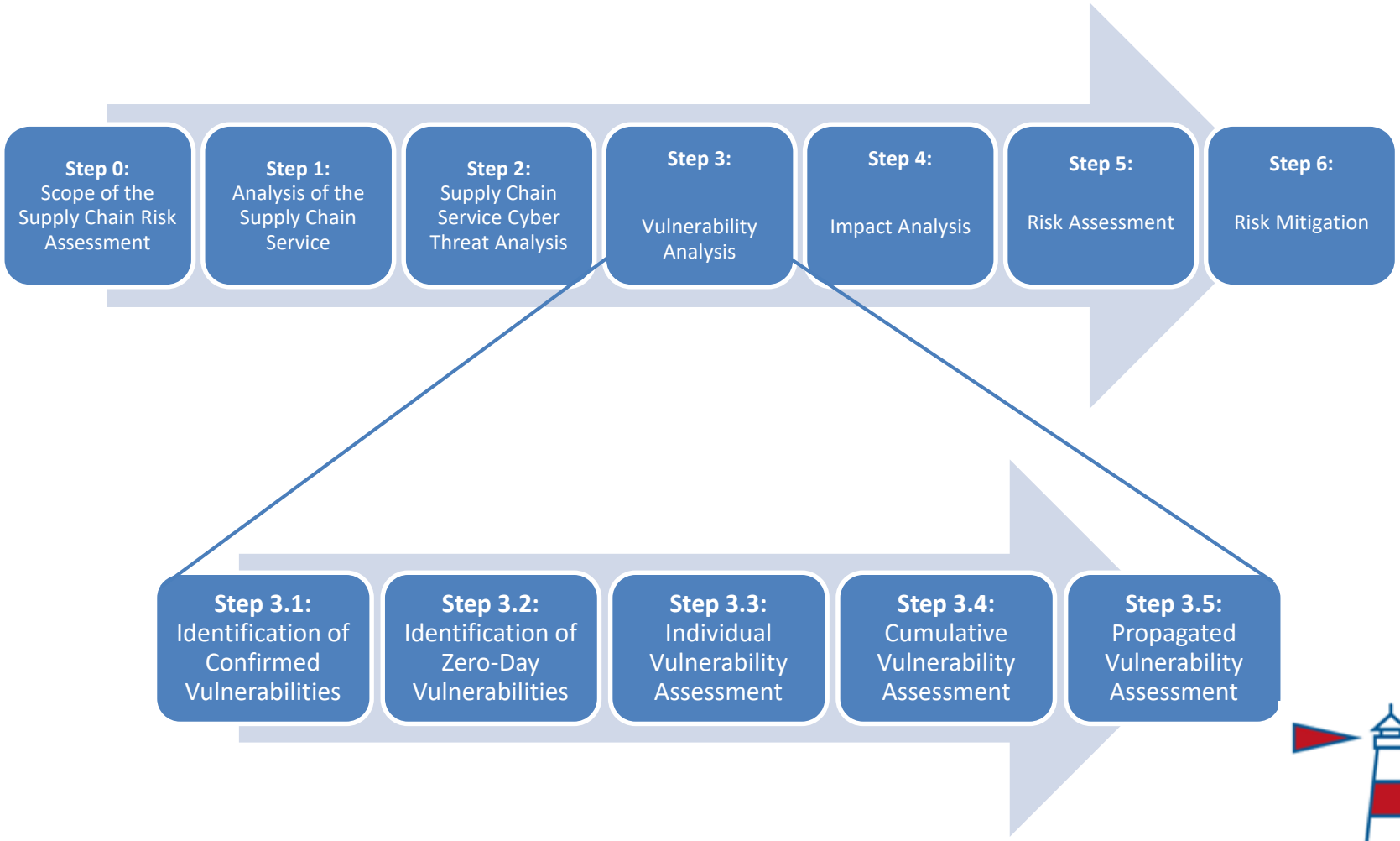
MITIGATE

Step 2.2: SCS Threat Assessment

- **Scope:**
  - Assessment of the probability of occurrence for each cyber threat scenario on each cyber asset
  - Calculation based on
    - **expected frequency of appearance** (history of previous incidents)
    - information retrieved from **existing repositories and social media** and
    - business partner's **expert knowledge**
- **Outcome:**
  - List of threat levels of each threat scenario to each cyber asset

Threat scale			Description of threat level		
Threat class	Value Range (%)	Default Value (%)	History of incidents	Intuition & knowledge	Social Information
Very High (5)	(80-100]	100	This threat was realized more than once in the last year (12 month period).	This threat is expected to occur within the assets of the business partner with very high probability (more than 80% probability)	This threat is expected to occur within the assets of the business partner with very high probability (more than 80% probability)
High (4)	(60-80]	80	This threat was realized once in the last 1 year (12 month period).	This threat is expected to occur within the assets of the business partner with high probability (61-80% probability)	This threat is expected to occur within the assets of the business partner with high probability (61-80% probability)
Medium (3)	(40-60]	60	More than one incident of this threat was realized in the last 2 years.	This threat is expected to occur within the assets of the business partner with medium probability (41-60% probability)	This threat is expected to occur within the assets of the business partner with medium probability (41-60% probability)
Low (2)	(20-40]	40	At most one incident of this threat was realized in the last 2 years.	This threat is expected to occur within the assets of the business partner with low probability (21-40% probability)	This threat is expected to occur within the assets of the business partner with low probability (21-40% probability)
Very low (1)	[1 – 20]	20	At most one incident of this threat was realized in the last 3 years or no incident was realised	This threat is expected to occur within the assets of the business partner with very low probability (at most 20% probability)	This threat is expected to occur within the assets of the business partner with very low probability (at most 20% probability)

Step 3: Vulnerability Analysis



MITIGATE

- **Example:**

Microsoft » Windows Server 2012 : Vulnerability Statistics

Vulnerabilities (546) CVSS Scores Report Browse all versions Possible matches for this product Related Metasploit Modules

Related OVAL Definitions : Vulnerabilities (184) Patches (0) Inventory Definitions (2) Compliance Definitions (0)

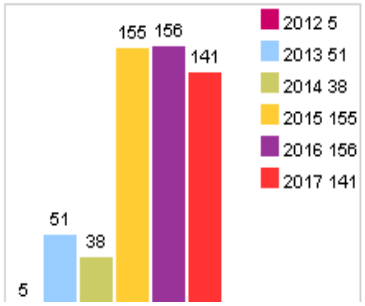
Vulnerability Feeds & Widgets

Vulnerability Trends Over Time

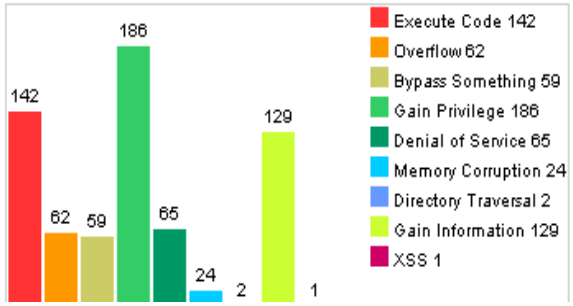
Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2012	5		2	2						1		2			
2013	51	12	17	17	3			1		2	2	21			4
2014	38	9	11	5	3					6	5	12			4
2015	155	16	46	11	9			1		31	26	60			1
2016	156	8	42	19	7					16	28	76			
2017	141	20	24	8	2		1			3	68	15			
Total	546	65	142	62	24		1	2		59	129	186			9
% Of All		11.9	26.0	11.4	4.4	0.0	0.2	0.4	0.0	10.8	23.6	34.1	0.0	0.0	

Warning : Vulnerabilities with publish dates before 1999 are not included in this table and chart. (Because there are not many of them and they make the page look bad; and they may not be actually published in those years.)

