Risk Analysis of Port Facility Security Based on the International Ship and Port Facility Security Code (ISPS CODE)

Mohammad Danil Arifin[1]

(Received: 08 June 2024 / Revised: 11 June 2024 /Accepted: 12 June 2024)

***Abstract*— The ISPS Code was created in response to the terrorism that occurred on September 11, 2001, in the United States. This prompted the IMO to review and draft the ISPS Code, which was then agreed to be included in the amendments to SOLAS 1974. The function of the ISPS Code is to minimize the occurrence of terrorism, piracy, cargo theft, stowaways, drug smuggling, money laundering, and other related issues. Due to the numerous incidents, particularly in Indonesia, this study reviews the security risk of the XYZ Port Facility based on the ISPS Code. These research objectives are to determine the security risk rating of the XYZ Port facility and to ascertain whether risk mitigation measures are necessary for the security facilities of XYZ Port. The method used in this research involves surveys and direct observations based on field data. The risk assessment in this study consists of three evaluations: threat, vulnerability, and impact assessment. Based on this research it can be identified that the security risk assessment of XYZ port facilities across 9 aspects revealed that 7 out of the 9 aspects have a risk rating of "Document (D)," while the remaining 2 aspects have a risk rating of "Consider (C)". Overall, it can be concluded that the security level of XYZ's port facilities is good.**

Keywords—*Risk Analysis, Port Facility Security, ISPS Code*

I. Introduction

The International Ship and Port Facility Security (ISPS) Code was established as a response to the heightened global awareness of security threats following the tragic events of September 11, 2001, in the United States. Recognizing the vulnerabilities within the maritime sector, the International Maritime Organization (IMO) undertook the task of formulating a comprehensive set of measures aimed at enhancing security for ships and port facilities worldwide. Consequently, the ISPS Code was developed and formally incorporated into the Safety of Life at Sea (SOLAS) Convention, 1974, through an amendment process [1].

The primary objective of the ISPS Code is to bolster maritime security by mitigating risks associated with terrorism, piracy, cargo theft, unauthorized access, drug smuggling, and money laundering, among other threats. The International Ship and Port Facility Security Code establishes a standardized, consistent framework through which ships and port facilities can assess and address their security needs, ensuring a high level of preparedness and response capability [2].

Given the increasing frequency and complexity of security incidents, particularly in regions like Southeast Asia, the implementation of the ISPS Code has become crucial. Indonesia, with its extensive maritime borders and numerous ports, has faced significant challenges in safeguarding its maritime infrastructure. This paper focuses on evaluating the security risk levels at the XYZ Port Facility in Indonesia, utilizing the ISPS Code as a benchmark.

This research aims to assess the current security measures at XYZ Port, determine the level of risk associated with potential security threats, and identify whether further risk mitigation strategies are required. By conducting detailed surveys and direct observations, the study evaluates the port facility's security through three core assessments: Threat Assessment, Vulnerability Assessment, and Impact Assessment. These assessments culminate in a comprehensive risk analysis, which informs the recommended mitigation actions based on a risk matrix encompassing three conditions: Document, Consider, and Mitigate.

A. Core Components of the ISPS Code

The ISPS Code is structured around a series of requirements and guidelines that must be adhered to by governments, port authorities, and shipping companies. These requirements include [3]:

- Security Assessments
  Conducting thorough security assessments to identify potential threats and vulnerabilities within port facilities and ships. The assessment process includes:
  - Identifying and evaluating potential threats, such as terrorism, piracy, and cargo theft.
  - Assessing vulnerabilities in physical infrastructure, access controls, and operational procedures.
  - Analyzing the potential impact of security incidents on port operations, economic activities, and human safety.
- Security Plans
  Developing and implementing comprehensive security plans tailored to the specific needs of each port facility and ship. These plans outline specific

[1] Mohammad Danil Arifin, Department of Marine Engineering, Darma Persada University, Jakarta, 13450, Indonesia. E-mail: danilarifin.mohammad@gmail.com

measures to address identified threats and vulnerabilities, including:

  - Access Control: Implementing strict access control measures to prevent unauthorized entry into port facilities. This includes the use of identification badges, surveillance cameras, and security checkpoints.
  - Perimeter Security: Enhancing perimeter security by installing fences, barriers, and surveillance systems to detect and deter intrusions.
  - Cargo Security: Implementing procedures to secure cargo, including inspections, sealing containers, and monitoring cargo movements.
  - Communication Protocols: Establishing communication protocols to ensure timely reporting and response to security incidents.

