Security Performance Measurement System for Port Facility in Compliance to ISPS Code

Zaly Muhammad Shah B Muhammad Hussien
University Teknologi Malaysia

Lee Ghim Teck
Malaysian Maritime Academy

Abstract:

Follow up from the attacked on two targets in United States on 11 September 2001, the International Maritime Organization (IMO) proposed the implementation of a new security measure applicable to ship and port facility. This proposal is contained in the International Ship and Port Facility Security (ISPS) Code and came into force on 1 July 2004.

The present compliance for the ISPS Code is measured through process of auditing via internal and external auditing approaches unlike the safety related processes where the availability of positive performance measurement system allows an organization to determine the effectiveness of the system implementation and identification of level of performance. The absent of such system in the security environment leave questions on the method of determination on it effectiveness level, and how the port facility would positively identified gap(s) in the implementation without having to expect for accidents or attacks on the facility to occur, to determine the level of effectiveness.

This research is trying to propose solutions to the questions arise:

i. Is the present security risk assessment methodology able to facilitate the PFSO to carry out security assessment unaided and at the same time fulfilled the requirement under the ISPS Code?

ii. What is the tool that can provide a proactive mean to measure effectiveness of the security measures and procedures implemented by the port facilities?

iii. Is the present ISPS code implementation audit allow the PFSO to determine the root causes of the weaknesses detected during audit in a structured manner?

Keywords: *International Ship and Port Facility Security (ISPS) Code, Security Risk Assessment, Effectiveness of security measures and procedures, Security Audit, Threats, Vulnerability and Consequences*

1.0 Introduction -- Background of the Problem

Follow up from the attacked on two targets in United States on 11 September 2001, the International Maritime Organization (IMO) proposed the implementation of a new security

measure applicable to ship and port facility. This proposal is contained in the International Ship and Port Facility Security (ISPS) Code and its came into force on 1 July 2004.

In Malaysia, the Ministry of Transport (MoT) which represents the Government of Malaysia as contracting party to the Code has designated the Marine Department of Malaysia (MarDep) as Designated Authority (DA) to oversee and enforce the implementation of the Code. For this to take effect, the MarDep issued two circulars titled Marine Guidance Notes (MGN) 45/2003 and 46/2003 in 2003 to Malaysian registered vessels and port facilities respectively. In MGN 45/2003, it is mandatory for ship operators or its management company to appoint a Company Security Officer (CSO) whose responsibilities is to oversee the security management of all the vessels under its management and for the vessel, one designated Ship Security Officer (SSO), who roles is to assist the CSO on site to manages the security activities on board. These security activities are stated in the Ship Security Plan. For the port or marine facility, MGN 46/2003 required the port operator to designate a Port Facility Security Officer (PFSO) as the person responsible to ensure compliance to the Code and ensure continual effectiveness of the measures and procedures stipulated in the Port Facility Security Plan (PFSP). These mandatory requirements must be adhered to before 1st July 2004 and all SSP and PFSP must obtain the approval from the DA.

As evidence to the compliance of the ISPS Code, the ship is issued with International Ship Security Certificate (ISSC) and the Statement of Compliance for Port Facility (SoCPF) for port facility with the validity of not more than five years. For the purpose of ensuring continuous effectiveness of the ISSC and SoCPF, the administration set out the mandatory requirement of periodical external and internal audit.

PFSO is responsible to ensure the PFSP is kept up to date via continual assessment and internal audit process, which is carried out periodically as well as whenever there are changes that affect the relevancy of the plan. PFSO must conduct regular training for those directly and indirectly involved in the implementation of the security measures stipulated in the plan and organise periodically security drill within the port, and security exercises with external organizations such as with the ship calling its port and local authorities on annually basis as stipulated in Part A Section 17 of the Code.

2.0 Statement of the problem

In the initial implementation of the ISPS Code for port facility, IMO empowered the port facility to carryout self-assessment audit on its own facility in the form of self-assessment questionnaires made available in Maritime Safety Committee (MSC) circular 1131. MSC Circular 1131 covered the implementation of the ISPS Code for the DA and Port Facility. It comprises of a set of questionnaires separated into two parts. The first part is for the DA and the second part is dedicated to Port Facility. Detailed study of the questionnaire demonstrated that the focus fulfilling terms and conditions spelt out in the Code. Thus the MSC 1131 checklist is superficial as the PFSP must fully comply with the Code before they could be approved for SoCPF Certificate be issued.

A study was carried out by the researcher in 2008 on two port facilities in Peninsular Malaysia. The analysis of the data collected and with reference to the literature review indicated that the

present checklist MSC Circ.1131 does not completely cover the audit requirement where it lacked the following areas:

- It focuses heavily on the fulfilling the ISPS Code requirement, thus neglecting the actual implementation of security measures and procedures in the PFSP;
- The Circ.1131 checklist only cross checked with a single source only and that is with the PFSO but not with other sources of data or information;
- The Circ.1131 does not provide a structured audit management program which was needed in this type of environment as the objective of the checklist only on ISPS Code general compliance but not the PFSP requirement which is more specific or individual in nature;
- There is no continuity between prevention and response with consequences management, which mean that the before event initiatives is not coincide with the mitigation strategies in after math of any particular event.

For the above reason, the statement of problem for this research is "The absent of security performance measure system for ISPS Code resulted in difficulty in measuring and managing the effectiveness in the implementation of the security plan for port facility".

3.0 Objectives of the research

With reference to the above statement, the objectives of the research are:

a. To develop a performance measurement system with the capability to provide advance warning to port facility of gaps/weaknesses in the security implementation based on the requirement of ISPS Code taking into consideration the internal capability of the port facility;
b. To provide a performance measurement tool to allow the port facility security officer to measure the effectiveness of the security implementation in the proactive manner.

The scope of the research covers the requirement under the ISPS Code implemented by port facilities operating in Malaysia for access control and protection of restricted areas only, as these two are generic elements involving all ports whereas the other four varies from port to port especially in their fields specialisation. For the purpose of specification, the Code itself, places more emphasis on proactive approach rather than reactive response, the research will focuses on before event activities rather than consequences management. The study will involve selected port facilities and the focus will be on the outcomes of the implementation rather than minimum requirement stipulated in the Code. Due to the confidentiality of PFSP, the input element will cover mainly the security assessment and development of the plan whereas the processes part covered the institutionalization of the security measures and procedures.

4.0 Research Questions

The present compliance to ISPS Code is measured through process of internal and external auditing approaches unlike the safety related processes where the availability of positive performance measurement system allows an organization to determine the effectiveness of the system implementation and identification of level of performance. The absent of such system in the security environment leave questions on the method of determination on it effectiveness level, and how the port facility would positively identified

gap(s) in the implementation without having to expect for accidents or attacks on the facility to occur, to determine the level of effectiveness.

For the purpose of this research, the questions arise are:

a. Is the present security risk assessment methodology able to facilitate the PFSO to carry out security assessment unaided and at the same time fulfilled the requirement under the ISPS Code?
b. What is the tool that can provide a proactive mean to measure effectiveness of the security measures and procedures implemented by the port facilities?
c. Is the present ISPS code implementation audit allow the PFSO to determine the root causes of the weaknesses detected during audit in a structured manner?

5.0 Literature Review

In security, for PMS, hazards occurred due to intentional activities with objectives of causing disruption, damages, injury and even to the extent of death and environmental catastrophes by the intent individual or organization. Reactive approach for performance measurement would not be the acceptable norm for security environment as the extent of damage would probably be huge and it is coupled with the capability of the individual or organization (Jones, 2006). Thus a proactive approach would be seen as the only option of ensuring unforeseen event or threat does not occur.

With reference to the ISPS Code, the process of developing the security plan will be involved the carrying out of the security assessment as the importance integral of the security plan. As the plan is an proactive plan, the assessment is in a form of risk assessment of the possible threats that would likely to be experienced by the organization's facility and it include the case history experience by the facility as well as its surrounding. The follow up from the security assessment will determining the right security procedures and measures to be in placed to ensure any possible threat identified earlier and provide protection to the potential targets which were determined through risk assessment.

MCS/Circ. 1131, is a tool allowing marine facilities to carry out self-assessing to demonstrate the continuing effectiveness of their PFSP and evidence of implementation of the relevant security measures in the plan. The circular was referred to as Interim Guidance on Voluntary Self-Assessment by SOLAS Contracting Governments and by Port Facility. The circular stated that the effectiveness of the implementation of port facility security measures is a continuing responsibility. It is suggested that Contracting Government (CG) self-assess their processes of ISPS Code implementation and thereafter, on five yearly basis and that marine facilities carry out self-assessment annually. The weakness of the self-assessment audit as well as any other auditing processes, where its worked on the comparison of stated objectives against the actual implementation of the agreed processes, but not the effectiveness of the security initiatives, which is protecting the facility against any possible threats.

