A Delphi Study to Identify Important Factors for Determining the Level of Adherence to ISPS Code Implementation

Aminuddin Md Arof [1], Ahmad Farhan Awis Khadzi [2]

Universiti Kuala Lumpur, Malaysian Institute of Marine Engineering Technology
Bandar Teknologi Maritim, Pantai Remis Road, 32100 Lumut Malaysia

[1]1aminuddin@unikl.edu.my

[2]farhan_awis@yahoo.com

***Abstract*— The International Ship and Port Facility Security (ISPS) Code was adopted in 2004 as a preventive measure to enhance maritime security in ports and on-board ships. The regulation was made compulsory under Chapter XI-2 of the International Safety of Life at Sea (SOLAS) Convention by International Maritime Organisation (IMO). Since the implementation of the ISPS Code is rather new as compared to other IMO regulations, it is deemed necessary to find out whether employees who work in ports are fully aware and adhere to the requirements of the Code. This research is therefore meant to identify the important determinants to ensure effective implementation of ISPS Code and investigate the level of adherence to ISPS Code implementation amongst Vale Malaysia Minerals (VMM) employees. In this research, the primary data is collected using the Delphi technique. This study concludes that other than those addressed in the literature, two more important factors can be used to determine the implementation of ISPS code and that VMM has been assessed as satisfactorily adhered to the general ISPS Code requirements.**

***Keywords*—** *Delphi, International Maritime Organisation (IMO), ISPS Code, SOLAS Convention, Qualitative Content Analysis*

1. Background

More than 80 percent of international cargoes are transported by ships and handled through various types of seaports. Due to the continuous increase in the cargo volume, efficient mobility is needed to ensure that ports and terminals are able to achieve optimum productivity. Among others, innovation and technology such as the security and safety system contribute to the efficient activities in ports and terminals. The wellbeing of the security frameworks is undoubtedly vital to port and terminal operators, partners and clients in light of the fact that the delivery exercises involve international exchanges by nature. Port security framework incorporates several important variables such as port facility security; port facility security plan (FPSP); port facility security officer (PFSO); port facility assessment (PFA); as well as training, drill and exercise on port facility security [1]. The development in port security management is imperative to port operations in order to make sure that the activities around the port and on-board transiting ships are safeguarded from any untoward incident. This is necessary since port is the primary gateway of import and export activities that contribute to economic growth and development of a country.

The ISPS Code was enforced on 1st July 2004 following the attack on the French tanker “Limburg” off the coast of Yemen in October 2002, the ramming of United States Ship (USS) Cole by a boat laden with explosives in 2000 and the infamous September 11th, 2001 incident. This led to the development of ISPS Code that was adopted on 12 December 2002 in the amendments to the International Convention for the Safety of Life at Sea (SOLAS) 1974, Chapter XI-2. To date, 161 governments worldwide have ratified and implemented this convention [2]. The Code was introduced as a preventive measure against any security incidents in international trade affecting ships and port facilities [1]. Maritime security can be enhanced through the implementation of this Code by the outlining of minimum security standards for ships and port facilities. Besides that, it forms a global framework in collecting and sharing information effectively in order to detect security threats such as terrorism and to take necessary preventive measures [3]. The Code applies to all international voyage passenger ships,

IJSCM, ISSN: 2050-7399 (Online), 2051-3771 (Print)

to all other international voyage cargo ships with more than 500 gross tonnage (GT), mobile offshore drilling units and also to all port facilities serving ships engaged in international voyages [1], [4]. ISPS Code provides a set of measures for international security where responsibilities of government authority, port authority, shipping companies and seafarers are stipulated. There are two parts in the Code; Part A and Part B. Part A, which involves general requirements is made compulsory, while Part B stipulates some guidance or suggestive actions that can be taken in preparing ship and port security plans as well as to carry out other responsibilities stated in Part A. Even though Part B is only meant as a guidance rather than a mandatory regulation, failing to adhere to its provisions might contribute to a failure to exercise the regulation in general [4].

2. Aim

This research is meant to assess the level of adherence on the general requirements of the ISPS Code among employees of Vale Malaysia Minerals or VMM. VMM is a subsidiary of a Brazilian based multinational mining company and operates as an iron ore regional distribution centre. Teluk Rubiah Maritime Terminal (TRMT), which is dry bulk port, is privately owned by VMM and is strategically located in Perak, on the west coast of Peninsular Malaysia. It faces the Straits of Malacca, one of the busiest shipping channels in the world. The terminal that services foreign-going vessels is able to handle iron ore up to 30 million tons a year with the help of its import and export wharf facilities [5]. Therefore, it is believed that VMM is a suitable organization for carrying out this research. The research is guided by the following objectives:

i. To identify the important variables that signify the implementation of ISPS Code.
ii. To determine the level of adherence to the general requirements of ISPS Code among employees of VMM.