- Security Officers
  The ISPS Code mandates the appointment of qualified security officers to oversee security measures. These officers include:
  - Port Facility Security Officer (PFSO): Responsible for the development, implementation, and maintenance of the port facility security plan. The PFSO coordinates security activities, conducts security drills, and liaises with relevant authorities.
  - Ship Security Officer (SSO): Responsibility for carrying out and upholding the ship security plan. The SSO organizes routine security drills and makes sure the ship corresponds with security standards.
- Training and Drills
  Continuous training and drills are essential to ensure the effectiveness of security measures. Port facilities must provide comprehensive security training to all personnel, including:
  - Security Awareness Training: Educating personnel on security threats, procedures, and the importance of vigilance.
  - Drills and Exercises: Conducting regular security drills and exercises to test and improve response capabilities. These drills simulate various security scenarios, such as unauthorized access, cargo theft, and terrorist attacks.

B. *Benefits of the ISPS Code for Port Security*

The International Ship and Port Facility Security (ISPS) Code is a pivotal framework for enhancing maritime security and ensuring the safety and protection of ships and port facilities around the world [4]. Here are several reasons why the ISPS Code is of paramount importance:

- Response to Global Security Threats. Post-9/11 Security Concerns: The ISPS Code was established in the wake of the September 11, 2001, terrorist attacks, highlighting the need for robust security measures to protect global maritime operations from similar threats. The Code addresses a wide range of security concerns, including terrorism, piracy, and other criminal activities.
- Standardization of Security Measures. Global Consistency: By providing a standardized set of security requirements, the ISPS Code ensures that port facilities and ships worldwide adhere to consistent security practices. This standardization is crucial for maintaining a uniform level of security across international maritime operations, reducing vulnerabilities that could be exploited by criminals.
- Protection of Maritime Infrastructure. Safeguarding Assets: The ISPS Code helps protect critical maritime infrastructure, including ships, ports, and cargo, from security breaches. By implementing the Code’s measures, port authorities and shipping companies can minimize the risk of damage to infrastructure and loss of valuable goods.
- Enhancing Safety for Personnel and Passengers. Human Safety: Ensuring the safety of maritime personnel and passengers is a primary concern. The ISPS Code mandates the implementation of security measures that protect individuals from potential threats, creating a safer working and traveling environment.
- Mitigation of Economic Risks. Economic Stability: Maritime security incidents can have severe economic repercussions, including disruptions to trade, financial losses, and increased insurance costs. By reducing the likelihood of such incidents, the ISPS Code helps maintain economic stability and continuity in global trade.
- Facilitating International Trade. Trade Efficiency: Secure ports and ships are essential for the smooth operation of international trade. The ISPS Code enhances the reliability and efficiency of maritime logistics by mitigating security risks that could cause delays or disruptions in the supply chain.
- Compliance with International Regulations. Legal Obligations: Compliance with the ISPS Code is mandatory for SOLAS (Safety of Life at Sea) member states. Adhering to these regulations is essential for legal operations within the international maritime community, ensuring that ships and port facilities meet the required security standards.
- Enhancing Preparedness and Response. The ISPS Code requires regular training, drills, and audits, which enhance the preparedness and response capabilities of maritime personnel. This continuous improvement process ensures that ports and ships are ready to effectively handle security incidents, minimizing potential impacts.
- Building Trust and Reputation. Industry Credibility: Ports and shipping companies that comply with the ISPS Code demonstrate a commitment to high-security standards, which can enhance their reputation and credibility in the industry. This trust is crucial for maintaining strong business relationships and attracting clients and partners.
- Adapting to Evolving Threats. Dynamic Security Environment: The ISPS Code encourages a proactive approach to security, requiring ongoing assessments and updates to security measures. This adaptability is vital in responding to new and evolving threats in the maritime domain.