Vulnerabilities By Year



Vulnerabilities By Type



MITIGATE

- **Example:**

Vulnerability Details : CVE-2016-0037

The forms-based authentication implementation in Active Directory Federation Services (ADFS) 3.0 in Microsoft Windows Server 2012 R2 allows remote attackers to cause a denial of service (daemon outage) via crafted data, aka "Microsoft Active Directory Federation Services Denial of Service Vulnerability."

Publish Date : 2016-02-10 Last Update Date : 2017-03-23

Collapse All Expand All Select Select&Copy Scroll To Comments External Links

Search Twitter Search YouTube Search Google

– CVSS Scores & Vulnerability Types

CVSS Score	5.0
Confidentiality Impact	None (There is no impact to the confidentiality of the system.)
Integrity Impact	None (There is no impact to the integrity of the system)
Availability Impact	Partial (There is reduced performance or interruptions in resource availability.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Denial Of Service
CWE ID	20

– Products Affected By CVE-2016-0037

#	Product Type	Vendor	Product	Version	Update	Edition	Language	
1	OS	Microsoft	Windows Server 2012	R2	-	~-~datacenter~~~		Version Details Vulnerabilities
2	OS	Microsoft	Windows Server 2012	R2	-	~-~standard~~~		Version Details Vulnerabilities
3	OS	Microsoft	Windows Server 2012	R2	-	~-~essentials~~~		Version Details Vulnerabilities

– Number Of Affected Versions By Product

Vendor	Product	Vulnerable Versions

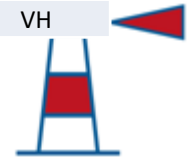
CWE - 20 : Improper Input Validation

CWE Definition	http://cwe.mitre.org/data/definitions/20.html
Number of vulnerabilities:	4542
Description	The product does not validate or incorrectly validates input that can affect the control flow or data flow of a program.When software fails to validate input properly, an attacker is able to craft the input in a form that is not expected by the rest of the application. This will lead to parts of the system receiving unintended input, which may result in altered control flow, arbitrary control of a resource, or arbitrary code execution.
Background Details	
Other Notes	

- **Example:**

Vulnerability	Asset	CVE Number	CVSS Exploitability			Individual Vulnerability Level
			AV	AC	Auth	
V_1	A_1	N/A	N	L	S	VH
V_2	A_1	N/A	A	M	S	M
V_3	A_1	N/A	N	M	N	VH
V_4	A_2	CVE-2013-6111	N	M	N	VH
V_5	A_2	CVE-2014-4721	N	H	N	H
V_6	A_3	CVE-2016-0099	L	L	N	M
V_7	A_3	CVE-2016-0037	N	L	N	VH
V_8	A_3	CVE-2016-0016	L	M	N	L

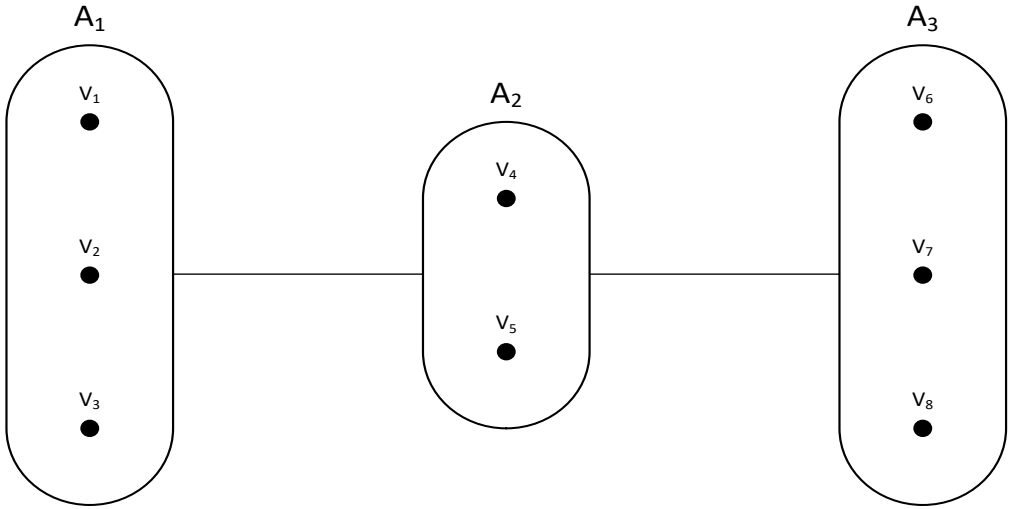
AV / AC / Auth	Local			Adjacent			Network		
	High	Medium	Low	High	Medium	Low	High	Medium	Low
Multiple	VL	VL	L	L	M	M	M	H	H
Single	VL	L	L	M	M	M	H	H	VH
None	L	L	M	M	M	H	H	VH	VH



MITIGATE

Step 3.4: Cumulative Vulnerabilities

- **Example:**



- **Scope:**
  - Individual vulnerability level does not take the “way to reach the cyber asset” into account (i.e., the preconditions)
  - Vulnerability of a cyber assets can be accessed by exploiting **vulnerabilities on other cyber assets** in the supply chain
  - Exploitation probability can be different to the individual vulnerability
    - Individual vulnerability level is calculated “high”, but the cyber asset may reside at a location that is very difficult for an attacker to access
    - Individual vulnerability level is calculated “low”, but an attacker might easily access the asset using a connected cyber asset with a “high” vulnerability
  - Path to **reach the cyber assets** needs to be taken into account
- **Outcome:**
  - The **Cumulative Vulnerability Levels** (CVL) including all sub-chains with vulnerabilities, entry and target points

MITIGATE

Propagation and Path Construction Rules

- Rules to discover which vulnerabilities on the SCS can be used as stepping stones (traversed) by the attacker to reach other vulnerabilities
- $\forall vuln, asset1, asset2, attacker \;\; Attacked(vuln, asset1, attacker) \wedge \left(\begin{array}{c} ExecuteCode(vuln) \vee Overflow(vuln) \vee XSS(vuln) \vee BypassSomething(vuln) \vee \\ GainPrivilege(vuln) \vee MemoryCorruption(vuln) \end{array} \right)$
  $Connected(asset1, asset2) \Rightarrow Traversable(vuln, asset1, asset2, attacker)$
  A connection between two assets is traversable if the starting vulnerability has been successfully attacked and its vulnerability type allows the attacker to use it as a stepping stone to access the end asset
- $\forall vuln1, asset1, vuln2, asset2, attacker \;\; Attacked(vuln1, asset1, attacker) \wedge (ExecuteCode(vuln1) \vee Overflow(vuln1) \vee XSS(vuln1) \vee BypassSomething(vuln1) \vee GainPrivilege(vuln1) \vee MemoryCorruption(vuln1)) \Rightarrow Traversable(vuln1, asset1, vuln2, asset2, attacker)$
  A connection between two vulnerabilities affecting assets (or the same asset) is traversable if the starting vulnerability has been successfully attacked and its vulnerability type allows the attacker to use it as a stepping stone to access the end vulnerability