5.1 Risk Assessment

Kuo (1998) defines risk as a measurement of a hazard's significance involving simultaneous examination of its consequences and probability of occurrence using a combination of practical experience and relevant information on the system and its operating

environment (Kuo, 1998) and risk assessment is define as “The process which determines what can go wrong: the pro-active approach (MCA, 2004)” and is intended to be a careful examination of what, in the nature of operations, could cause harm, so that decisions can be made as to whether enough precautions have been taken or whether more should be done to prevent harm. British Standard (BS 4778) defines risk management as the process whereby decisions are made to accept a known or assesses risk and /or the implementation of actions to reduce the consequences or probability of its occurrence. According to United State Coast Guard (USCG)’s Coast Guard Marine Safety and Environmental Protection Business Plan (2005), there are different types of risk are an important factors in many types of decisions and risk assessment can be range from very simple, personal judgements by individuals to very complex assessments by expert teams using a broad set of tools and information. The key to risk assessment is choosing the right approach to provide the needed information without overworking the problem.

Risk assessment is the proactive approach in identifying risks or hazards, and it will likely be experience in certain work processes (Eliana, 2008). It is generally carried out before the commencement of any tasks and it is used as an approach of proactively developing or incorporating preventive measures to ensure the least possible disturbance toward achieving organizational objectives. In simple wording, it is a process that provides early warning of possible risk or threats. Risk assessment can be approach in a macro and micro way as the process can be varied depending on the nature of the objectives and resources involved in supporting the realization of the objectives. Risk assessment has to be systematically done because failure to identify the correct hazards would result in the failure to apply correct preventive measures (MCA, 2007).

There are two forms of approaches used in carry out risk assessment and at time both approaches are combined to provide more effective evaluation of the specific area of work or concern (FATF, 2008). The first approach is the quantitative approach which is used when there is sufficient data to work with in identifying hazard and likelihood of threat, such data include previous accident/incident records, survey reports, research data and equipment manufacturer manual, which are provide factual data to allow for the quantifiable input to be placed in evaluating processes.

The second approach is used in situation where the related work processes is still new and lack of factual data, the qualitative approach of risk assessment is used to facilitate risk identification and formulation of preventive measures including placement of necessary physical barriers.

The existing of records of past event would able to provide quantitative assessment possible but in situation where the absent of such data in situation where it is a new facility and lack of enforcement agencies support, the qualitative assessment approach have to be in place and data collection is through second party resources through public domain. Ratings allocated for the likelihood of occurrences to allow easy measurement and determination in the focuses on the undesired event. It is necessary so that the organization could place priority of a particular event and at the same instances to allow allocation of resources and concentration during the risk assessment processes as there may be large numbers of possible occurrences that might be experience by the organization especially when handling high volatile cargo or consignment. As time would be limited, thus by assigning specific value rating, it allow the organization to paid extra attention on undesired event that having high value and allow the organization to return to tackle low value event. The availability of past record would further facility this stage of assessment.

At time, the assessor will require to provide measurable statement to each sub-heading to facilitate the level of consequences for measurement purposes. The level of consequences will be based on the weightage place on each consequences and its contribution to the functions of an organization and the rate of recovery in case where the actual event occurred. The ratings allocated generally depending on the risk assessment tools that are being applied at the time of the assessment. Some of these risk assessment tools are such as Fault Tree, Checklist, Brainstorming, HAZard Operability (HAZOP), What if, Structured What If, and Failure Mode Effect Analysis (FMEA).

5.2 Accident Investigation

The reverse of risk assessment is accident investigation. It is the reactive and systematic approach in determining what causes a particular accident or incident. The focus is from the identification of direct, indirect and root causes, a lesson can be learned so that future similar occurrences can be avoided all together (Sklet, 2002).
Accident is defines as “An unexpected, unplanned, unorganized, unpleasant, unfortunate “event” that happened and resulted in damage, injury etc”. Whereas investigation is defined as “An effort to discover and examine all the information, facts about “something” (e.g near miss, incident, accident etc), in order to obtain the truth by study or research”. Accident is always unplanned and generally does not necessary occurred in a particular instances or single cause, as it is always believed, there must be existence of error chain or error trail that leading to an unsafe event. The accident investigation purposes are to determine those causes and identified weaknesses in the existing barriers. Only from that approach is the investigator would be able to identify the root cause and recommend enhancement in the existing processes and/or procedures to prevent recurrences. Accident investigation is a process of determining the facts contributing to an accident and no intention of placing blame on any individual although presently that the common practice in the industry (Sklet, 2002, Clifton, 2000 and DOE, 1999).

Fact-finding or investigation begins during the collection of evidence. All sources of information (e.g., accident site walk-throughs, witness interviews, physical evidence, policy or procedure documentation) contain facts that, when linked, create a chronological depiction of the events leading to an accident. Facts are not hypotheses, opinions, or analysis. Facts are deduced to determine the causal factor that contributed to the accident and DOE (1999) defined Causal Factors as “the events and conditions that produced or contributed to the occurrence of the accident”. Causal factors can be divided into three separate but inter-related types of causal factors and they are:

a) Director causes
b) Contributing causes or indirect causes
c) Root causes

The direct cause of an accident is the immediate events or conditions that caused the accident whereas contributing causes are “events or conditions that collectively with other causes increased the likelihood of an accident but that individually did not cause the accident”, and root causes are the causal factors that, if corrected, would prevent recurrence of the same or similar accidents. Root causes may be derived from or encompass several contributing causes.

After any accident, the investigator commences evidence collection activities through various resources available at the time in various forms mainly human or testamentary evidence, physical evidence and documentary evidence. The evidences collected will be studied in three general approaches, they are the deductive approach, the inductive approach and the

morphological approach using various tools available today such as Fault Tree Analysis, FMEA, HAZOP, Tripod Beta and Event Tree Analysis. All these tools have a single objective that is to identify failed barrier and determine why these barrier failed.

5.3 Combination of Risk Management and Accident Investigation

The Nautical Institute defines safety management as a process which coordinates resources and activities to ensure that an acceptable level of safety is achieved for a situation or system (Kuo, 2007), and in Clause 8 Paragraph 8.1 and 8.3 of International Safety Management (ISM) Code made it mandatory for the shipping companies to document the actions required in situations that may be constitute as emergency situation and at the same time identified all possible hazard that the vessel/s would likely encountered or experienced. Similar requirement also stated in Section 9.4 and 16.3 Part A of the ISPS Code where the ship and port facility respectively in their security plan to document the possible hazards or risk that they might encountered and the response measures in cases of emergency. It has becomes a mandatory requirement in any company safety or security management system and manual to have risk management as well as mitigation strategies for emergency situations to be in place.

Both Kuo (2007), Jones (2006), Sklet (2002) and Stranks (2001) emphasis the need to include both element of risk management and emergency respond in the security and safety manual respectively as it provide a totality in the safety management of the company activities. Presently both activities of risk management and emergency respond are handled as separate initiatives and most of the occasion they are not interrelated. When the activities were developed on the piece meal basis, the effectiveness of the implementation may become a question as the barriers created will also be fragmented.

5.3.1 Bow-tie Method

The earliest origins of bow-tie methodology are unknown but the earliest mention appears to be an adaptation from the ICI plc Hazan Course Notes 1979, presented by The Universitity of Queensland, Australia (Hurst, 2005). The ultimate aim of bow-tie to demonstrate control of hazards, it is therefore necessary to identify those hazards in the first place and follow up with the risk assessment and provide a framework to demonstrate effective control (Hurst, 2005 and Turksema, 2007). Figure 1 illustrate typical structure of bow-tie diagram where the event is placed at the centre of the attention rather than at the end if compared with risk assessment and accident investigation methodologies where the event is located at either end and from there works forward or backward.

Bow-tie models are tools for integrating broad cases of cause-consequence models. The familiar fault tree and event tree models are ‘bow-tied’ in this way and indeed attaching the fault tree’s ‘top event’ with event tree’s ‘initiating event’ originally suggested the bow-tie methodology. It is provide a ‘bird’s eye view for focusing on causal chains and projecting these onto the space of consequences. These consequences will be factored into decision problems for risk management. Bow-tie consequences side forms an interface with the decision models. Decision taken will reflect backward to causes. This structure not only has proven a worthwhile concept in accident prediction, it also has proven its worth in analyzing past accidents and suggesting improvements to prevent further re-occurrence which back up the original objective of accident investigation of “lesson learned”. The selection of the centre of the bow-tie is

crucial for the analysis. The causes and consequences of this event form the bow-tie and form a slice out of all the things that happen in this world (Bellamy, 2006). Any event can be considered a cause and any event can be considered a consequences.

According to Hurst (2005), Bow-tie provides a robust, comprehensive yet simple means of "rolling out" the main points from a risk assessment exercise or HSE case. It is possible to use the bow-tie in conjunction with Tripod technique as well as layer of Protection Analysis (LOPA) which provide qualitative and quantitative approach respectively in risk assessment.