C. *Examples of Security Threats in Ports*

Ports are critical hubs in the global supply chain, making them attractive targets for various security threats. Below are examples of terrorism, piracy, cargo theft, unauthorized access, and drug smuggling in ports.

○ Terrorism

The examples of terrorism incidents that occurred at ports related to the implementation of the ISPS Code i.e.,

- Port of Colombo Bombing (1996) The Liberation Tigers of Tamil Eelam (LTTE) carried out a suicide bombing at the Port of Colombo in Sri Lanka, targeting a container ship [5]. The attack caused significant damage to the port infrastructure and disrupted port operations. This incident highlighted the vulnerability of port facilities to terrorist attacks and underscored the need for stringent security measures.
- Port of Ashdod Attack (2004) Palestinian militants infiltrated the Port of Ashdod in Israel, killing 10 people and injuring many others. The attackers smuggled themselves into the port using hidden compartments in cargo containers. This attack demonstrated how terrorists could exploit vulnerabilities in port security and highlighted the importance of comprehensive screening and access control measures.

○ Piracy

The examples of piracy incidents that occurred at ports related to the implementation of the ISPS Code i.e.,

- Somali Pirate Attacks (2008-2011) Ports along the Somali coast and in the Gulf of Aden were heavily impacted by piracy during this period [6]. Pirates targeted ships entering and leaving these ports, hijacking vessels, and holding crew members for ransom. The presence of pirates in these waters led to increased security costs and significant disruptions in maritime trade routes.
- Port of Lagos, Nigeria (2019) Pirates attacked a container ship near the Port of Lagos, kidnapping several crew members [7]. The incident underscored the ongoing threat of piracy in West African waters and the need for improved maritime security measures in and around port facilities.

○ Cargo Theft

The examples of cargo theft incidents that occurred at ports related to the implementation of the ISPS Code i.e.,

- Port of Los Angeles Cargo Theft Ring (2013) A sophisticated cargo theft ring operated at the Port of Los Angeles, stealing millions of dollars worth of electronics and other high-value goods [8]. The thieves used insider information and exploited security gaps to access cargo containers. This case highlighted the need for robust security protocols and employee vetting processes to prevent insider threats.
- Rotterdam Port Theft (2017) Thieves used a combination of cyber-attacks and physical intrusion to steal containers filled with valuable cargo at the Port of Rotterdam [9]. They hacked into the port's computer systems to obtain information about container locations and then physically accessed the containers to steal the goods. This incident demonstrated the intersection of cyber and physical security threats.

4. Unauthorized Access

The examples of unauthorized access incidents that occurred at ports related to the implementation of the ISPS Code i.e.,

- Port of New York and New Jersey Stowaways (2000) Several stowaways were discovered hidden in cargo containers at the Port of New York and New Jersey [10]. The individuals had entered the port area undetected and boarded ships without authorization. This incident highlighted vulnerabilities in access control and the need for thorough inspections and monitoring of port premises.
- Port of Felixstowe Intrusion (2018) A group of environmental activists gained unauthorized access to the Port of Felixstowe in the UK to protest the shipment of nuclear waste [11]. They managed to breach port security and stage a demonstration on the docks. This incident emphasized the importance of securing perimeters and having robust response plans for unauthorized access events.