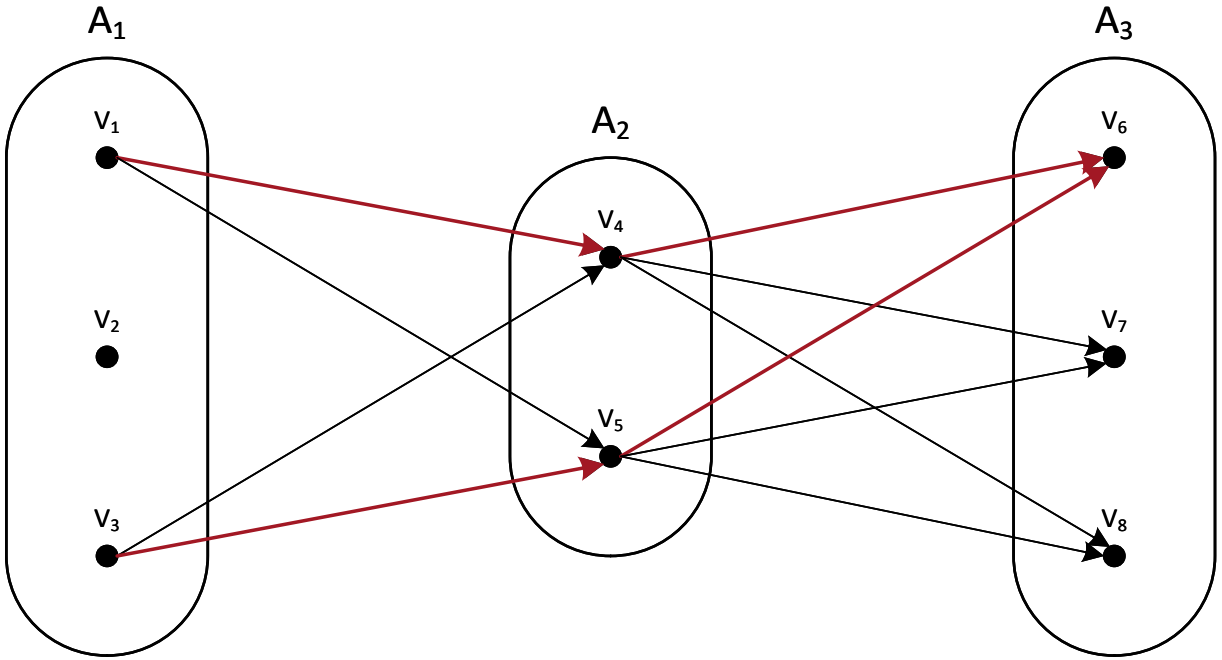
MITIGATE

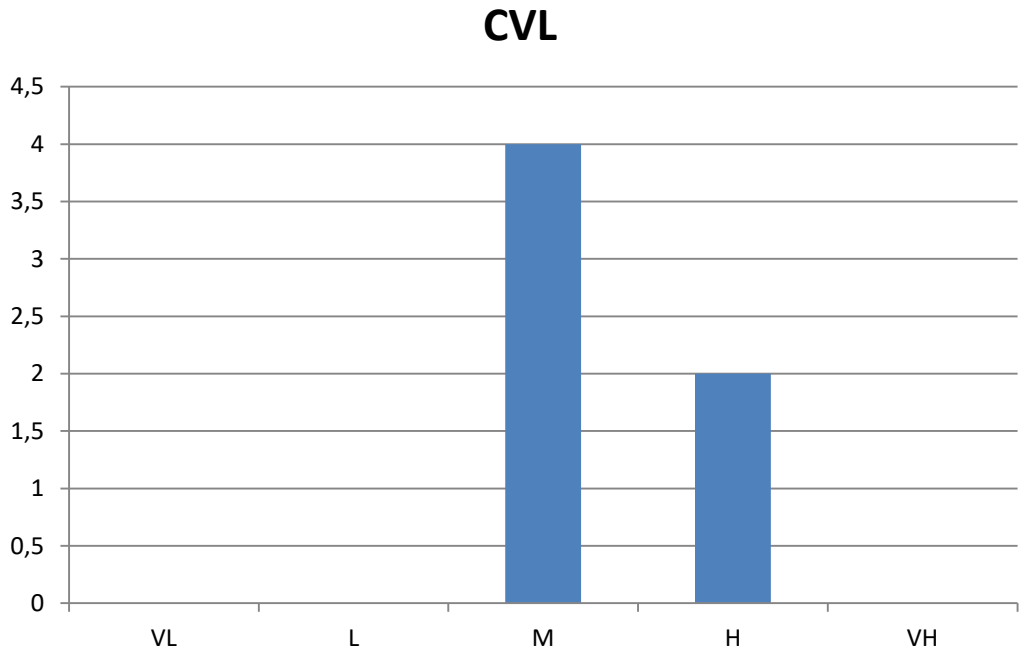
- **Example:**

Entry Point	Chain	Categories	Probability	ICVL
V_1	$V_1 \rightarrow V_4 \rightarrow V_6$	$VH \rightarrow VH \rightarrow H$	$0.93 \times 0.93 \times 0.75 = 0.65$	H
V_1	$V_1 \rightarrow V_5 \rightarrow V_6$	$VH \rightarrow H \rightarrow H$	$0.93 \times 0.75 \times 0.75 = 0.52$	M
V_3	$V_3 \rightarrow V_4 \rightarrow V_6$	$VH \rightarrow VH \rightarrow H$	$0.93 \times 0.93 \times 0.75 = 0.65$	H
V_3	$V_3 \rightarrow V_5 \rightarrow V_6$	$VH \rightarrow H \rightarrow H$	$0.93 \times 0.75 \times 0.75 = 0.52$	M
V_4	$V_4 \rightarrow V_6$	$H \rightarrow H$	$0.75 \times 0.75 = 0.56$	M
V_5	$V_5 \rightarrow V_6$	$H \rightarrow H$	$0.75 \times 0.75 = 0.56$	M

MITIGATE Probability Scale		
Qualitative Values	Representative	
	Range	Number
Very High	0.85 – 1.00	0.93
High	0.65 – 0.84	0.75
Moderate	0.35 – 0.64	0.50
Low	0.15 – 0.34	0.25
Very Low	0.00 – 0.14	0.07

IVL \ Capability	Very Low	Low	Moderate	High	Very High
Very Low	VL	VL	L	L	M
Low	VL	L	L	M	H
Moderate	L	L	M	H	H
High	L	M	H	H	VH
Very High	M	H	H	VH	VH