3. Problem Statement

TRMT was fully operational in 2014 and was certified to be in compliance with ISPS Code by the Marine Department of Malaysia [6]. Although ISPS Code has been implemented since 2004, there are several issues concerning to the security and safety of port facilities. For instance, Burmester (2004) argues that ISPS Code does not provide uniform global standards and clear guidelines, which might be partially due to different governmental interpretations of ISPS Code requirements [7]. On the other hand, Jeong (2013) discovered that there have been a number of challenges such as confusion out of the difference between the ISPS Code Act implemented at national level with the ISPS Code that is set out by IMO, lack of focus on ship/port interface, low level of enforcement by contracting government as well as poor response to incidents [8]. Similarly, Ng (2009) describes that stakeholders often feel discontent with the imposition of further rules based on security issues [9]. Since the ISPS Code is rather new as compared to other regulations made by IMO, the challenges in its implementation as highlighted in earlier literature may be unavoidable but could be minimised. As research on ISPS code in Malaysia is still lacking, it is deemed necessary to find out whether employees who work at seaports and terminals are fully aware with the requirements of the Code. Therefore, this research analyses the level of adherence to the ISPS requirements and identify the important variables that employees think are important to signify the effective implementation of the ISPS Code.

4. Maritime Security Threats

Maritime security is one of the jargons of international relations. It can be defined as “freedom from the risk of serious incursions against a nation’s sovereignty launched from the maritime domain, and from the risk of successful attack against a nation’s maritime interests” [10]. Maritime transport has been exposed to different types of security threats such as piracy, terrorist attacks, smuggling and human trafficking [11]. Since ocean is a huge space, it poses high vulnerability to terrorist attacks and other unlawful activities. The September 11 incident in 2001 was a wake-up call to many countries especially the United States of America as many analysts believe that similar kind of incident may also occur through the sea. Since shipping industry plays such a vast and vital role in international trade and commerce, ships as well as ports are highly exposed to the threat of terrorism. Several attacks at sea such as al-Qaeda’s attacks on USS Cole, while berthing at

Aden harbour in 2000 and the attack on oil tanker, MV Limburg in 2002 provide the evidence of what terrorists are capable of doing at sea. Besides that, the rise in the number of piracy incidents especially off the coast of Somalia that caused danger to international trade has also brought worldwide consciousness on another aspect of maritime security that requires serious concern and legal actions [12].

For this study, the focus will be laid on the requirements of port facilities. IMO (2017) explains that under ISPS Code, requirements for port facilities that include the requirements for governments to carry out port facility security assessments; and for port facility security plans to be developed, implemented and reviewed, are covered [13]. As written in Part A of the Code, port security framework incorporates several important elements such as port facility security, port facility security plan (FPSP), port facility security officer (PFSO), port facility assessment (PFA), as well as training, drills and exercise on port facility security [1]. These five major elements of Part A are some of the criteria used in assessing the objectives of this study. A port facility is obliged to carry out the security levels set by the Contracting Government. Security measures and procedures shall be put into place at the port facility in such a way as to reduce interference with, or delay to, passengers, ship, ship's personnel and visitors, goods and services [1]. The operation of security requirements is based on variation depending on the potential risk to security. Current situation of that country and the condition of its regional coastal area in relation to maritime security threat will guide the Designated Authority to set the security level required at each of its port facilities [4]. There are three maritime security levels introduced under the ISPS Code. The security levels are distinguished based on the degree of risk; low risk (Level 1), medium risk (Level 2), and high risk (Level 3). Level 1, which is also called as normal level, requires minimum protective security to be maintained at all time. Level 2, which is called as heightened risk level, requires appropriate additional measures to be implemented when the risk is intensified. Whereas, Level 3 which is also known as imminent danger level, requires further and specific protective measures to be maintained at all time when the security incidents are threatening and probable [1].

Secondly, PFSP should be drawn in compliance with ISPS Code. In order PFSP to be drawn, Port Facility Security Assessment (PFSA) should be carried out and need to be reviewed from time to time [3]. PFSA plays an important part in the process of development and the updating of PFSP. It is the responsibility of the Contracting Government to carry out PFSA and approve PFSP for the port facility placed within their territory [1]. PFSA is also important in deciding which port facilities are obligatory to assign PFSO, who is a person designated for each port facility and responsible for the preparation, maintenance and implementation of the PFSP. He is also responsible in giving assistance, when requested, to ship security officers (SSO) in confirming the identity of persons seeking to board the ship [1]. The PFSO is also required to make certain that the PFSP provisions are executed and checked on the ongoing effectiveness and applicability of the approved plan, including assigning independent internal audits of the application of the plan [4]. Under part B of the Code, the PFSO and personnel involved with port facility security shall have knowledge and have received training, according to the guidance given. They shall understand their duties and responsibilities as described in the PFSP and are also capable to perform their assigned duties accordingly. Drills shall be carried out regularly based on relevant circumstances such as types of operation of the port facility, the type of ship the port facility is serving and other pertinent factors, in order to ensure that the PFSP is implemented effectively. It is the duty of the PFSO to ensure the effective coordination and implementation of the PFSP by taking part in exercises at appropriate intervals as outlined in part B of this Code.