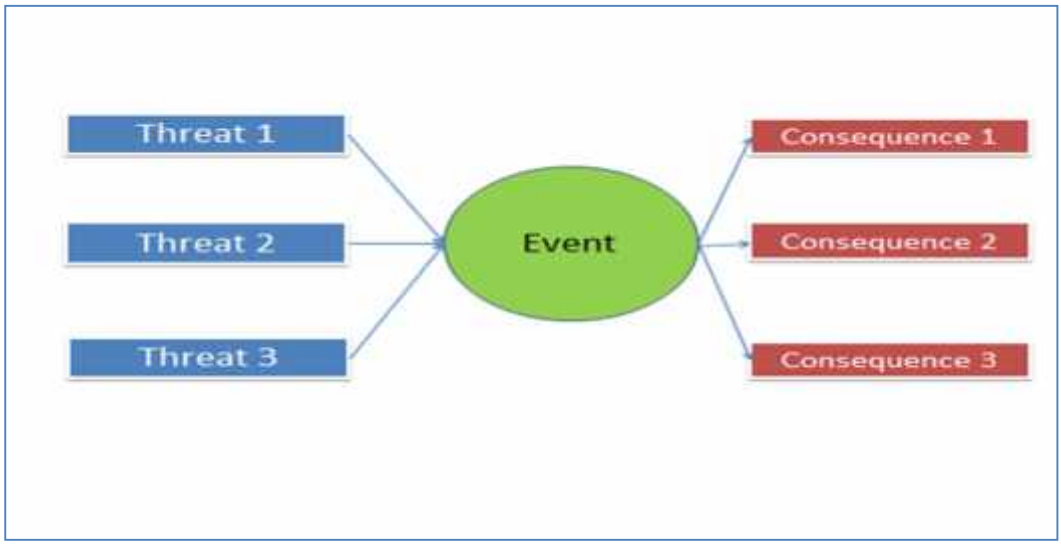

Figure 1 Illustrate a typical Bow-tie diagram in security contact

After the causes and consequences are recognized, the barriers can be placed in between them which may be in the form of operation procedures and management system. The barriers as illustrated in Figure 2 can be comprises of various approaches and generally they comprises of passive barriers, active barriers and behavioural barriers. Passive barriers are those barriers that perform their function without any intervention, whether they control expected flows of energy or protect against unexpected one. Active barriers do need some activation to become functional, which may be hardware or software driven. Behavioural barriers or elements that involved some kind of human intervention. Very often a barrier involved hardware, software and behavioural elements because the full operation of a barrier to fulfil a safety function has to have 3 separate activities or phases. The 3 phases are detection, diagnosis and action.

Both Cambon (2008) and Visser (1998) agreed that the setting of barriers at the fore part of the event alone would not be sufficient thus it is recommended barriers to be setup after the event has occurred with the purpose of ensuring further damage or lost of life would be minimized.

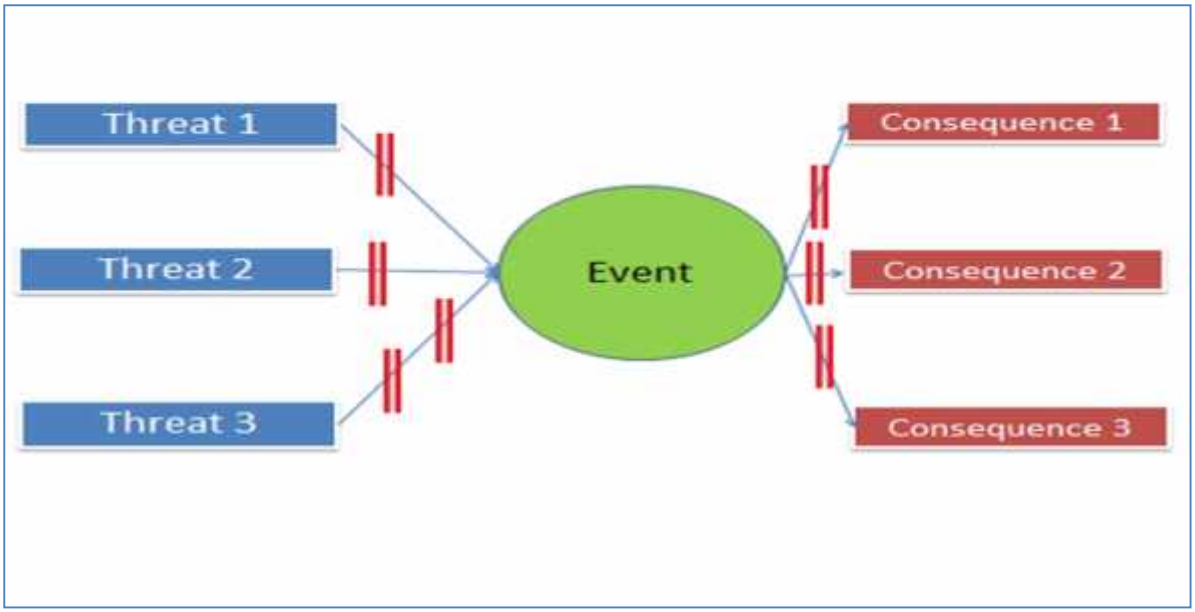

Figure 2 Bow-tie with barriers placed on either side of the event

In the effort to determine the most suitable methodology to be used for the purpose of this research for the development of Security Performance Measurement System (SPMS) with the purpose of providing the Port Facility Security Officer (PFSO) with structured security risk assessment methodology and a measurement tool to allow the PFSO to measure the effectiveness of the security implementation in the proactive manner. An analysis of the various risk assessment and accident investigation methodologies describes in Table 1. A total of 24 risk assessment and accident investigation methodologies were studied with the following criteria:

a) Value to the analysis – whether qualitative and/or quantitative;

b) The need of specialization and training in the use of each methodology;

c) Its application – whether applicable for risk assessment, accident investigation or both;

d) Its ability to determine the root cause/s;

e) Its process application – whether for existing work process, new work process or applicable to both new and existing processes.

The above five criteria were chosen for the following reasons:

1. In item (a) above, the qualitative or quantitative approaches would allowed the analysis outcome to be determined either on the quality or quantity of the assessment for the purpose of evaluating the relevancy of the data collected and at the same time allowing assessor to make decision based on specific facts or numerical measurement, or both;

2. With reference to (b), the knowledge and experience poses by the evaluator/assessor/investigator would able to add value to any analysis as they are able to appreciate the processes involved and the reason for specific actions taken in assessing specific situation or scenario and the knowledge and experience would allow the assessor to provide specific recommendation to further enhances the processes and suggest improvement steps to

Methodology	Quantitative Approach	Qualitative Approach	Need Subject Matter Expert	Risk Assessment (RA) /Accident Investigation (AI)	Identification of root causes	Applicable to New Activity (NA)/Existing Activity (EA)
Pareto Analysis	Yes	No	No	RA	No	EA
Checklist Analysis	No	Yes	Yes	RA/AI	Yes	EA
Relative Ranking / Risk Indexing	No	Yes	No	RA	No	EA
Preliminary Risk Analysis	Yes	Yes	Yes	RA	No	NA/EA
Change Analysis	Yes	No	Yes	RA	No	EA
What If Analysis	No	Yes	Yes	RA	No	NA/EA
Failure Modes and Effect Analysis (FMEA)	No	Yes	Yes	RA	No	NA/EA
Hazard & Operability (HAZOP)	No	Yes	Yes	RA	No	EA
Fault Tree Analysis (FTA)	Yes	Yes	Yes	RA/AI	Yes	NA/EA
Event Tree Analysis (ETA)	Yes	Yes	Yes	RA/AI	Yes	NA/EA
Preliminary Hazard Analysis (PrHA)	No	Yes	Yes	RA	No	NA
Event & Causal Factor Charting (ECFC)	No	Yes	Yes	RA/AI	No	NA/EA
Barrier Analysis	No	Yes	Yes	AI	No	EA
Change Analysis	No	Yes	Yes	AI	No	EA

avoid future recurrences, the subject matter expert knowledge and experience would be more relevant in methodology where qualitative approach of assessment is in discussion;

3. With reference to (c), some methodology is design purely for specific activities and at time it has difficulties to provide complete picture or bird eye's view of the whole assessment processes. The criteria is chosen to determine the methodology that would able to cover the whole work activities and demonstrate that various steps are put in place to manage the risk as well as mitigate the consequences, which is at the after the event where the mitigation activities are demonstrated;

4. With reference to (d) above, root cause analysis is a critical step to determine what are the actual causes that contributing to the failed barriers and it also demonstrate the level of support up to the management level put into place to ensure it is implemented;

5. Reference to (e) above, any level of application reflect the effectiveness of the system to foresee potential risks and determine the action necessary to prevent unforeseen occurrences.