5. Drug Smuggling

The examples of drug smuggling incidents that occurred at ports related to the implementation of the ISPS Code i.e.,

- Port of Antwerp Cocaine Seizure Belgian authorities seized a record 11.5 tonnes of cocaine hidden in containers at Port Antwerp [11]. The drugs were concealed among legitimate cargo and were part of a large-scale smuggling operation linked to South American drug cartels. This case illustrated the use of commercial shipping routes by drug traffickers and the need for advanced screening and intelligence-sharing mechanisms.
- Port of Miami Drug Bust (2019) U.S. Customs and Border Protection (CBP) agents intercepted a shipment containing over 1,000 pounds of cocaine at the Port of Miami [12]. The drugs were concealed in cargo containers and were discovered during routine inspections. This bust highlighted the effectiveness of routine inspections and the importance of vigilance in combating drug smuggling.

These examples illustrate the diverse and complex security threats faced by port facilities worldwide. Effective implementation of the ISPS Code, combined with advanced technology, rigorous training, and international cooperation, is essential to address these challenges and safeguard global maritime operations.

D. Theoretical Framework for Risk Analysis

Risk analysis in the context of port facility security involves identifying potential threats, assessing vulnerabilities, and evaluating the impact of security incidents. This approach aligns with the risk management principles outlined in international standards such as ISO 31000 and the ISPS Code itself. The ISPS Code emphasizes the need for continuous assessment and enhancement of security measures to adapt to evolving threats [13].

E. Components of Risk Analysis

The component of risk analysis consists of three main components i.e.,

- Threat Assessment
  This component involves identifying and analyzing potential threats to port security. It encompasses both external threats (e.g., terrorism, piracy) and internal threats (e.g., employee theft, sabotage). The threat assessment is critical in understanding the nature and likelihood of security incidents based on Notteboom & Vernimmen [14] [15].
- Vulnerability Assessment
  Vulnerability assessment examines the weaknesses within a port facility's security infrastructure that could be exploited by threats. This includes physical vulnerabilities (e.g., inadequate fencing, surveillance) and procedural vulnerabilities (e.g., lack of proper access controls, and inadequate security protocols) [16].
- Impact Assessment
  Impact assessment evaluates the potential consequences of security incidents, considering both direct and indirect effects. Direct impacts include damage to infrastructure and loss of cargo, while indirect impacts cover economic losses, reputational damage, and disruptions to port operations (Lam & Su, 2015).
- Risk Assessment
  Risk assessment is a critical process in port facility security, involving the identification, evaluation, and prioritization of potential risks. This process helps in developing effective strategies to mitigate security threats and ensure the safety and efficiency of port operations.

II. METHOD

The risk assessment method for port facility security at XYZ port is carried out based on several stages, namely threat assessment (T), vulnerability assessment (V), and impact assessment (I). Detailed explanations regarding these stages are as follows:

A. Threat Assessment

Threats are defined as potential sources of harm, danger, or adverse effects that can compromise the security and functionality of port facilities and operations. The threat assessment method for XYZ port facilities is identified based on the likelihood of threat sources. The possible sources of threats include:

- Destruction or damage to the port or ships using explosives, arson, sabotage, vandalism, and other dangerous actions.
- Hijacking or seizure of ships or people in the port.
- Damaging the ship's cargo, equipment, systems, and goods.
- Violation or unauthorized access or use, including the presence of stowaways.
- Smuggling of weapons or devices.
- Using illegal ships to transport individuals intending to cause security incidents and their equipment.
- The use of the ship itself as a weapon to cause damage or destruction.
- Blocking the entrance to the port and approaching.
- Nuclear, biological, and chemical attacks.

The probability of an incident occurring for each threat scenario and potential event at each security level should be assessed on the following scale:

1.	High level	= 3
2.	Moderate level	= 2
3.	Low level	= 1

B. Vulnerability Assessment

Vulnerability is defined as the susceptibility of a system, asset, or organization to harm or exploitation due to weaknesses or gaps in security measures, controls, or procedures. It refers to the extent to which an entity can be adversely affected by threats, considering its ability to prevent, withstand, or respond to adverse conditions. The probability of an incident occurring for each vulnerability scenario and potential event at each security level should be assessed on the following scale:

- 4 Score
  There are either no security measures in place or those that are ineffective (such as unfettered access, lack of monitoring, lack of trained personnel, and easily damaged targets), or it is not practical to provide security measures because of resource limitations, target location, or cost of security measures exceeding target value.
- 3 Score
  Only temporary protective measures are allowed where there are insufficient security measures in place (such as unidentified restricted areas, insufficient access control processes, irregular monitoring, no formal security training program, and targets that are susceptible to certain forms of harm).
- 2 Score
  Only partial protection is possible due to insufficient resources or inadequate security measures (such as designated restricted zones with access controls, a structured security training program, sufficient monitoring, threat awareness, and targets that are difficult to destroy).
- 1 Score
  Completely successful security measures (such as all of the previously mentioned "2"); additionally, they should be able to quickly scale to higher levels of protection when necessary; they should also be hard to breach or have enough redundant service to prevent disruption if some functions are compromised; and they shouldn't gain from the addition of extra security measures.

C. Impact Assessment

Impact is defined as the potential consequences or effects of an incident or threat on an organization, system, or asset. It refers to the extent of harm, damage, or disruption that can result from an adverse event. The impact is assessed to understand the severity and scope of potential losses or damages, which can guide the prioritization of risk mitigation efforts. The impact assessment method involves assessing the consequences of each unexpected event when it occurs as it should not have. Certain "impacts" and priorities for specific ports may be overridden by the designated authority to meet the requirements of the national security profile. The probability of an incident occurring for each impact scenario and potential event at each security level should be assessed on the following scale:

- 5 Score
  Incredibly harmful to security and safety (may cause fatalities, severe injuries, and/or provide a serious risk to the public's health and safety).
- 4 Score
  Detrimental to the reputation of the country and/or public safety (may result in serious environmental harm and/or local public health and safety risks).
- 3 Score
  Harmful to the environment and/or the port's economic viability (may result in a protracted suspension of port operations, large financial losses, and harm to the country's reputation).
- 2 Score
  Detrimental to cargo security, utilities, assets, and infrastructure (expected to cause little damage to companies, individual assets, or infrastructure).
- 1 Score
  Detrimental to customers/trust of the port community.

D. Risk Assessment

The risk score is a numerical representation of the severity of a risk, calculated by combining the threat of the risk occurring with the vulnerability and the potential impact it could have. This score helps in prioritizing risks and determining the appropriate response measures. The threat and risk analysis matrix (TRAM) method is obtained with the following formulas [17]:

$$\textit{Risk Score} = T \times V \times I \qquad (1)$$

The detailed risk score range and the priority action assessment in this study are divided into three ranges as follows:

- Risk score 1-20 = Priority action is Document (D)
- Risk score 21-40 = Priority action is Considered (C)
- Risk score 41-60 = Priority action is Mitigate (M)

Based on the above risk scores, they can be explained and interpreted as follows:

- Mitigate (M) or reduce implies that developing mitigating solutions is necessary to lower the risk targeting/combination of scenarios. A security plan should include evaluated scenarios, evaluation results, and mitigation actions.
- Consider (C) implies that mitigation methods should be designed on a case-by-case basis, considering the target or mix of circumstances.
- Document (D) indicates that the target or collection of scenarios just needs to be documented and does not presently require mitigation techniques.

The flowchart of this study is illustrated in Figure 1.

III. Results and Discussion

A. Threat Assessment Result

The threat assessment of the facilities at XYZ port is identified based on the observational data that has been collected. The threat score can be described as shown in