5. Implementation of ISPS Code in Malaysia

In Malaysia, the onus of executing the ISPS Code, under the term of Contracting Government lies with the Ministry of Transport (MOT). They are responsible, among others, in setting maritime security levels and appointing an authority to be responsible in ensuring the implementation of the provisions stated in the ISPS Code. Razali and Dahalan (2012) mention that, the National Security Council (NSC) in consultation with the Malaysian Marine Department (MARDEP), shall be responsible in deciding the maritime security levels. MARDEP is the designated authority responsible in implementing the ISPS Code [4]. They are responsible to approve the PFSA and PFSP and their subsequent amendments, to determine the port facilities that required to appoint PFSO, and also to exercise control and monitoring compliance measures under the Code. Yilmazel and Asyali (2005) state that in accomplishing an efficient and effective management of security in maritime transport, controlling plays an important role [14]. This is because controlling provides the process of monitoring activities to ensure that they are being accomplished as what have been planned and is also used as a way to fix any significant divergence. Meanwhile, the PFSO is responsible to develop, maintain, implement and exercise the PFSP. In addition, his responsibilities extend to undertaking security inspections of the port facility and ensuring the carrying on of appropriate security measures [4].

6. Methodology

For this study, questionnaire is the main instrument used which contains open-ended and closed-ended questions and are given to respondents in a minimum of two rounds under the Delphi technique. The Delphi technique is a method initially developed by RAND (Research and Development) Corporation in the United States of America in the 1950s. However, it was only introduced by Dalkey and Helmer to the public in 1963. According to Grisham (2009), it is used to assess variables that are vague by drawing on the knowledge and abilities of a selected group of experts, via a form of anonymous and repetitive consultations [15]. Delphi technique involves knowledgeable and expert respondents who are individually responding to questions through a repeated questionnaire and submitting the result direct to the researcher who would later process the answers looking for central tendencies and their rationales [15], [16]. It means that the respondents in a Delphi survey are those who are from a panel of selected experts responding to a series of questionnaire delivered by using multiple repetition process in order to gather data. For this study, the Delphi survey has been conducted in two rounds. Generally, they are four key features that need to be adhered in the Delphi process which are; (1) Anonymity of the respondents; (2) Iteration that allows the respondents to refine their views; (3) Controlled feedback; and (4) Statistical data for aggregation of group response. These key features are important as they allow for quantitative analysis and interpretation of data. The Delphi questionnaire is used as the main method in obtaining data for this study. For this study, the questionnaire survey was conducted in two rounds under a modified-Delphi technique. The first round involves open-ended and closed-ended questions, while the second round involves closed-ended questions [17], [18]. (Rowe & Wright, 1999) (Arof, Md Hanafiah & Ooi, 2016). A seven-point Likert scale has been chosen in the closed-ended part of this questionnaire survey. The reason to adopt this seven-point Likert scale is mainly because experts have defined that the important determining factors using a Likert scale between 1 (least important) to 7 (most important) help to distinguish between important determinants and very important determinants in research. Furthermore, Finstad (2010) mentions that a seven-point scale could be said as a good balance between having enough point of discrimination and without having too many options in the response [19].

6.1 Data Analysis

Data analysis is a process of systematically applying statistical and factual technique to describe, illustrate and evaluate data. This study analyses the primary data obtained from the questionnaire survey which consists of both open-ended and closed-ended questions. As previously stated, the questionnaire survey is conducted in two rounds. It started with open-ended questions and subsequently followed with closed-ended questions. The open-ended questions were done in the first place as it allowed each of the respondents to freely express their thoughts and knowledge while answering the given questions. The data gathered was analysed by using qualitative content analysis in order to identify the important variables that signify the implementation of ISPS Code. The information received in the first-round lead to the construction of closed-ended questions, which were subsequently given back to the same respondents. The second round of this questionnaire survey helped the respondents to re-evaluate their previous answers. This has enabled the final data to be less dispersed and produced a better end-result.

6.2 Validity and Reliability

Few instruments were used in this research in checking the validity and reliability of the Delphi responses. Hasson and Keeney (2011) explain that validity refers to the generalisability of the findings, whereas reliability is understood as the consistency of the measurement within a research [20]. In order to test the validity of the questionnaire for this research, a pilot testing was done on four respondents from the academia and the industry with adequate knowledge on ISPS Code. Besides that, this study uses Standard Deviation (SD) and Cronbach's Alpha for reliability. According to Giannarou and Zervas (2014), SD is arguably the most popular tool used for consensus measurement in studies using Delphi technique. Cronbach's Alpha determines the internal consistency or average correlation of items in a survey instrument to gauge its reliability [21]. Therefore, Cronbach's Alpha was applied to the questionnaire responses in order to determine the reliability of the responses. According to Malhotra and Birks (2007), Cronbach's alpha is; (a) very good when the value is given 0.80 and above; (b) acceptable when the value given is above 0.70; (c) moderate when the value given is above 0.60 and; (d) unacceptable when the value given is below 0.60 [22].