Table 1 – Analysis of Risk Assessment and Accident Investigation Methodology

Change Analysis	No	Yes	Yes	AI	No	EA
Root Cause Analysis	No	Yes	Yes	AI	No	EA
Management & Organizational Review Technique (MORT)	No	Yes	Yes	RA/AI	No	EA
Systematic Cause Analysis Technique (SCAT)	No	Yes	Yes	AI	No	EA
Sequential Timed Event Plotting (STEP)	No	Yes	Yes	AI	No	EA
MTO (Menneska Technology Organzation) Analysis	No	Yes	Yes	AI	Yes	EA
Accident Evolution & Barrier Function (AEB)	No	Yes	Yes	AI	Yes	EA
Tripod	No	Yes	Yes	AI	Yes	EA
Tripod Beta	No	Yes	Yes	RA/AI	Yes	NA/EA
Acci-Map	Yes	Yes	Yes	RA/AI	No	EA
Bow-Tie	Yes	Yes	Yes	RA/AI	Yes	NA/EA

With reference to the analysis of the various methodologies as demonstrated in Table 1 above, it is observed that Event Tree Analysis (ETA) and Fault Tree Analysis (FTA) methodology are the two analysis tools that can be applied for the risk assessment and accident investigation and at the same time provide qualitative and quantitative analysis/measurement outcome. At the same time, FTA and ETA also suitable to be used for existing activities as well as new activities. For the context for this research, existing activities are referred to activities that has been carried out before or routine in nature whereas new activities are referred to activities that

is new to the organization and never been done before, at the same time the organization has no experience.

FTA and ETA processes also allow the assessors/investigators the determined the root causes or contributing factors leading to any failure in the process delivery so that remedial actions can be taken to prevent future recurrences.

It is also observed that Tripod Beta methodology which traced its origin from Tripod methodology provide full view of the assessment flow including it capability by be used not only from the traditional accident investigation point of view but also risk assessment (Turksema and Postman, 2007). As Tripod Beta methodology main focus is to identify root causes to system/process failure, it is feasible tool to determine system effectiveness and with reference to the earlier security assessment principle that the vulnerability of a particular security measures and procedures would depend on the internal organization effective in ensuring effective implementation as the external factor such as threat is beyond organizational control. Thus Tripod Beta methodology would be an ideal tool for measuring effectiveness of the security implementation and at the same time identified root causes of implementation failure.

Bow-Tie methodology is observed in comparison with other methodologies that provide combination of risk assessment and accident investigation in assessment of risk, is that it provides a total coverage in a simplified bird-eye view (single diagram). At the same time, Bow-Tie methodology allowed adaptation of other methodologies in risk assessment or accident investigation, and combination of both. This combination would be ideal in the security environment, the stress in not only in risk assessment but also consequences management for the purpose of preventing or minimizing further damage.

6.0 ISPS Code -- Security Assessment

This part contained in Section 1.2 Part A of the Code and it comprises of 5 objectives and followed with Section 1.3 with additional 7 functional objectives. In section 1.2.4 where it is mention “to provide a methodology for security assessment so as to have in place plans and procedures to react to changing security levels”.

The challenge at this point is the absent of the single acceptable methodology to carry-out the security assessment, and it is made difficult event to determine the level of threat that are likely to be experience by specific facility which will be explained below.

Presently there are two assessment methodologies that are commonly used for port facilities. One is the 3 by 3 Matrix recommends by United State Coast Guard (NVIC-11-02) and the other is Threat and Risk Analysis Matrix (TRAM) (IMO/ILO Code of Practice on Security in Ports, 2004) recommends by International Labour Organization (ILO). Majority of the administration do specified the methodology of their choice but some may leave it to the port facility to decide. In Malaysia, the TRAM approach of security assessment is recommended by MarDep to port facilities under their purview. Both used the equation of:

Security Risk = Likelihood X Vulnerability X Consequences

In the above equation, likelihood is the multiplication of threat and frequency which is beyond the control of the port facility whereas for the consequences, it is dependence on the ability of

the port facility recover mode. Only the vulnerability element is within the control of the port facility (Brooks and Pelot, 2008). Vulnerability is referred to effectiveness of the security measures and procedures in place to positive protection and prevent untoward incidences.

Both methodologies provide good guidelines to carry-out the security assessment for port facility but at the same time there exist areas where certain elements are left to the judgement of the port facility which may result in inconsistencies in the assessment outcomes. The comparison in term of flexibility and challenges faced by both methodologies are described in Table 2.

Table 2: USCG and ILO Risk Assessment Methodology Comparison.

	NVIC-11-02 (USCG)	**TRAM (ILO)**
Threat	Threat scenario focuses specifically on the possible action that may be taken against facility in the whole and provide detailed description of scenario types. The number of scenarios is left to the judgement of the facility. Confirmation of likely occurrences of the identified threat scenarios is difficult to determine as most port facility do not kept record on security incidences surrounding their facility.	Threat focuses of specific potential target in the facility and the facility need to determine the level of threats which are divided into 3 different levels. The number of scenarios is left to the judgement of the facility. Similar issues faced in determining the level of threat and confirmation of likely occurrences as for the USCG's methodology.
Vulnerability	Cover in 4 different elements but for port facility only two elements (accessibility and organic security are considered). The criteria for scoring concentrated on the measures and procedures in place to provide protection against any possible threats. The vulnerability score is cover in 3 ranges and the criteria for each score are up to the port facility to define.	4 levels vulnerability scores and each score has their specific descriptor. The criteria for scoring focuses on levels of protection or security measures in place and almost similar to the USCG criteria.
Consequences /Impact	3 levels of consequences score and focuses mainly on the nature of port operation in	5 levels of consequences/impact score and the criteria for the scoring

	whole with particular focus on type of cargoes handle. Little avenue available to change the score as it reflex the facility in totality.	are focuses on the nature of loss. Provide flexibility to alter consequences score as well.
Assessment Outcome	The assessment outcome is derived from the matrix provided with reference to the scoring from vulnerability and consequences scoring. It uses the 3 by 3 matrix and the outcomes are divided into 3 categories namely Document, Considered or Mitigate. Thus provide clear action of the follow-up action that need to be carried out. The assessment outcome is reflected in Mitigation determination worksheet.	Assessment outcome is reflected as risk score in the column F of the TRAM table. The scoring is derived from multiplication of the scoring of threat, vulnerability and impact. Acceptable risk score is not mentioned thus it left with the port facility to determine.
Mitigating actions	Further action to reduce vulnerability of the facility to identify threat is documented in Mitigation Implementation Worksheet and the only flexibility of scoring is available in the Vulnerability column. After the mitigation strategy is identified, new mitigation result has to be worked out to demonstrate lower score.	Mitigation available by reducing either vulnerability or impact score or both to reduce the risk score through specific mitigation activities/initiatives. New risk score need to be worked out to measures the outcome of the mitigation initiatives.

6.1 Determining of threat level, vulnerability and consequences/impact

Confirmation on nature of likely threats to specific facility or even potential target/s in the facility have to be considered from various angles as even though some or most of the threats identified during the assessment process may not have been experienced before by the port facility but they should not disregard similar occurrences surrounding the facility. For this purpose, the PFSO need to obtain the assistance of external governmental security related agencies for confirmation of likely threat and determination of the threat score.

For the identification of vulnerability, actual physical inspection and observations are better than purely table top assessment as it provide better picture as to actual environment at the time

of assessment and at the same time, any defect or malfunction can be immediately identified and recommendation of rectification be made. As before additional measures and initiatives taken to enhance security measures, it is recommended to carryout in day light as well as night time environment. This is necessary as it provide a clear picture of view of sight in different lighting condition.
The ILO recommendation for determining of level of impact provide better apportioning of scoring as the division of criteria provide flexibility to distance the victims from the potential target as part measures to reduce the risk score as one of the element that mentioned in part A Section 16.3.5 of the ISPS Code. Table 3 is the format of TRAM table.

Under the ILO recommendation, the common challenge faced during the security assessment is the determining of level of acceptable risk score. In the USCG's recommendations the mitigation determination worksheet linking to the matrix provide clear action of what to be done form the assessment outcome whereas in the ILO recommendation, acceptable risk score is not mentioned to guide further mitigation initiatives. As the risk score is derived from multiplication of result in threat, vulnerability and impact assessment, any single changes in the score would generally double the risk score and as the ranges of threat, vulnerability and impact are various for all three deliverables, the equal ranges separation of division cannot be applied to equate it to the recommendation by USCG on assessment outcome as Document, Considered or Mitigate. In this case, the port facility will has to determine the result of acceptable risk score in term of percentage, example allowing 5% of the highest score (which is 60) as acceptable risk score where no further action is required or allowing 5% gap and any outcome more than 5% mean additional initiative of enhancing existing security measures or barrier/s need to be put in place or even place additional new security barriers or measures.

Table 3: Example of TRAM table, (ILO, 2003).

Scenario No.	Threat Scenario	Threat	Vulnerability	Impact	Risk Score	Action priority
A	B	C	D	E	F	G
1	Destroy port authority's communication tower by explosives	1	2	3	6	

7.0 Port Facility Security Plan

The final outcome from the security assessment will be used for the development of security plan or Port Facility Security Plan (PFSP) (ISPS Code Part A Section 15.1). The general content of the plan is outline in Part A Section 16.3 of the Code, which comprises of 15 sub-sections. These sub-sections can be divided into 3 main categories, namely Prevention, Respond and Consequences Management as illustrated in Table 4 below. Some sub-sections were not in the Table 7 as it covered management of human resources or the plan itself.