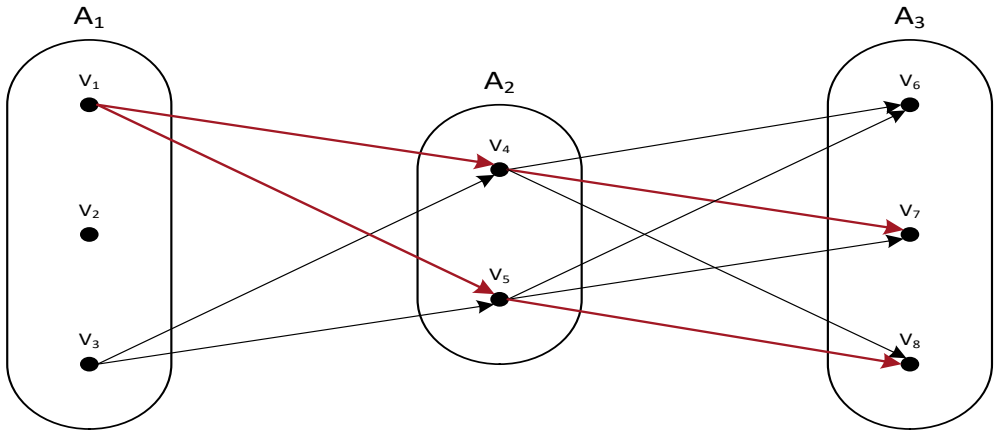


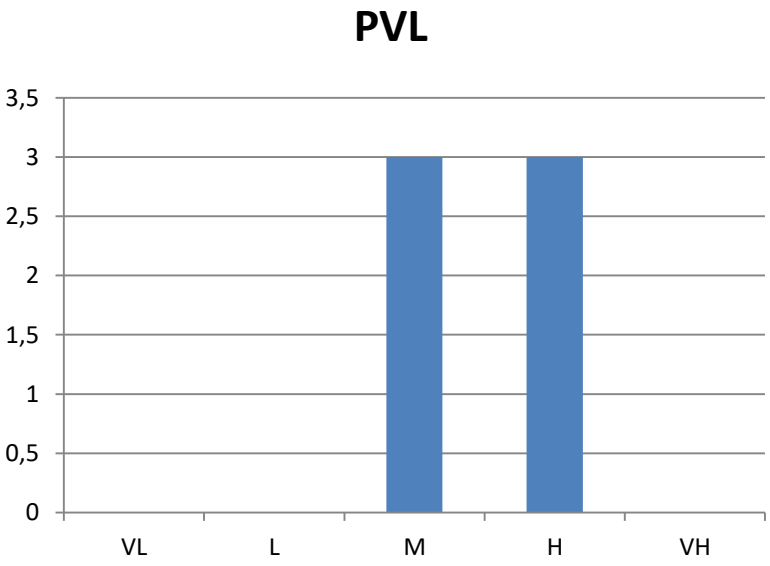


MITIGATE

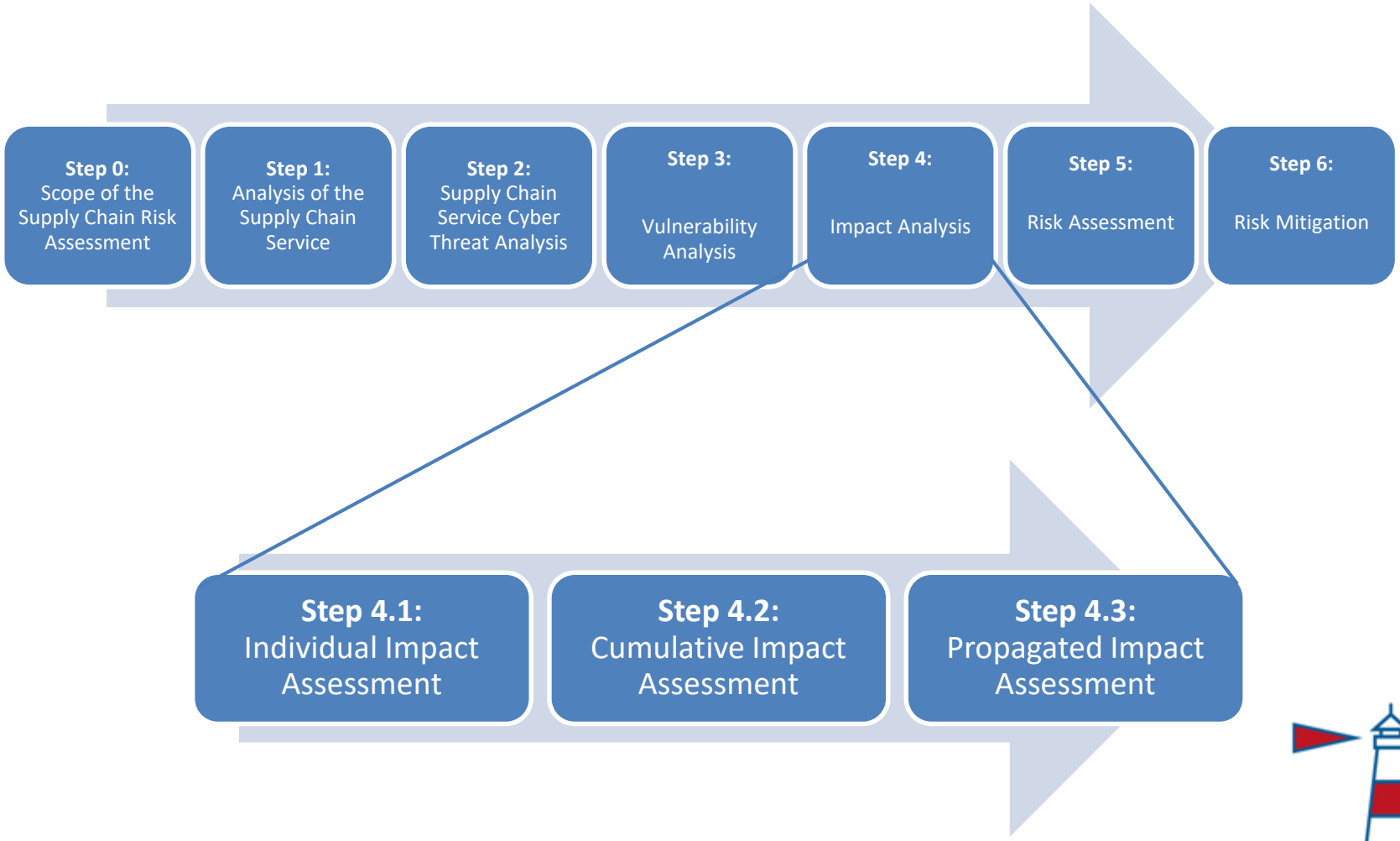
Step 3.5: Propagated Vulnerabilities

Entry Point	Chain	Categories	Probability	ICVL
V_1	$V_1 \rightarrow V_4 \rightarrow V_6$	VH → VH → H	$0.93 \times 0.93 \times 0.75 = 0.65$	H
V_1	$V_1 \rightarrow V_4 \rightarrow V_7$	VH → VH → VH	$0.93 \times 0.93 \times 0.93 = 0.80$	H
V_1	$V_1 \rightarrow V_4 \rightarrow V_8$	VH → VH → M	$0.93 \times 0.93 \times 0.50 = 0.43$	M
V_1	$V_1 \rightarrow V_5 \rightarrow V_6$	VH → H → H	$0.93 \times 0.75 \times 0.75 = 0.52$	M
V_1	$V_1 \rightarrow V_5 \rightarrow V_7$	VH → H → VH	$0.93 \times 0.75 \times 0.93 = 0.65$	H
V_1	$V_1 \rightarrow V_5 \rightarrow V_8$	VH → H → M	$0.93 \times 0.75 \times 0.50 = 0.35$	M