7. Discussion

7.1 Validity and Reliability

The first round of this research has involved literature review and data collection using Delphi questionnaire. The questionnaire in this Delphi survey was constructed mainly with reference to the ISPS Code (2003 edition) especially on Part A of the Code as it is the mandatory part of its implementation. The questionnaire was designed with three sections namely:

i. **Section A:** Background information of the respondents.
ii. **Section B:** Open-ended questions that facilitate respondents' opinions and allow them to include additional information.
iii. **Section C:** Closed-ended questions with seven-point Likert scale used to determine the current situation of ISPS Code implementation at VMM.

The questionnaire was subsequently pilot tested by four selected respondents that have adequate knowledge about ISPS Code with minor amendments and subsequently disseminated to respondents through the email on 30th August 2017. Official accompanying letter was also attached together in the email. The first response was received on 15th September 2017 and the last response was received on 24th of September 2017. As some of the respondents worked on shift basis and hardly had free time for consultation, researchers decided to follow up with face to face meetings, emails, short messaging messages and phone calls. One of the other main reasons for the long-time of response in this Round-1 Delphi survey was basically due to respondents' tight work schedule. From a total of 20 questionnaires disseminated, eleven respondents participated in this Round-1 survey. The findings on general background information of the respondents and their familiarity with ISPS Code are summarised as follows:

a. Average age of respondents is 30 years old.
b. Respondents' education level is mostly diploma.
c. Respondents' position in the company varies from technical personnel, security officer and executive.
d. Respondents' work experience is 4 years and above.
e. Most of the respondents have medium level of familiarity with ISPS Code.

The Round-1 Delphi survey was implemented to qualitatively find answer for research question one (RQ1), i.e. What are the important variables used to determine the effectiveness of ISPS Code implementation? As previously mentioned, the literature review played a partial role in answering the RQ1. From Part A of the ISPS Code (2003 edition), researchers were able to extract five important variables, which have been used to determine the effectiveness of ISPS Code implementation. The variables are:

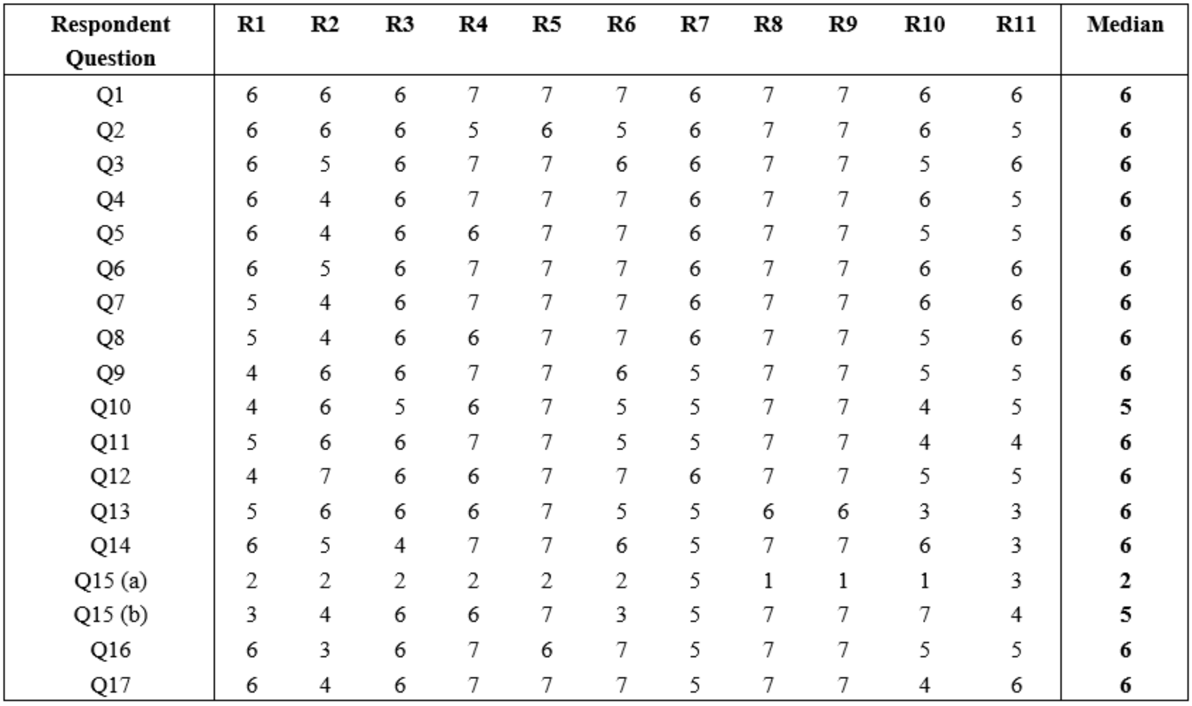
i. Port Facility Security
ii. Port Facility Security Assessment (PFSA)
iii. Port Facility Security Plan (PFSP)
iv. Port Facility Security Officer (PFSO)
v. Training, Drill and Exercise on Port Facility Security.