Table 4: Categorization of Contents in PFSP

Sr. No	Categories	Sub-Section of 16.3

1	Prevention	16.3.1, 16.3.2, 16.3.7, 16.3.11, 16.3.12, 16.3.13 and 16.3.15
2	Respond	16.3.4, 16.3.9 and 16.3.14
3	Consequences Management	16.3.3 and 16.3.5

It was observed that the Consequences management portion seem to be distanced from the security assessment especially in the emergency preparedness elements. The diagram in Figure 3 illustrated the right flow of the whole security assessment process where the author noticed a common practice is HSE safety assessment. Thus during the development of emergency response procedures, consideration has to be taken into consideration of the earlier identified threat and its associated scenario and mitigation initiatives in case the breach of security is successful. This will provide a continuous flow of the total inclusive security plan.

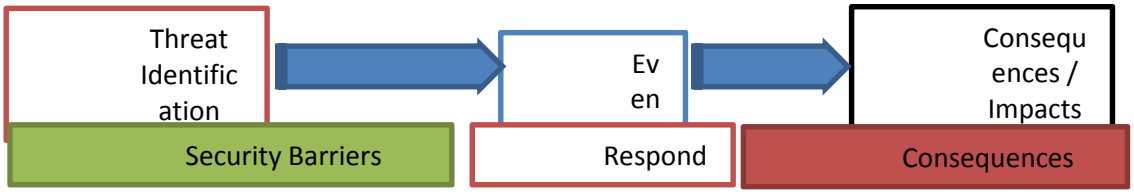

Figure 3: Brief Flow Diagram of Security Assessment Processes

8.0 Security Performance Measurement System (SPMS)

A good performance measurement system must possess the following qualities:

a. They must be objective driven where the end state must be spelt out and this will allow careful planning to be carried out for the purpose of ensuring the planning, organizing and controlling of the clear direction available to achieve the set objectives;

b. Clear measurable indicators, these will allow the assessor/s to have asses the outcome of the set initiatives and to determine the extent of success or failure, and at the same time identify further actions that need to be taken to arrive at the set objectives.

As the methodology for identification of possible security risk is based on the risk assessment methodology and from the literature review, the methodology for risk assessment and accident investigation can be interchanged (Hurst, 2005 and Bellamy et al, 2006) and as the initial process of risk assessment is to identify the associate hazards exist in the surrounding, in the environment, the process involved and even the nature of work or material involved in particular activities. After reviewing the methodologies that being applied, it was propose the tripod accident investigation methodology is used for the purpose of evaluating the effectiveness of the security measures and procedures being enployed as it provide the following advantages:

(a) The direct cause or active failure stage would be able to be identified as it is the beginning evaluation of the effectiveness of the measures that contributed to the actual weaknesses or strength of implementation on the immediate security initiative;

(b) the second level of the Tripod methodology focuses the contributing factors or pre-condition that result in the failure of the initial preventive measures and this would allow the identification of the support available to facilitate the implementation of preventive measures and procedures;

(c) The third level is the latent failure or the root causes that contributed to the failure of the total preventive measures and this level of failure could be traced right up to the management level.

By having the capability to measures that total organizational involvement in support of the effectiveness of the implementation of specific measures and procedures, it would be to detect any possible cuases of failure and at the same time detect whether the detection mechanism are in placed so that such failure do not occur.

As the requirement of the security plan are identification of possible risks or threats, preventive measures and procedures in relationship to the identified threats as well as procedures and measures in responding in situation where the occurance of the said risk or the failure of the preventive, thus emergency preparadeness activites must also be developed as part of the security plan. Taking that into consideration, the Bow Tie approach is the most suitable as it provide platform to gudge the relationship in term of identified threats as well as linking it to the mitigation initiatives in cases of subsequent failure in the prevention measures. This is necessary so that the consequences management is also taken into consideration and taken as part of effectiveness study. The figure 3.1 below provide the generic diagram of the utilization of the Bow Tie concept with the Tripod analysis in the study to determine the effectiveness of the security performance for a port facility in term of risk assessment and mitigation of consequences of failed security barriers. Figure 3.1 also reflect the equation in Chapter 2 (USCG's NVIC, 2007, ILO, 2003 and Brooks and Pelot 2008) where Security Risk is the multiplication of Threat, Vulnerability and Consequences. Where the vulnerability elements are reflected security measures/barriers created/set to prevent the undesire occurences or undesire event.

In Figure 4, the threat identification methodology utilised for this study is the one recommended by ILO's Code of practice on security in ports (ILO, 2003) with additional elements of data coverage to provide a more systematic of assessment which will be discussed later in this chapter. The ILO's security assessment methodology was chosen as it is the recommended methodology by the marine administration of Malaysia and that is the Marine Department Malaysia and at the same time majority of the marine facilities in Malaysia conduct their security assessment based on the similar methodology.

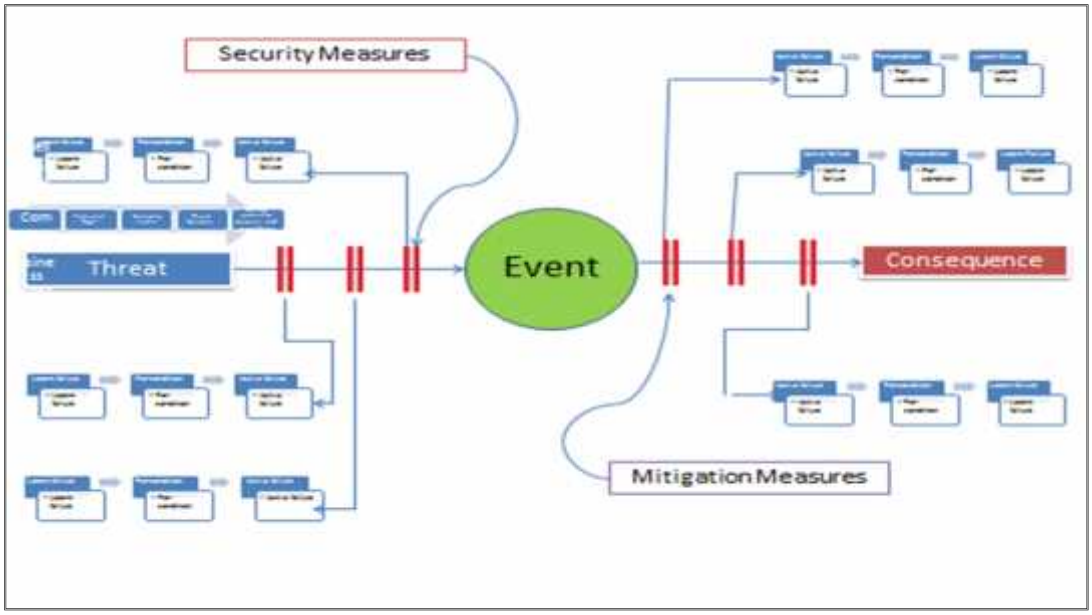

Figure 4 – Security Performance Measurement System (SPMS) Structure

With reference to Figure 5, the identifications of security risk will commences with the inventory of port activities available in the port facility where it is divided into four difference categories namely operation, facilities, infrastructure and commercial or business entity. In operation, its cover the entire marine related activities such as loading and unloading of goods/passengers including the transfer of goods, movement of vessels in and out of the port or piloting movement, physical movement of goods or stevedoring, handling of dangerous or hazardous goods including chemicals and petroleum products, and handling of goods while in transit such as storage, warehousing, packaging and value adding activities. As this operation may be varies from the port to port based on the area of specialization and focus. The researcher will need to have full understanding of the port operation to develop the inventory of operation. The next related activities that will be study are the physical facilities that facilitate the activities of the port such as such as berth spaces for vessel berthing and unberthing and at the same time play the roles of ship-port interface to facilitate the movement of goods and /or passengers, warehouses for storage of goods beside supporting other activities such as packaging and value creation, container yards, access points for vessel including the navigational aids and vessel traffic information and monitoring system, physical perimeter fencing on the shore side including fence lighting and remote monitoring facilities, physical information communication and technology network and other facilities that contributed to the smooth and efficient operational activities. The detailed is illustrated in Figure 6 below.

The other two are the insfrastructure and commercial/business information data. These two may not directly contributed to the effective movement of goods/passengers in the port facility but their existance are to ensure the connectivitiy as well as to provide continuous safeguarding and mitigate any unforseem consequences of internal events. The infrastructure in focus are roads and access such as bridges and rail track, water access areas so to ensure sufficient underkeel clearance and good anchoring holding ground free from any obstructions, berthing facilities such as mooring bitts, fenders, fresh waterline etc., lifesaving and fire fighting and prevention facilities such as lifebuoys with lights and lines, portable and fixed fire extinguishing system, fire and smoke detection. Finally on the commercial/business information data, refer to the software to facilitate the smooth movement of goods and containers, measuring and monitoring the loading/unloading and transfer of dry and liquid

bulk, shipboard containers distribution , ships' bending moment and shearing forces diagrams etc.