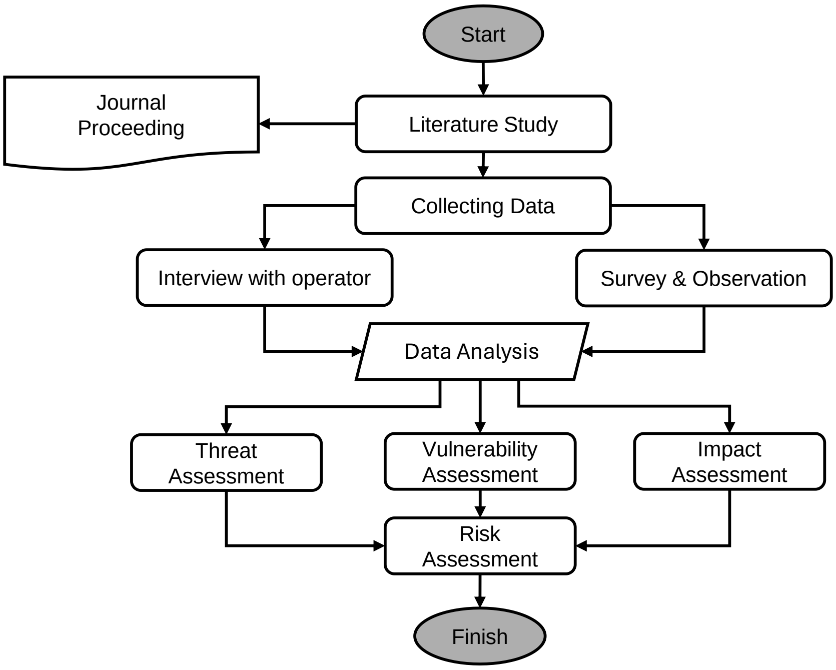

Figure 1. Flowchart

Table 1.

B. Vulnerability Assessment Result

The next step after conducting a threat assessment at XYZ port is to conduct a vulnerability assessment. In this research, the security vulnerability assessment results of port XYZ port facilities are described as shown in Table 2 below.

TABLE 1.
THREAT ASSESSMENT

No	Potential Threats	Score	Description
1	Destruction or damage to the port or ships using explosives, arson, sabotage, vandalism, and other dangerous actions.	3	The absence of barriers or limited access in restricted areas such as the Generator Set (Genset) area and Reservoir Tank area raises concerns about potential sabotage or damage to these areas
2	Hijacking or seizure of ships or people on the port.	1	Satisfactory security measures, adequate monitoring and threat awareness, along with restricted entry to the designated location
3	Damaging the ship's cargo, equipment, systems, and goods.	1	Satisfactory security measures, adequate monitoring and threat awareness, along with restricted entry to the designated location
4	Unlawful usage or access, including when stowaways are present	3	At the checkpoint, procedures are not consistently applied to all visitors, raising concerns about potential sabotage or stowaways.
5	Smuggling of weapons or devices.	1	Satisfactory security measures, adequate monitoring and threat awareness, along with restricted entry to the designated location
6	Using illegal ships to transport individuals with the intent to damage their equipment and trigger security problems.	2	Minimal security measures/resource constraints, and the target is vulnerable to certain types of security threats.
7	The act of causing harm or destruction by using the ship itself as a weapon.	1	Satisfactory security measures, adequate monitoring, and threat awareness, along with restricted entry to the designated location.
8	Blocking the entrance to the port and approaching.	1	Satisfactory security measures, adequate monitoring, and threat awareness, along with restricted entry to the designated location.
9	Nuclear, biological, and chemical attacks.	1	Satisfactory security measures, adequate monitoring, and threat awareness, along with restricted entry to the designated location.

TABLE 2.
VULNERABILITY ASSESSMENT

No	Potential Threats	Score	Description
1	Destruction or damage to the port or ships using explosives, arson, sabotage, vandalism, and other dangerous actions.	2	Satisfactory security measure, and the target is vulnerable to certain types of damage, such as in the genset area and the water reservoir tank area are no barriers or limited access to those areas.
2	Hijacking or seizure of ships or people on the port.	2	The main office is located far from the waterfront area, resulting in low vulnerability.
3	Damaging the ship's cargo, equipment, systems, and goods.	2	Satisfactory security measure, and the target is vulnerable to certain types of damage
4	Unlawful usage or access, including when stowaways are present	3	Minimal security measures, and the target is vulnerable to certain types of damage
5	Smuggling of weapons or devices.	1	There are many workers, and tight security is enforced from the main entrance.
6	Using illegal ships to transport individuals with the intent to damage their equipment and trigger security problems.	2	Satisfactory security measure, and the target is vulnerable to certain types of damage
7	The act of causing harm or destruction by using the ship itself as a weapon.	1	Satisfactory security measures, adequate monitoring and threat awareness, along with restricted entry to the designated location
8	Blocking the entrance to the port and approaching.	1	Satisfactory security measures, adequate monitoring and threat awareness, along with restricted entry to the designated location
9	Nuclear, biological, and chemical attacks.	1	Satisfactory security measures, adequate monitoring and threat awareness, along with restricted entry to the designated location