Step 4:
Impact Analysis



MITIGATE

Step 4.1: Individual Impacts

- **Scope:**
  - Estimation of the **impact of all identified vulnerabilities**
  - Calculation of the (qualitative) damage in case a vulnerability is successfully exploited
    - Using the CVSS metrics (retrieved from the online databases)
    - Taking into account the applied controls described in the Enhanced Security Declaration (e.g., for policy related/social/organizational vulnerabilities)
- **Outcome:**
  - **Individual Impact Levels** (IIL) of each vulnerability in all cyber assets

Example:

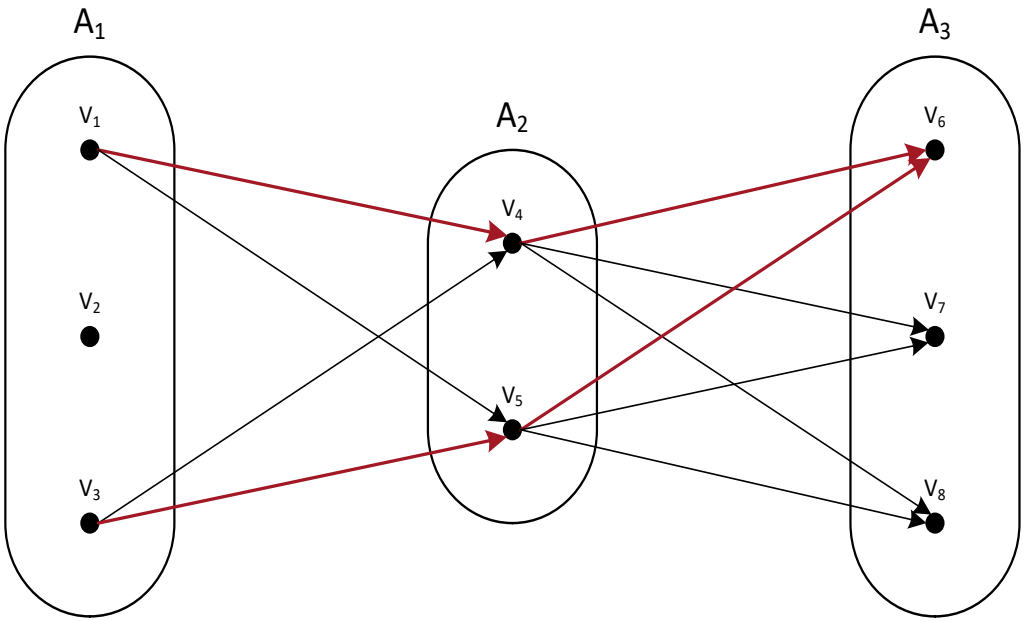
Vulnerability	Asset	CVE Number	CVSS Impact			Individual Impact Level
			C	I	A	
V_1	A_1	N/A	C	C	C	VH
V_2	A_1	N/A	P	P	N	M
V_3	A_1	N/A	C	C	P	VH
V_4	A_2	CVE-2013-6111	N	P	N	VL
V_5	A_2	CVE-2014-4721	N	P	N	VL
V_6	A_3	CVE-2016-0099	C	C	C	VH
V_7	A_3	CVE-2016-0037	N	N	P	VL
V_8	A_3	CVE-2016-0016	C	C	C	VH

C / I / A	None			Partial			Complete		
	None	Partial	Complete	None	Partial	Complete	None	Partial	Complete
None	VL	VL	L	L	M	M	M	H	H
Partial	VL	L	L	M	M	M	H	H	VH
Complete	L	L	M	M	M	H	H	VH	VH

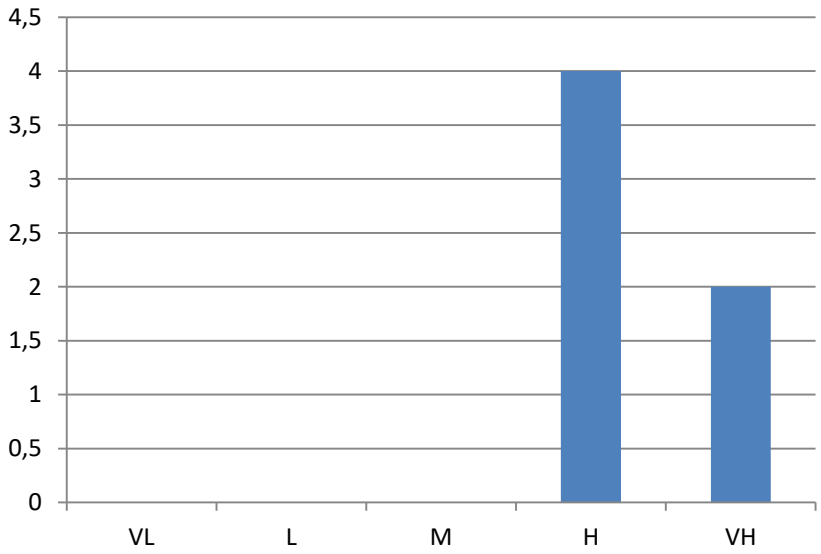
Step 4.2: Cumulative Impacts

Example:

Entry Point	Chain	Categories	ICVL	Impact	ICIL
V_1	$V_1 \rightarrow V_4 \rightarrow V_6$	VH → VH → H	H	VH	VH
V_1	$V_1 \rightarrow V_5 \rightarrow V_6$	VH → H → H	M	VH	H
V_3	$V_3 \rightarrow V_4 \rightarrow V_6$	VH → VH → H	H	VH	VH
V_3	$V_3 \rightarrow V_5 \rightarrow V_6$	VH → H → H	M	VH	H
V_1	$V_4 \rightarrow V_6$	H → H	M	VH	H
V_2	$V_5 \rightarrow V_6$	H → H	M	VH	H