These five variables were stated in the Section B of the questionnaire that were agreed by the respondents as similar to the variables implemented at VMM. Over and above the five important variables, the respondents have also recommended two additional variables that they felt as equally important in ensuring the successful implementation of ISPS Code, which are as follows:

i. Monitoring, assessment and audit on ship/port facility security (5 respondents).
ii. Access control on cargo, ship/wharf, and people (5 respondents).

The above mentioned two added variables were analysed through content analysis that involved thematic patterns, where all the given comments by respondents were grouped together under suitable headings. This has helped researchers to analyse the given data on the general requirements under ISPS Code that have been practised at VMM. Section C in this Round-1 Delphi survey has involved closed-ended questions with a seven-point Likert scale used to identify the level of adherence on the implementation of the general requirements of ISPS Code at VMM. There were eighteen (18) questions to be quantitatively analysed. By using Microsoft Excel, the median scores for each question were identified in order to provide feedback for the subsequent round of the Delphi survey.

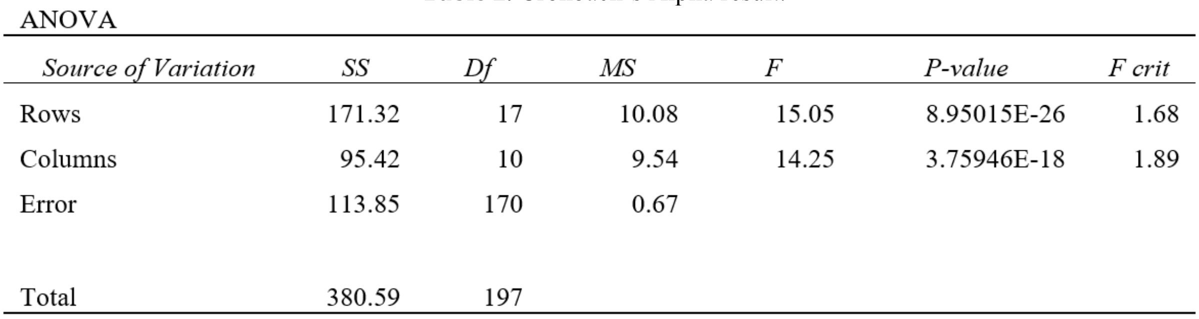
Table 1. Rating and median scores in Round-1 Delphi Survey



Respondent Question	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	R11	Median
Q1	6	6	6	7	7	7	6	7	7	6	6	**6**
Q2	6	6	6	5	6	5	6	7	7	6	5	**6**
Q3	6	5	6	7	7	6	6	7	7	5	6	**6**
Q4	6	4	6	7	7	7	6	7	7	6	5	**6**
Q5	6	4	6	6	7	7	6	7	7	5	5	**6**
Q6	6	5	6	7	7	7	6	7	7	6	6	**6**
Q7	5	4	6	7	7	7	6	7	7	6	6	**6**
Q8	5	4	6	6	7	7	6	7	7	5	6	**6**
Q9	4	6	6	7	7	6	5	7	7	5	5	**6**
Q10	4	6	5	6	7	5	5	7	7	4	5	**5**
Q11	5	6	6	7	7	5	5	7	7	4	4	**6**
Q12	4	7	6	6	7	7	6	7	7	5	5	**6**
Q13	5	6	6	6	7	5	5	6	6	3	3	**6**
Q14	6	5	4	7	7	6	5	7	7	6	3	**6**
Q15 (a)	2	2	2	2	2	2	5	1	1	1	3	**2**
Q15 (b)	3	4	6	6	7	3	5	7	7	7	4	**5**
Q16	6	3	6	7	6	7	5	7	7	5	5	**6**
Q17	6	4	6	7	7	7	5	7	7	4	6	**6**

Legend: R = Respondent; Q = Question

Table 2. Cronbach's Alpha result.