C. Impact Assessment Result

The next step after conducting threat and vulnerability assessments at XYZ port is to perform an impact assessment to identify potential consequences resulting from the threats and vulnerabilities at XYZ port. The results of the impact assessment due to vulnerabilities and threats at XYZ port are shown in Table 3 below:

In this impact assessment, many factors are considered, including the impact on customers, economic impact, environmental impact, social public impact, and finally, the impact affecting worker conditions such as injuries, fatalities, and so on. The final step, after conducting threat, vulnerability, and impact assessments at XYZ

TABLE 3.
IMPACT ASSESSMENT

No	Potential Threats	Customer	Economic	Environment	Social Public	Life/ Injury	Impact Score
1	Destruction or damage to the port or ships using explosives, arson, sabotage, vandalism, and other dangerous actions.	√	√	√	√	√	**5**
2	Hijacking or seizure of ships or people on the port.	√	√	-	-	√	**3**
3	Damaging the ship's cargo, equipment, systems, and goods.	√	√	√	-	-	**3**
4	Unlawful usage or access, including when stowaways are present	√	√	-	√	√	**4**
5	Smuggling of weapons or devices.	√	√	-	√	√	**4**
6	Using illegal ships to transport individuals with the intent to damage their equipment and trigger security problems.	√	√	-	-	√	**3**
7	The act of causing harm or destruction by using the ship itself as a weapon.	√	√	√	-	√	**5**
8	Blocking the entrance to the port and approaching.	√	√	√	√	√	**5**
9	Nuclear, biological, and chemical attacks.	√	√	√	√	√	**5**

TABLE 4.
RISK ASSESSMENT

No	Potential Threats	Threats (T)	Vulnerability (V)	Impact (I)	Risk Score (Tx V X I)	Priority Act
A	B	C	D	E	F	G
1	Destruction or damage to the port or ships using explosives, arson, sabotage, vandalism, and other dangerous actions.	3	2	5	**30**	**C**
2	Hijacking or seizure of ships or people on the port.	2	1	3	**6**	**D**
3	Damaging the ship's cargo, equipment, systems, and goods.	1	2	3	**6**	**D**
4	Unlawful usage or access, including when stowaways are present	3	3	4	**36**	**C**
5	Smuggling of weapons or devices.	1	1	4	**4**	**D**
6	Using illegal ships to transport individuals with the intent to damage their equipment and trigger security problems.	2	2	3	**12**	**D**
7	The act of causing harm or destruction by using the ship itself as a weapon..	1	1	4	**4**	**D**
8	Blocking the entrance to the port and approaching.	1	1	5	**5**	**D**
9	Nuclear, biological, and chemical attacks.	1	1	5	**5**	**D**

port is to perform a risk assessment.

Based on the risk assessment result as shown in Table 4, it was found that out of the nine potential threats, seven have a risk score below 20, meaning that the target or collection of scenarios just needs to be documented and does not presently require mitigation techniques. The remaining two potential threats have risk scores between 20 and 40, indicating that mitigation methods should be designed on a case-by-case basis, considering the target or mix of circumstances

Regarding the two threats with a C rating, the following preventive strategies are necessary:

- Threat No. 1
  1. Frequency of Patrols: Conduct patrols at random intervals. Security officers must maintain adequate communication with the guard post to provide constant updates and send situation reports as quickly as possible. Reporting procedures should be established in the communication protocols to ensure consistent reporting.
  2. Coordination of Water Patrols: Maintain continuous communication with the port authorities and related organizations to ensure situation reports are always updated.
- Threat No. 4
  1. Education: Educate all security personnel and port employees to better understand and implement ISPS Code procedures for all visitors. Smuggling can be reduced by stationing additional police officers at the facility.
  2. Security Equipment: Equip the facility with hardware such as CCTV security systems, metal detectors, and X-ray machines to detect and identify smuggled weapons or substances.