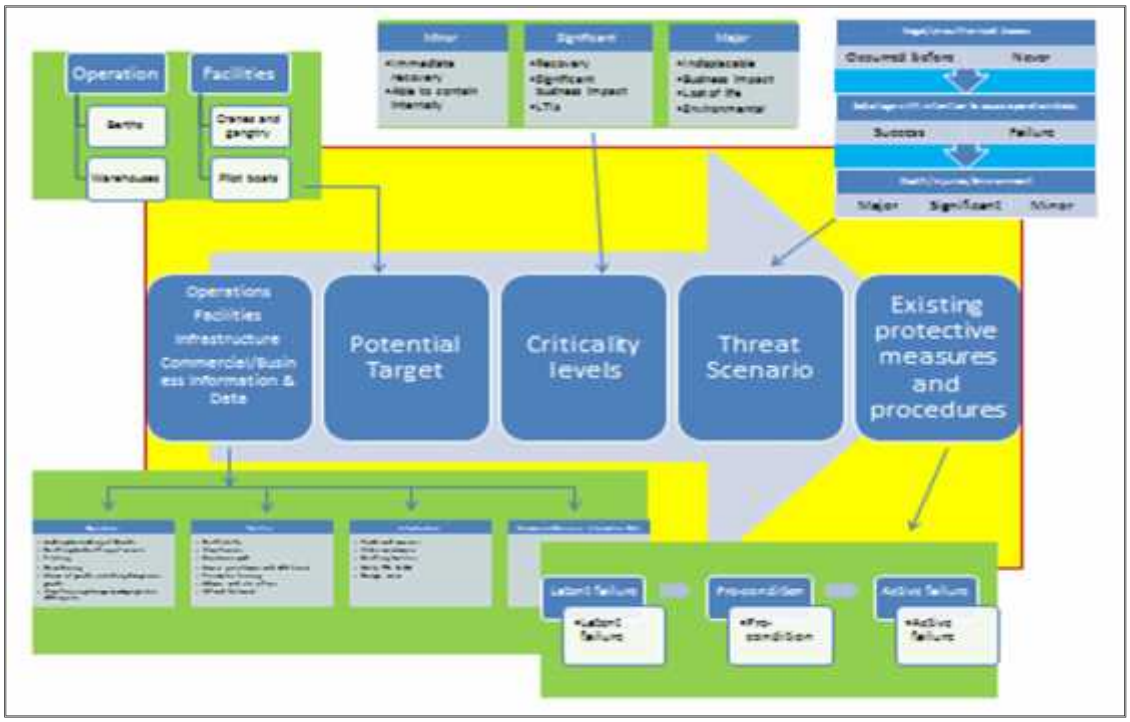

Figure 5 – Threat Identification Flow Diagram

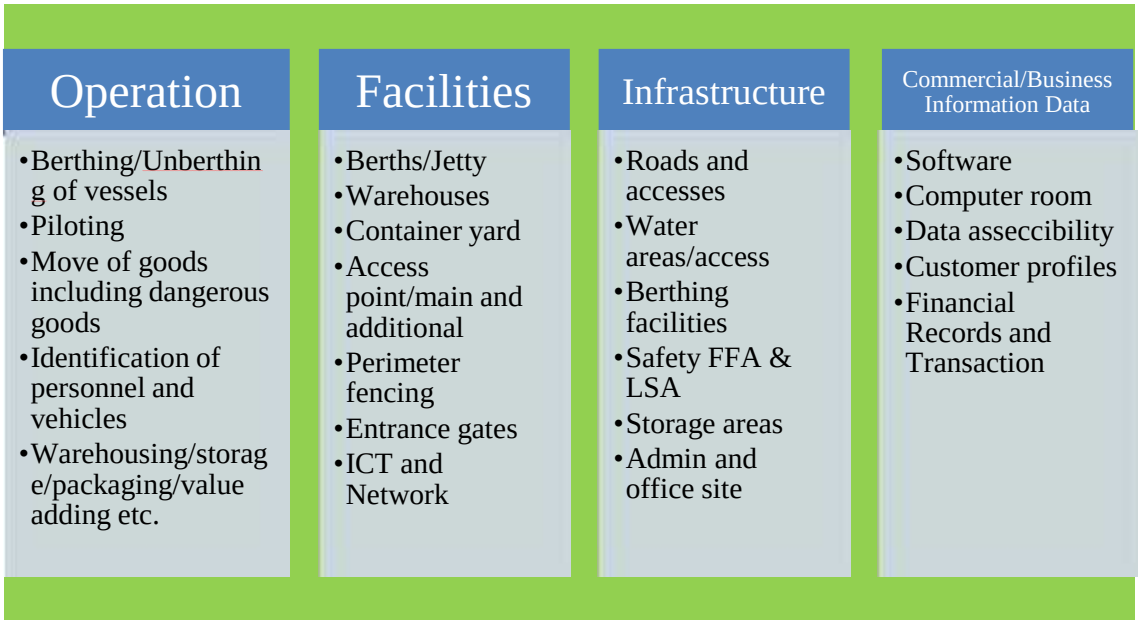

Figure 6 – Diagram of Port Activities

With reference to potential target (PT) in Figure 5, the PT for each activity is identified. PTs are refer to as key points or persons in the port and in the immediate environs, that may, if subject to an unlawful act, detrimentally impact on the security, safety of personnel or function

of the port (ILO, 2003). As each activity will require support of key points either in the form of fixed or moveable asset and human intervention, and any attempt to interrupt the routine operation of these assets or personnel would result in the deviations from expected outcomes. Thus any individual or group with the desire to cause undesired event would target these key points or personnel to achieve their objective.

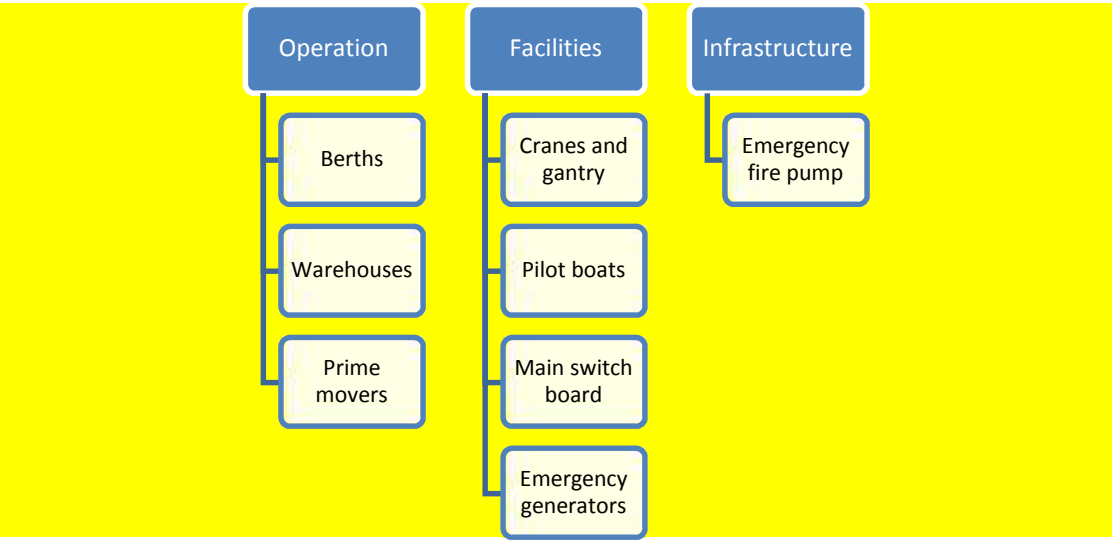

Figure 7 – Example of Potential targets for each port activity

Figure 7 above would reflect the potential targets identified that relates to the individual port activity. Each asset or personnel identified as potential target will be assessed in term of its criticality. Criticality is refer to the effect to the port in cases which these assets or personnel are being forcefully or unlawfully removed from the routine support element as well as the ability to recover if such incident occurred. The criticality of particular asset or personnel is classed under three categories, namely minor, significant and major. The measurement descriptors are illustrated in Table 8.

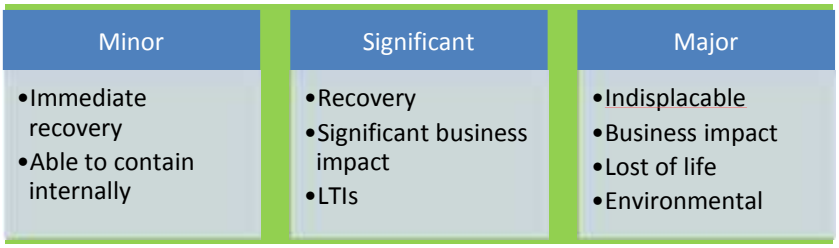

Figure 8 – Descriptor for criticality assessment

Table 8: Descriptor for Criticality Level

Table 8: Descriptor for Criticality Level

Criticality Level	Measurement criteria
Minor	Has the ability to recover with little intervention and can be brought back to operational status with shortest possible duration (Less than 24 hours) by mean of immediate

	replacement of identical unit, availability of secondary unit with similar capability or ability to restart/reset without requiring skill/ specialist intervention. Port facility has sufficient skilled personnel to ensure continuous operation. No lost time injury or significant damage.
Significant	Able to recover with the intervention of skilled specialist or replacement unit need to be brought in from external resources. Not able to recover within the same day of disruption, stoppages, may require repair work for damage target. Port facility will required to assemble external resources or specialist to assist in the recovery processes. Involved injury to personnel for period of more than one day.
Major	No ability to recover from the initial stoppages and require complete acquisition of the similar or identical unit from external sources. This may include complete build-up of the damage target. Involved loss of life.