CIL



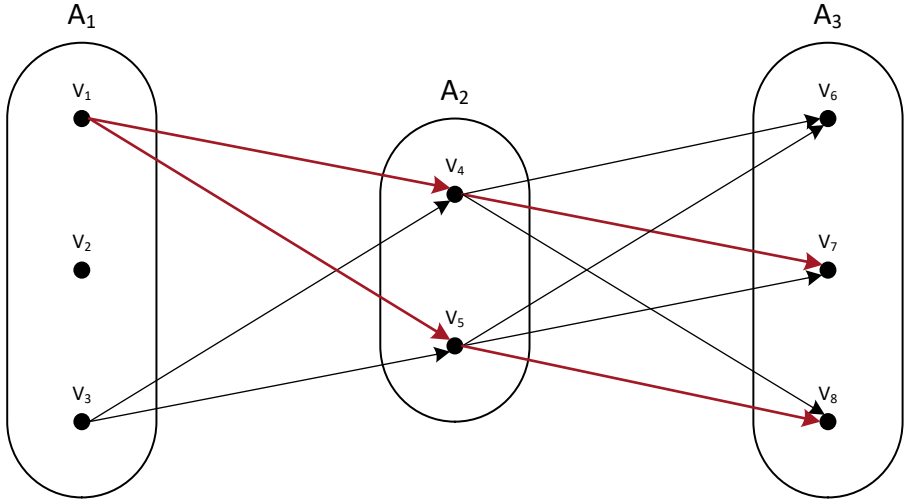
Step 4.3: Propagated Impacts

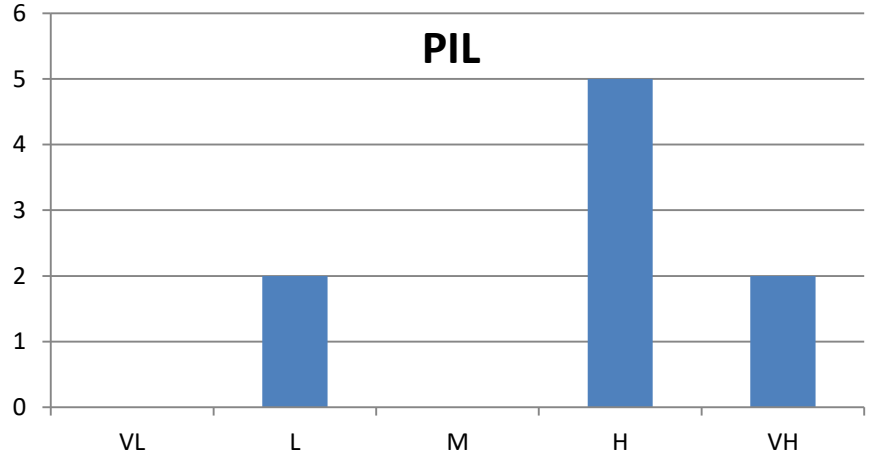
- **Scope:**
  - Definition of the **impact** after exploiting a specific asset/vulnerability combination and **further moves on into the network**
  - Relates to the damage an attack can cause at **any asset/vulnerability combination on his way through the network**
  - All damage on all paths of length l through the network is taken into account

- **Outcome:**
  - **Propagated Impact Level** (PIL) of each vulnerability in all SCS cyber assets

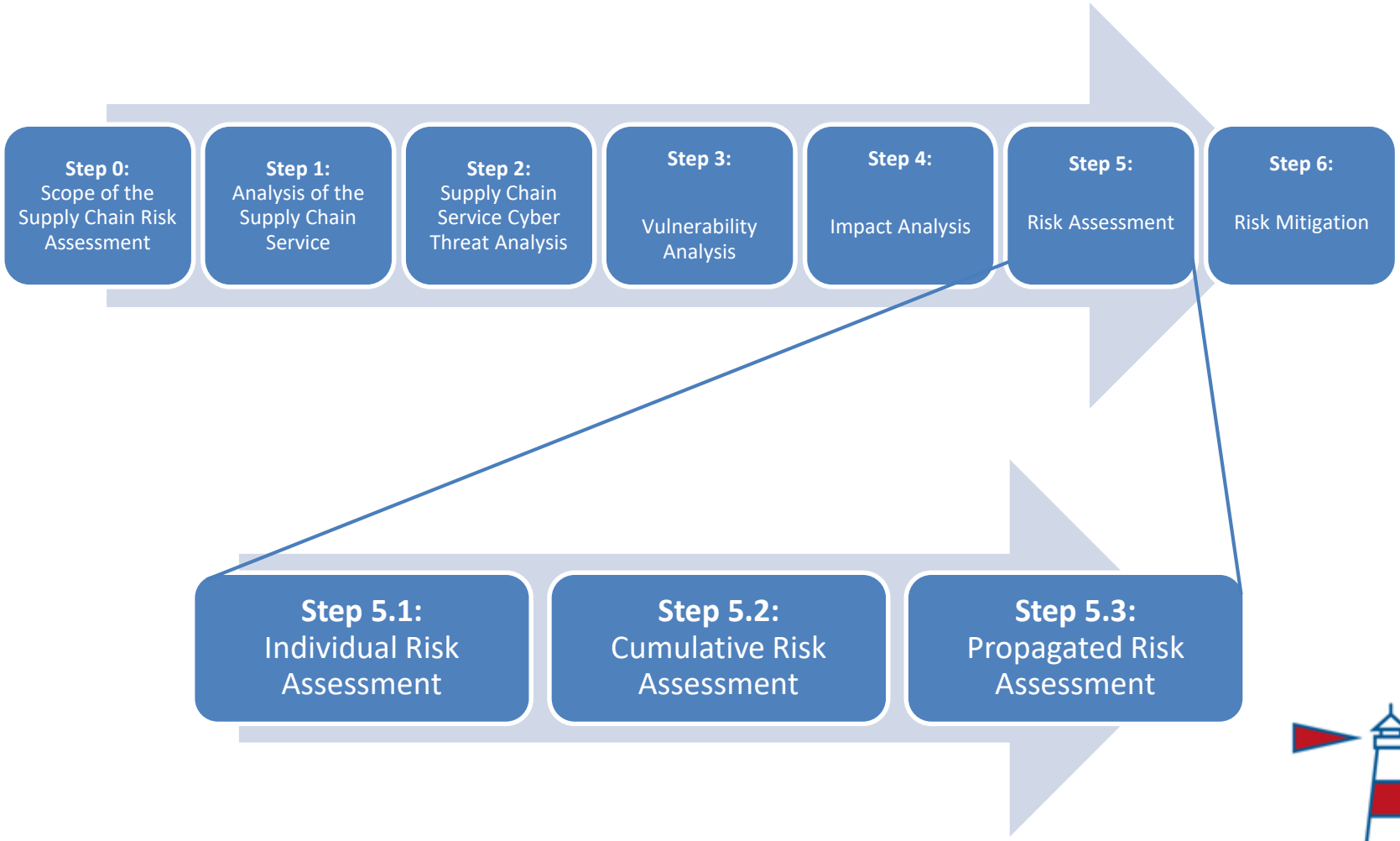
MITIGATE

Entry Point	Chain	Categories	ICVL	Impact	IPIL
V_1	$V_1 \rightarrow V_4 \rightarrow V_6$	VH → VH → H	H	VH	H
V_1	$V_1 \rightarrow V_4 \rightarrow V_7$	VH → VH → VH	H	VL	L
V_1	$V_1 \rightarrow V_4 \rightarrow V_8$	VH → VH → M	M	VH	H
V_1	$V_1 \rightarrow V_5 \rightarrow V_6$	VH → H → H	M	VH	H
V_1	$V_1 \rightarrow V_5 \rightarrow V_7$	VH → H → VH	H	VL	L
V_1	$V_1 \rightarrow V_5 \rightarrow V_8$	VH → H → M	M	VH	H
V_1	$V_1 \rightarrow V_4$	VH → VH	VH	VH	VH
V_1	$V_1 \rightarrow V_5$	VH → H	H	H	H
V_1	V_1	VH	VH	VH	VH