IV. Conclusion

Based on the above analysis it can be concluded that the security risk assessment of XYZ port facilities across 9 aspects revealed that 7 out of the 9 aspects have a risk rating of "Document (D)," while the remaining 2 aspects have a risk rating of "Consider (C)," specifically scenario 1 and scenario 4. For the results rated as “D,” no further mitigation is required, and they are only documented. Meanwhile, for the results rated as “C,” risk mitigation is necessary. Overall, it can be concluded that the security level of XYZ's port facilities is good.

References

[1] IMO. (2002). International Ship and Port Facility Security (ISPS) Code. International Maritime Organization. IMO Publishing.

[2] George G. Mason. (2005). The ISPS Code: A Practical Guide. Journal of Maritime Policy & Management. Vol. 32 No 3 Pp. 297-310.

[3] John F. Frittelli. (2004). Maritime Security and the ISPS Code: Implementation Issues and Perspectives. Journal of Transportation Law, Logistics and Policy. Vol. 71. No. 2 Pp. 165-182.

[4] David Attard. (2004). The Implementation of the ISPS Code in the Light of the SOLAS Convention. International Journal of Marine and Coastal Law. Vol. 19 No. 4 Pp. 493-506.

[5] International Crisis Group. (2019). After Sri Lanka’s Easter Bombings: Reducing Risks of Future Violence. Pp. 1-46.

[6] Santiago Iglesias-Baniela. (2010). Piracy at Sea: Somalia an Area of Great Concern. Journal of Navigation 63(02):191 – 206. DOI: 10.1017/S0373463309990439

[7] Piracy monthly report for March 2019 Acts of piracy and armed robbery allegedly committed against ships reported by Member States or international organizations in consultative status. Retrieved from https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Piracy%20monthly%20report%20Mar%202019.pdf

[8] D. Burges. (2013). Cargo Theft, Loss Prevention, and Supply Chain Security. Science Direct. https://doi.org/10.1016/C2011-0-06850-3

[9] Frans A. J. Van Den Bosch. (2011). The strategic value of the Port of Rotterdam for the international competitiveness of the Netherlands: A first exploration. Research Report for the Port of Rotterdam Authority. RSM Erasmus University / INSCOPE ISBN: 978-90-817220-2-5

[10] Kusi, Bernard. (2015). PORT SECURITY-Threats and Vulnerabilities. Laurea University of Applied Sciences.

[11] Environment Report. (2020). Retrieved from https://www.portoffelixstowe.co.uk/files/7016/1133/0477/Environmental_Report_2020.pdf

[12] EU Drug Markets Impact of COVID-19. 2020. ISBN 978-92-9497-493-8 doi:10.2810/19284

[13] Williams, J. (2004). The Impact of the ISPS Code on the Management of Port Security. Maritime Economics & Logistics, 6(4), 354-368.

[14] Notteboom, T. E., & Vernimmen, B. (2009). The effect of high fuel costs on liner service configuration in container shipping. Journal of Transport Geography, 17(5), 325-337.

[15] Notteboom, T. E. (2010). From Multi-Porting to a Hub Port: The Port of Rotterdam. Research in Transportation Economics, 27(1), 35-52.

[16] Mitchell, J. (2006). What role do security measures play in the transport of dangerous goods? Journal of Transportation Security, 1(1), 23-34.

[17] Chunlin Liu, Chong-Kuan Tan, and Yea-Saen Fang. (2012). The Security Risk Assessment Methodology. Procedia Engineering 43:600-609. DOI: 10.1016/j.proeng.2012.08.106