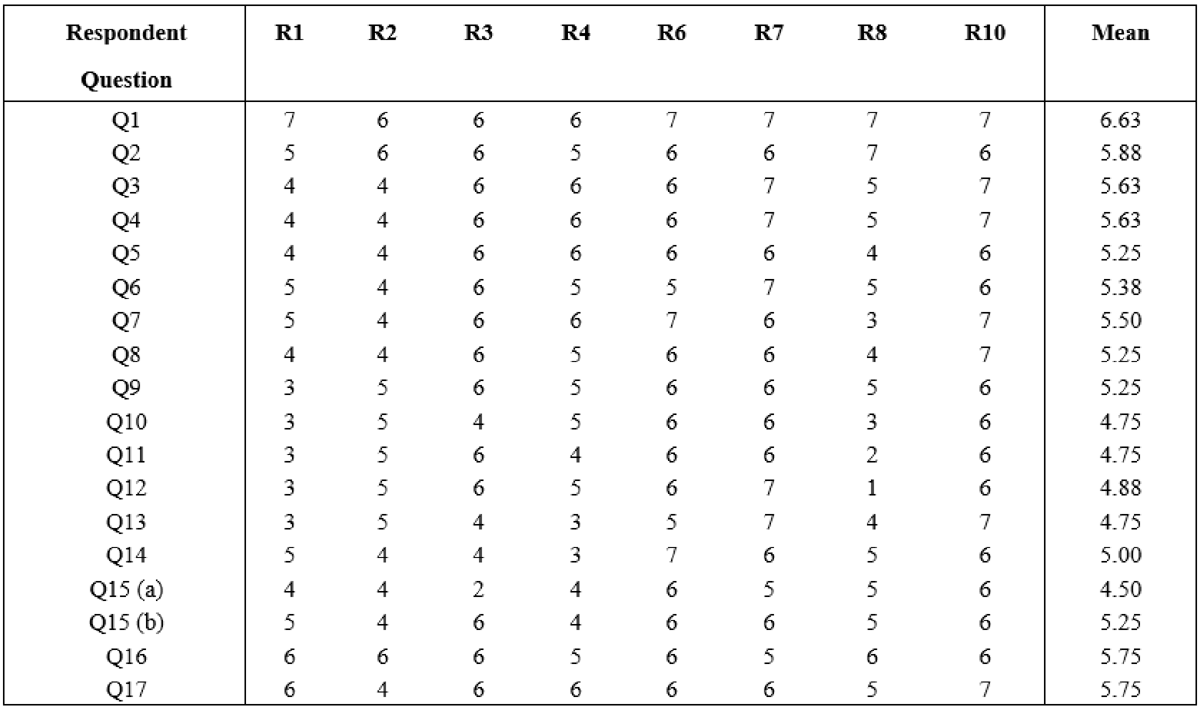


ANOVA

Source of Variation	*SS*	*Df*	*MS*	*F*	*P-value*	*F crit*
Rows	171.32	17	10.08	15.05	8.95015E-26	1.68
Columns	95.42	10	9.54	14.25	3.75946E-18	1.89
Error	113.85	170	0.67			
Total	380.59	197				

α = 0.93355

Table 3. Score rating and mean values in Round-2 Delphi Survey



Respondent Question	R1	R2	R3	R4	R6	R7	R8	R10	Mean
Q1	7	6	6	6	7	7	7	7	6.63
Q2	5	6	6	5	6	6	7	6	5.88
Q3	4	4	6	6	6	7	5	7	5.63
Q4	4	4	6	6	6	7	5	7	5.63
Q5	4	4	6	6	6	6	4	6	5.25
Q6	5	4	6	5	5	7	5	6	5.38
Q7	5	4	6	6	7	6	3	7	5.50
Q8	4	4	6	5	6	6	4	7	5.25
Q9	3	5	6	5	6	6	5	6	5.25
Q10	3	5	4	5	6	6	3	6	4.75
Q11	3	5	6	4	6	6	2	6	4.75
Q12	3	5	6	5	6	7	1	6	4.88
Q13	3	5	4	3	5	7	4	7	4.75
Q14	5	4	4	3	7	6	5	6	5.00
Q15 (a)	4	4	2	4	6	5	5	6	4.50
Q15 (b)	5	4	6	4	6	6	5	6	5.25
Q16	6	6	6	5	6	5	6	6	5.75
Q17	6	4	6	6	6	6	5	7	5.75

Legend: R = Respondent; Q = Question

These median scores have been used in Round-2 survey, which compared each respondent's personal rating score. The personal score and median score from all eleven respondents are shown as per Table 1. The median is used as it will allow respondents to easily compare and re-assess their personal score for each question. By using ANOVA formula in the Microsoft Excel, the reliability of the questionnaire response is proven through the Cronbach's Alpha figure as stated at Table 2, where α = 0.93. As mentioned by Malhotra and Birks (2007), Cronbach's alpha is very good when the value is given at 0.80 and above; acceptable when the value given is above 0.70; moderate when the value given is above 0.60, and unacceptable when the value given is below 0.60 [22]. Therefore, the response to the questionnaire in this Round-1 Delphi survey is highly reliable.