The fourth box in the Figure 8 is the Threat Scenario. This box describe the possible scenario that can occure to the potential target if unlawful or undesire attempt is made on the potential target. This requirement is stated in Part B Section 15.9 to 15.11 of the Code.

For the purposes of evaluating the effectiveness of the security measures and procedures implemented by the port, the evaluation process include the information about past occurances experience by the facility and whether the attempt was successful or not. This is for the purpose of identify criticality of the potential target and any further improvement was made previously to enhance the measures and procedures. The process flow is taken from the concept of event tree analysis of possible causes to an accident and LOPA approaches in measuring the effectiveness of the barriers created in risk assessment. Figure 9 below is the combination of the event tree analysis and LOPA methodology. This step has to be taken as external criminal data from the relevant enforcement agencies are usually not obtainable due to it nature of confidentiality.

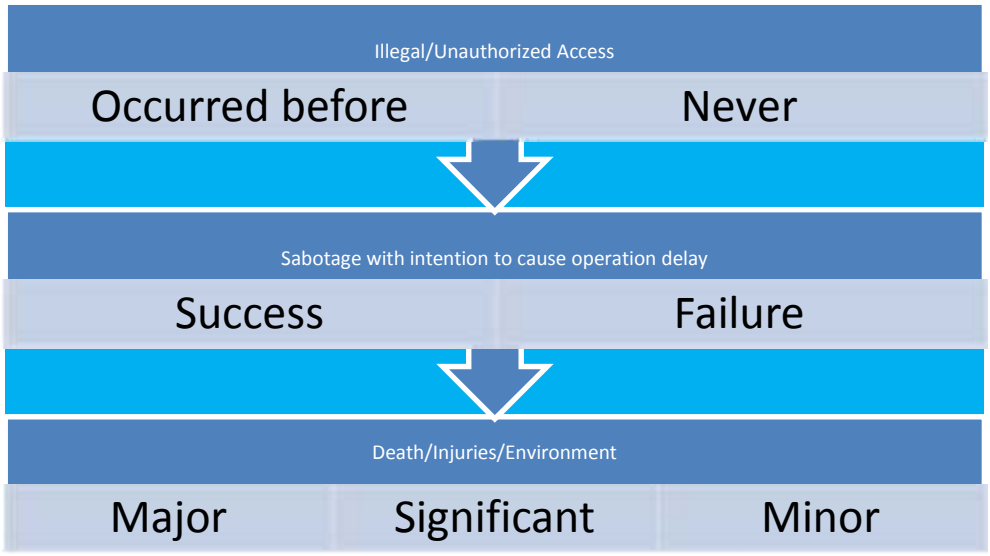

Figure 9: Process of identification of criticality level base on possible threat scenario

The final part of the identification of threat is to study the existing security barriers that created to protect the potential target. For this purpose, Tripod methodology is applied to identify possible failure in each security barrier and identify whether these possible failure in the security barriers were recognised by the management of the facility and preventive actions were in-place to ensure sufficient supports were provided to ensure these security barriers do not collapsed. The detailed process flow at this stage of evaluation is illustrated in Figure 10. For each security barriers in-placed to provide protection to the potential target, the possible immediate cause to the barrier failure is identified and this is known as active failure, Pre-condition is where the contributory factor/s that may cause the failure and the Latent failure is the root cause/s that contributed the this overall failure and in most cases that may be leading to the failure of management to provide effective support. Example of Pre-condition is the particular area was not identified as one of the patrol point in the overall patrol areas thus leading to the security leakage. Example of active failure is no patrol was made in the particular areas.

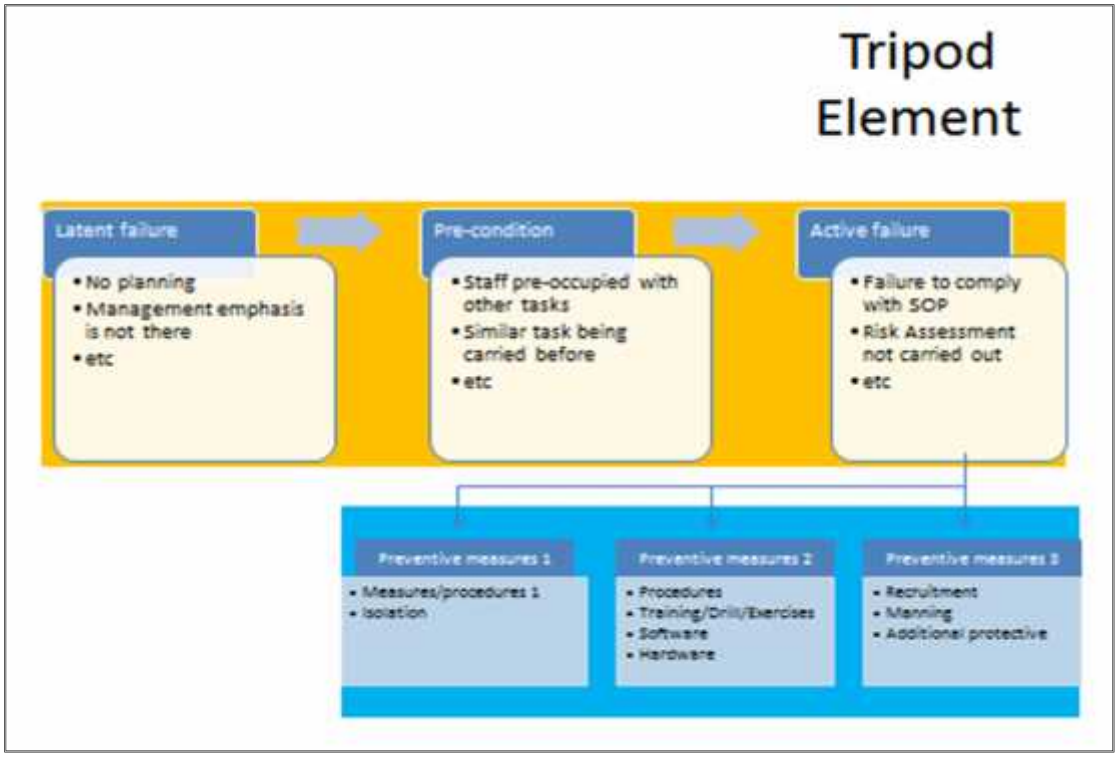

Figure 10 – Structure for identification of performance gaps

After the “Event”, all possible measures must be taken to mitigate the further development of the threats to ensure minimum loss of live or injuries, damage to the facility, control environmental degradation due to pollution as well as protection of the local surrounding. This stage of activities is known as Consequences management or Emergency Preparadeness (Part A, Section 16.3.5, ISPS Code, 2003). Similarly at this stage, the barriers must be in-placed to minimise the extent of damage. As the scope of the research will only focuses on the before event, this part of the research can be the next propose research.

The flow chart in figure 11 illustrated the entire process flow of the risk assessment.