Step 5: Risk Assessment



MITIGATE

Step 5.1: Individual Risks

- **Scope:**
  - Individual risk consisting of all the collected values for each asset in the SCS
    - Individual Vulnerability Level (IVL)
    - Individual Impact Level (IIL)
    - Threat Level
  - All three **qualitative values are combined**
  - Result is again a qualitative value
- **Outcome:**
  - **Individual Risk Levels** (IRL)for a specific threat on specific asset

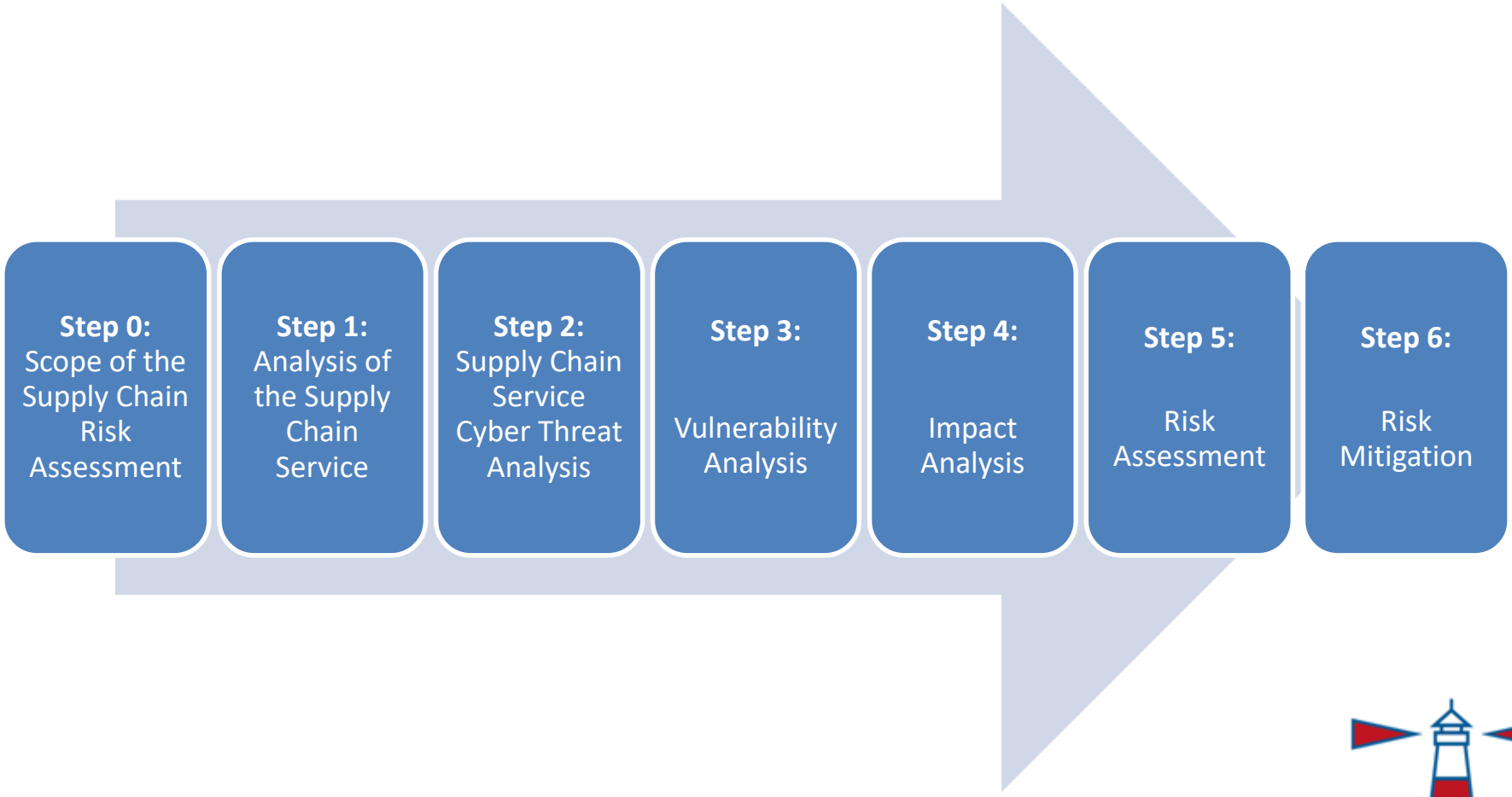
Step 5.2: Cumulative Risks

- **Scope:**
  - The Cumulative Risk refers to the risk of a specific threat occurring due to a vulnerability in a **specific target point**
  - Possible ways to **reach and exploit that vulnerability** are considered
    - Vulnerability levels of all paths leading to a specific asset
    - Impact levels of the target asset
    - Threat level
  - Cumulative Impact already contains the cumulative vulnerabilities
  - Resulting histogram is scaled using the threat level
- **Outcome:**
  - **Cumulative Risk Level** (CRL) for a specific threat on specific asset

Step 5.3: Propagated Risks

- **Scope:**
  - The Propagated Risk refers to the risk of a specific threat occurring due to a vulnerability in a **specific entry point**
  - Possible ways to **reach and exploit other vulnerabilities** are considered
    - Vulnerability levels of all paths starting from a specific asset
    - Impact levels of all assets on these paths
    - Threat level
  - Cumulative Impact already contains the cumulative vulnerabilities
  - Resulting histogram is scaled using the threat level
- **Outcome:**
  - **Propagated Risk Level** (PRL) for a specific threat on specific asset