7.2 Round-2 Delphi Survey

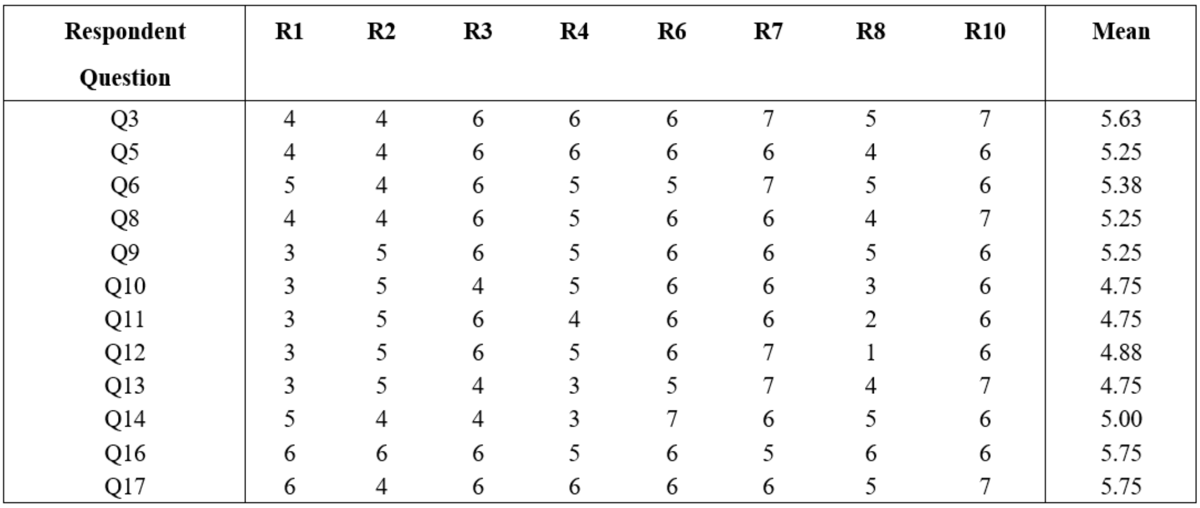
Round-2 Delphi questionnaire was consequently constructed and disseminated to the respondents through the email on the 29th October 2017. The first response was received on 4th November 2017 and the last response was received on 13th November 2017. Similar to the first round, follow up emails, short messaging messages and phone calls were made to assist the respondents where necessary. However, from a total of 11 questionnaires sent out, only eight completed forms were returned in this second round of Delphi survey. The reason for this to happen is due to tight work schedule of the respondents involved. Round-2 Delphi survey was done to comply with the iterative and feedback requirements, as well as to quantitatively find the answer for research question two (RQ2), i.e. What is the level of awareness on the general requirements of ISPS Code among VMM employees? This second-round survey focussed on Section C, which was to identify the level of adherence to the implementation of ISPS Code at VMM. In order to determine the level of adherence to the general requirements of ISPS Code, some important determinants in the questionnaire have been selected for analysis. By using Microsoft Excel, Table 3 was developed showing the findings of Round-2 Delphi survey, which indicates mean values from a total of eighteen questions.

From the 18 questions administered, only 12 questions were used in order to determine the level of respondents' awareness on the general requirements of ISPS Code as follows:

Q3. The PFSO and port facility security personnel have the knowledge and have received adequate training.

Q5. The PFSO undertakes regular security inspections of port facility.
Q6. The PFSP has been produced after a comprehensive security assessment by the relevant authority.
Q8. The PFSP has been periodically (e.g. annually) tested or audited by the appropriate authority.
Q9. The company conducts regular drills as required by the ISPS Code.
Q10. ISPS drills have been conducted every quarterly.

Table 4. Determinants to assess level of adherence to ISPS Code



Respondent Question	R1	R2	R3	R4	R6	R7	R8	R10	Mean
Q3	4	4	6	6	6	7	5	7	5.63
Q5	4	4	6	6	6	6	4	6	5.25
Q6	5	4	6	5	5	7	5	6	5.38
Q8	4	4	6	5	6	6	4	7	5.25
Q9	3	5	6	5	6	6	5	6	5.25
Q10	3	5	4	5	6	6	3	6	4.75
Q11	3	5	6	4	6	6	2	6	4.75
Q12	3	5	6	5	6	7	1	6	4.88
Q13	3	5	4	3	5	7	4	7	4.75
Q14	5	4	4	3	7	6	5	6	5.00
Q16	6	6	6	5	6	5	6	6	5.75
Q17	6	4	6	6	6	6	5	7	5.75

Legend: R = Respondent; Q = Question

Q11. The company conducts regular exercises as required by the ISPS Code.
Q12. ISPS exercises have been conducted at least once a year.
Q13. The company has exercised all the three security levels required under ISPS Code.
Q14. Stakeholders (contractors, suppliers, shippers, etc.) have fully complied with the port facility requirements.
Q16. There is no conflict between visiting ships and the port management in implementing the ISPS Code requirements.
Q17 All activities related to the requirements of the ISPS Code are recorded and safely kept in appropriate place.

Table 4 demonstrates data from Round-2 Delphi survey focusing on the 12 important factors that were used in the analysis.

In analysing Table 4, all the 12 questions to indicate the level of adherence to the general requirements of ISPS Code ranges from 4.75 to 5.75 and achieved and aggregate mean of 5.20, which lies between “Somewhat Agree” and “Agree”. The aggregate result generally indicates that VMM has satisfactorily adhered to the general requirements of the ISPS Code. Notwithstanding the above findings, the areas that require further improvement may be focussed on those addressed by Q10, Q11, Q12 and Q13 involving the conduct of regular drills and regular exercises.

8. Conclusion

In retrospect, it can be concluded that other than the five determinants highlighted by the ISPS Code in ensuring compliance with ISPS requirements, this Delphi study has managed to shortlist two more key determinants as recommended by VMM employees. The two additional determinants are “monitoring, assessment and audit on ship/port facility security” and “access control on cargo, ship/wharf, and people”. In order to ensure a comprehensive adherence to the ISPS code, the determinants identified in Round 1 Delphi survey have also been included in the subsequent Delphi round. The outcome of the survey has concluded that VMM has satisfactorily adhered to requirements of the ISPS Code. It can also be argued that, with some enhancement in the conduct of regular drills and regular security exercises, the level of adherence will certainly be improved. As this research is only a short research done in one academic semester, it is proposed that a follow-up research to be conducted. This will enable the important factors to determine the level of adherence to ISPS requirements to be given the necessary weightages. It can be subsequently used to develop a decision-making model to assess the level of compliance for VMM and other ports with similar operations in more detail.

References

[1] International Maritime Organization, *ISPS Code: International Ship and Port Facility Security Code and SOLAS Amendments 2002,* IMO Publication, London, 2003.

[2] International Maritime Organization, http://www.imo.org/en/About/Conventions/StatusOfConventions/Pages/Default.aspx, (Accessed 1 May 2018).

[3] Razali, N.H.A., Dahalan, W.S.A., *"The ISPS Code and Its Implementation in Malaysia",* Arena Hukum, Vol. 6 No. 1, pp 1-74, 2012.

[4] Peppinck, A., FindLaw Australia, at http://www.findlawaustralia.com.au/articles/1595/ (Accessed 5 May 2017).

[5] Vale, *Teluk Rubiah Maritime Terminal*, at http://www.vale.com.my/business (Accessed 30 March 2017).

[6] Marine Department of Malaysia, *Organization Chart on Malaysian Port Security under ISPS Code*, at http://www.marine.gov.my/jlm/pic/article/, (Accessed 5 May 2017).

[7] Burmester, C., *International Ship and Port Facility Security (ISPS) Code: The Perceptions and Reality of Shore-Based and Sea-Going Staff* at iamu-edu.org/wp-content/uploads/2014/07/s2-burmester.pdf (Accessed 11 Nov 2017).

[8] Jeong, J., *"Progress and Challenges: Ten Years after the ISPS Code"*, World Maritime University Dissertations, 2013.

[9] Ng, A.K.Y., *"Maritime Security Instruments in Practice: A Critical Review of the Implementation of ISPS Code in the Port of Hong Kong",* Proceedings of the IFSPA 2009 Conference, 24-27 May 2009, Hong Kong, pp. 334-348, 2009.

[10] Hodges, D., *"What is International Maritime Security",* Center for International Maritime Security at http://cimsec.org/what-is-international-maritime-security/2698 (Accessed 5 May 2017).

[11] Zec, D., Francic, V., Simic Hlaca, M., *"Port Security Organization and Functionality: Implementation of the ISPS Code in Medium and Small Country"*, Docplayer, at http://docplayer.net/ (Accessed 4 April 2017).

[12] Bueger, C. (2015). *"What is Maritime Security?"*, Marine Policy, Vol 53, pp 159-164.

[13] International Maritime Organization, *"SOLAS XI-2 and the ISPS Code"*, at http://www.imo.org (Accessed 26 March 2017).

[14] Yilmazel, M., Asyali, E., *"An Analysis of Port State Control Inspections Related to the ISPS Code"*, Proceedings of 6th IAMU AGA 2005, 24-26 October 2005, Malmo, 2005.

[15] Grisham, T., *"The Delphi technique: A method for testing complex and multifaceted topics",* International Journal of Managing Projects in Business, Vol 2, No 1, pp 112-130, 2009.

[16] Gordon, Theodore J., *"The Delphi Method in Glenn, J.C & Gordon"*, Futures Research Methodology, Version 3.0, Rockefeller Foundation, 2009.

[17] Rowe, G., & Wright, G., *"The Delphi Technique as a forecasting tool: Issues and Analysis*", International Journal of Forecasting, Vol 15, pp 353-375, pp 211.

[18] Arof, A. M., Md Hanafiah, R, Ooi, I.U.J., *"A Delphi Study on the Potential Benefits and obstacles of Interstate Short Sea Shipping in Archipelagic Southeast Asia"*, International Journal of e-Navigation and Maritime Economy, Vol 5, pp 97 – 110, 2016.

[19] Finstad, Kraig, *"Response Interpolation and Scale Sensitivity. Evidence Against 5-Point Likert Scale"*, Journal of Usability Studies, Vol 5, No 3, pp 104-110, 2010.

[20] Hasson, F., Keeney, S., *"Enhancing rigour in the Delphi technique research"*, Technological & Forecasting & Social Change, Vol 78, pp 1695-1704, 2011.

[21] Giannarou, L., Zervas, E., *"Using Delphi technique to build consensus in practice",* Int. Journal of Business Science and Applied Management, Vol 9, No 2, pp 65 – 82, 2014.

[22] Malhotra, N. K., Birks, D. F., *"Marketing Research, An Applied Approach, 3rd Ed.",* Prentice Hall/Financial Times, 2007.