Step 6:
Risk Mitigation



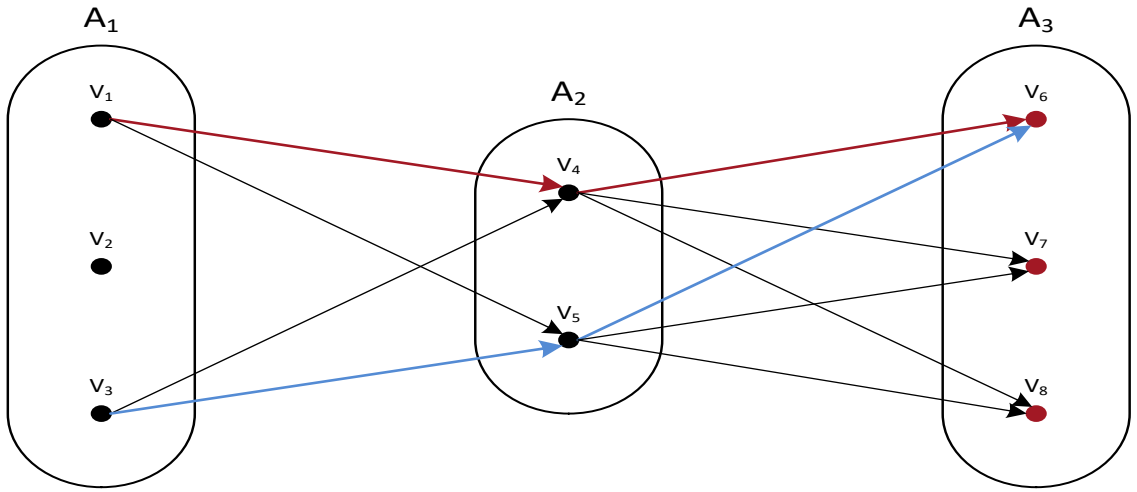
MITIGATE

- **Scope:**
  - Current risk levels might be **above** a required threshold
  - **Additional security controls** need to be chosen by the business partners and by the SCS (as a whole) to meet that thresholds
  - Selection of an **optimal set of security controls** using game theory
    - Based on potential attack strategies
    - Based on available security measures
    - Based on potential damage done by the attacker
- **Outcome:**
  - Optimal security strategy (set of security measures) to be applied by all business partners
  - Maximum risk level (damage) that can be caused by an attacker
- Action space of attacker
  - Each **path in the asset graph** describes a possible attack strategy
  - Characterized through the **exploited vulnerability** of the target asset
- The defender has a **list of possible actions** to perform
  - Integration of new security systems
  - Periodical update/upgrades of software
  - Periodical security awareness trainings

MITIGATE

- Action space of defender
  - **Countermeasures that reduce vulnerabilities** of the target node (e.g. patch the system)
  - Countermeasures that reduce vulnerabilities earlier on an attack path
- Payoff is **damage on target asset** (goal of attacker)
- Determine this damage for each possible attack path
  - Count number of paths yielding a specific loss
  - Summarize the result in a histogram (do not aggregate)
- Main goal for the defender is to **reduce vulnerabilities** in the attack graph that could be exploited
  - Reduce the number of attack paths (and attack strategies)
  - Lower the probability for a specific attack strategy to be successful
- Mathematical approach towards **minimization of the risk** as a decision support for security experts

Example:



MITIGATE

Benefits of the Methodology

- Provision of up-to-date threat and vulnerability information
  - Integration of information from vulnerability databases
  - Application of open data sources and social media
  - Dynamic adaption to currently changing threat level

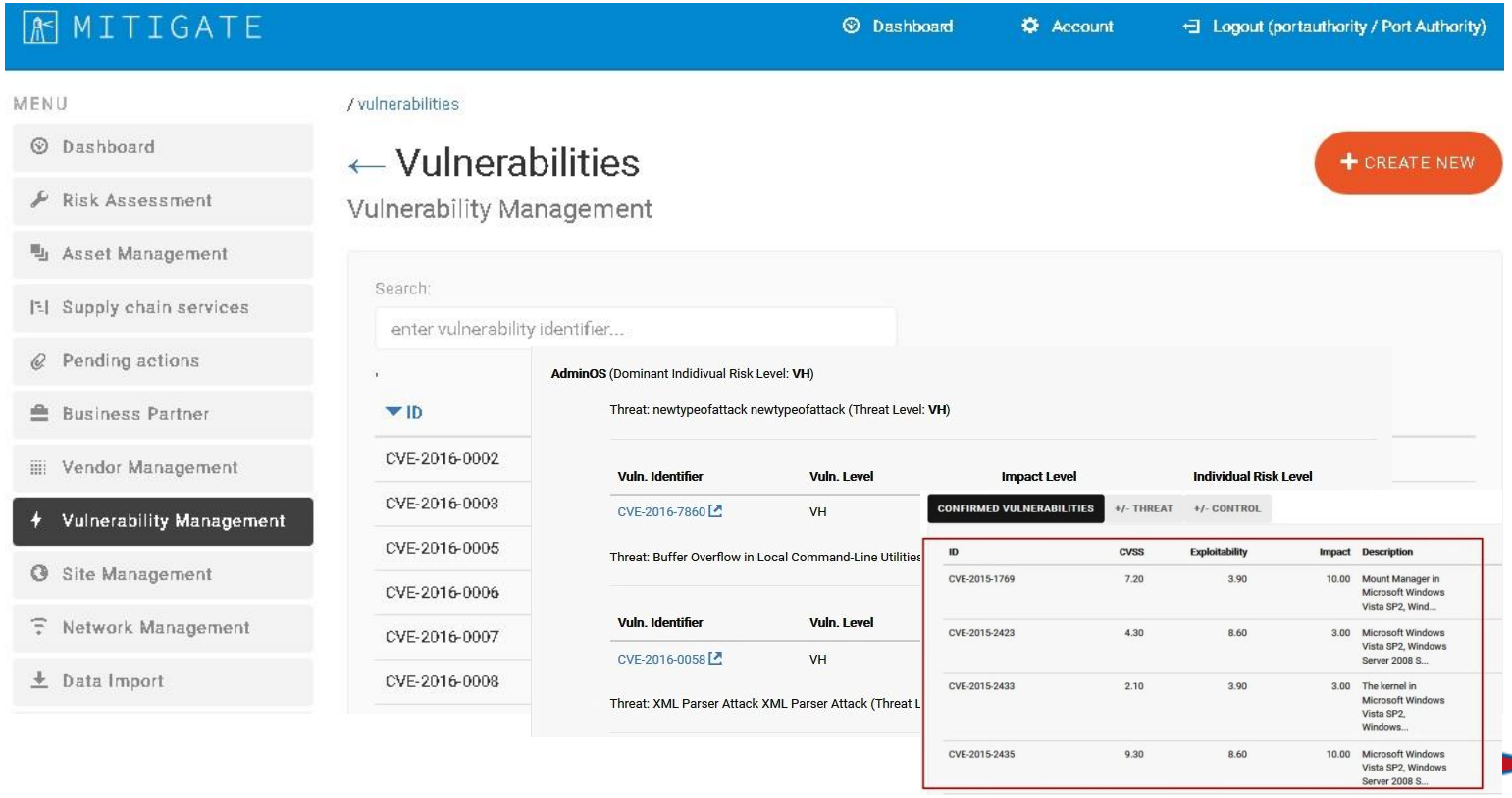
- Addressing the highly-interconnected port infrastructures' area
  - Identification of interdependencies of cyber security assets
  - Assessment of cascading effects on these assets

- Compliant with standards, EU and international regulations
  - ISO 31000, ISO 28001, ISO 27005, ISPS, etc.
  - Applicable to various transport-related sectors (not port-specific)

MITIGATE

Mitigate: Maritime SC Dynamic Risk Assessment System

http://mitigate.euprojects.net/



MITIGATE

MITIGATE Consortium

Instituto Portuario de Estudios y Cooperación de la Comunitat Valenciana

dbh Logistics IT AG

- Static Ports' RM methodology and tool (ISO27001, 27005, ISPS, CIIP)
- Dynamic evidence-driven Maritime SC RM environment (simulation, crowd-sourcing, open data) (ISO27001, 27005, ISPS, CIIP, ISO28000)

Protection of CIIs

- Static SC RM' methodology and tool (ISPS, CIIP, ISO28000)
- Situational Awareness platform

Thank You