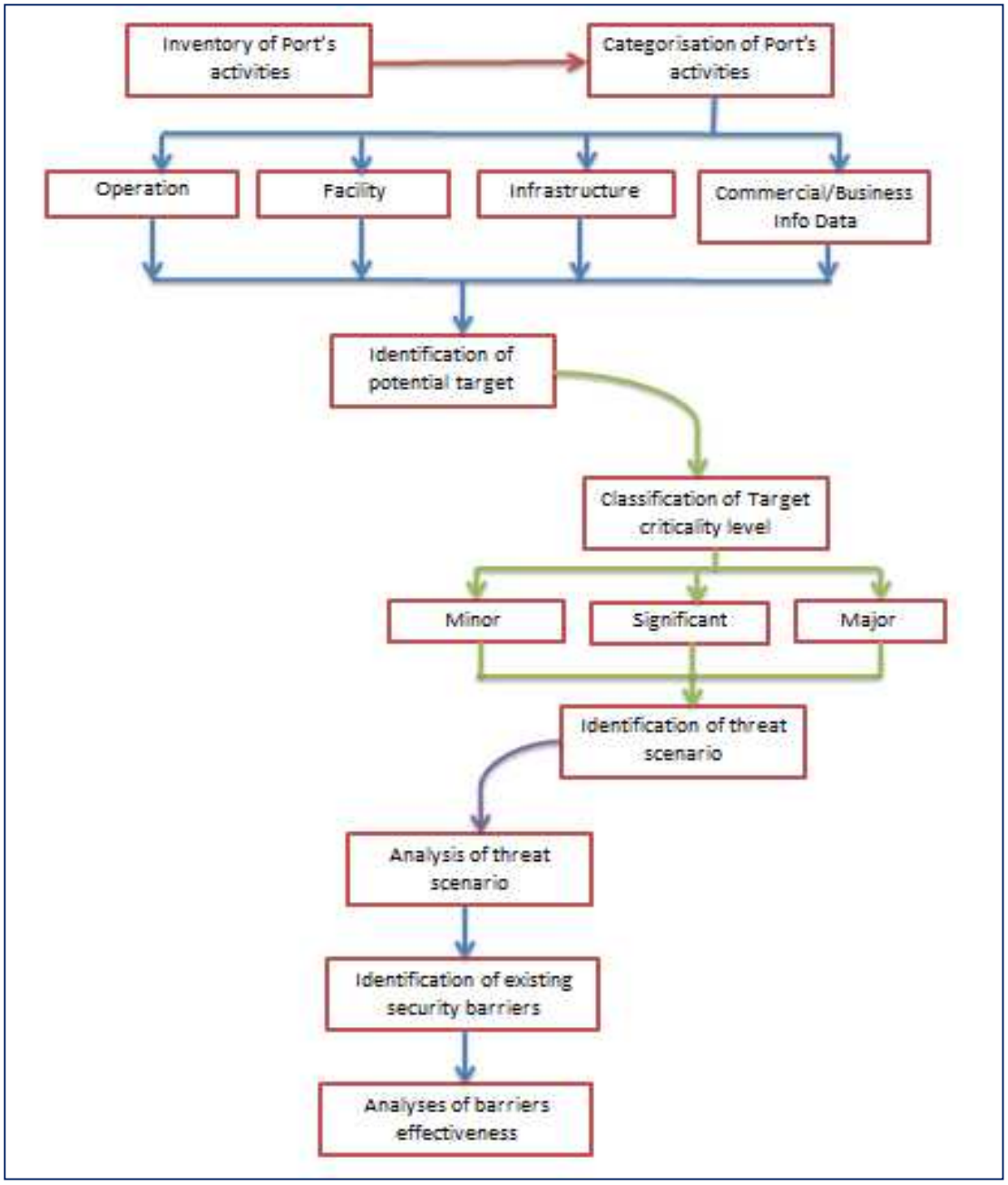

Figure 11 – Flow chart of the Assessment

The SPMS is the adaptation from the Bow tie approach which is commonly used in the management of safety related system with ability to provide total coverage in the reactive as well as proactive manner. The pro-active section lies on the left hand part of the Bow tie from the event section in the middle, and reactive section lies on the right hand of the event section as in Figure 3 above. The additional enhancement to the Bow tie is the inclusion of Threat Identification Flow which provided the structure flow of threat identification and classification in term of its criticality as well as identifying the existing security measures and procedures in place to ensure protections are accorded to the entities in the facilities. The whole process flow is illustrated in Figure 11.

9.0 Development of Security Measuring Tool

Measuring tool for the purpose of measuring the effectiveness of the security measures and procedures as stated in the PFSP which already put into placed and its full implementation are being monitored and tested on regular basis by the PFSO as required under the Code.

This measurement of effectiveness is critical as any weaknesses in the implementation will provide opportunities for external or internal parties with the opportunities to cause any undesired event to occur that would benefits the party's objective/s.

In determine the effectiveness of the ISPS Code implementation. The checklist contain in the Appendix 5 of MSC 1131 will be used as the reference for the research. MSC 1131 is the tool used at the moment for port facilities in Malaysia to examine the status of the ISPS Code implementation and it assist to identify any aspects of the ISPS Code that the port facility security officer can address to enhance the ISPS Code implementation process. As the scope of the research is limited to study the effectiveness of the security measures and procedures for the access control of the port facility, only 43 sub-parts or 47% out of total 92 will be exam in this research. The parts involved are:

1. Ensuring the performance of port facility security duties (ISPS Code Section A/14.2.1 and A/14.3) – Part A and B – 18 sub-parts;

2. Controlling access to the port facility (ISPS Code Section A/14.2.2, A/14.2.1 and A/14.3) – Part A and B – 16 sub-parts;

3. Monitoring of the port facility, including anchoring and berthing area(s) (ISPS Code Section A/14.2.3 and A/14.3) – Part A and B – 9 sub-parts.

The other parts that were not taken into consideration but can be taken in future research are:

4. Monitoring of restricted areas (ISPS Code Section A/14.2.4 and A/14.3);

5. Supervising the Handling of Cargo (ISPS Code Section A/14.2.5 and A/14.3);

6. Supervising the handling of ship's stores (ISPS Code Section A/14.2.6 and A/14.3);

7. Ensuring security communication is readily available (ISPS Code Section A/14.2.7 and A/14.3);

8. Training, Drills and Exercises (ISPS Code Section A/18); and

9. Miscellaneous.

Controlling access to the port facility and monitoring of the port facility, including anchoring and berthing area(s) are the 2 main parts above covered mainly the control of access to the port facility from the shore as well as from the water side which contributed the most in the implementation of security measures and procedures that must be stipulated in the PFSP. The part of ensuring the performance of the port facility security duties is included in the research as this support the implementation and execution of the security administration for the port facility.

The Tripod Risk Analysis approach is use as the tools to measure the effectiveness of the implemented security initiative as it provide an inclusive view of every aspect in term of mechanism of implementation as well as root causes of possible failure. The Tripod Beta

approach is favour in this research as it is a tool that provides a complete view of possible direct failure as well as indirect contribution to implementation of specific approach in accident investigation as well as in risk assessment as described by Hurst (2005), Cambon (2008) and Visser (1998), and supported by Turksema and Postman (2007).

One of the process involved in measuring the effectiveness of the security measures and procedures implemented by the port, is drills and exercises recommended in Section 18.3 of the Code. But in Part B Section 18.5, minimum recommended period of drill is atleast once every 3 months and for exercise (Part B, Section 18.6), one every calendar year with the distance between exercises not more than 18 months. Based on Part A Section 16.3 of the Code, there were altogether 15 areas that the PFSP must covered and in MSC circular 1131, there were altogether 93 sub-parts that must be dealed with by a port facility and instituted in the PFSP. Based on the minimum fulfillment of the Code requirement, it will take 23.25 years for a port facility to put these security measures and procedures into test to determine its effectiveness.

Tripod is the methodology which can be applied to identify possible failure in each security barrier and identify whether these possible failure in the security barriers were recognised by the management of the facility and preventive actions were in-place to ensure sufficient supports were provided. For each security barriers in-placed as barrier to provide protection to the potential target, the possible immediate cause to the barrier failure is identified and this is known as active failure, Pre-condition is where the contributory factor/s that may cause the failure and the Latent failure is the root cause/s that contributed the this overall failure and in most cases that may be leading to the failure of management to provide effective support or better known as root cause. This approach is recommended based on account that the major elements that is within the control of the port facility against any possible threat is its vulnerability and the raise or down grade of the vulnerability lies sole with the port facility as the first line of defence whereas intervention by government security agencies generally will be based on intelligent information received at the time and after event response, which would be too late in term of avoiding damages or the event occurrences. In most instances, single security measure will be able to provide solid security barriers against any possible threats and at the same time, any security barriers would require organization commitments to materialize it. These commitments will be based on the nature of barriers put in place. For example, if security personnel are position at the guardhouse to monitor the movement of vehicle accessing the facility and at the same time to ensure no unauthorized person able to gained access into the facility. The port facility need to ensure that the security personnel are trained in identifying and recognising behaviour of suspicious person or vehicles, parking bays are allocated outside the guardhouse to allow sufficient time for security personnel to verify the driver identification and contact relevant person in the facility without obstructing the incoming vehicles, physical barrier such as vehicle posts are positioned at the gate to inform approach vehicle that they have to stop and obtain permission before access, clear signage before the entrance to let the vehicle know that they are approaching a restricted are.

Table 5: Example of Tripod Methodology Adaptation to Proactive Assessment

Security Measure	Active failure	Pre-Condition	Latent Failure
Procedures to prevent unauthorized	• Training of security personnel	• Training need analysis	• Company security policy

person and vehicle accessing the port facility	• Vehicle waiting area • Guard post/barrier • Signage	• Threat and risk identification	• Management support

In the Tripod approach, the Active Failure is referred to the direct causes of particular accident and generally it associated with unsafe act or unsafe condition whereas Pre-Condition is associated with Personal Factor or Job Factor, and Latent Failure is the root cause leading toward the development of unsafe act or unsafe condition. Table 5 is the example of Tripod Methodology Adaptation to Proactive Assessment.

Table 6: Security Initiatives Effectiveness Measurement Criteria

ISPS Code Requirement (MSC Cir 1131)	**Active Failure**	**Pre-Condition**	**Latent Failure**
Ensuring the performance of port facility security duties (ISPS Code sections A/14.2.1and A/14.3)			
1. Does the port facility's means of ensuring the performance of all security duties meet the requirements set out in the PFSP for security level 1 and 2? (ISPS Code section A/14.2.1)	• Security assessment • Acceptable risk score • Barriers in placed • Clear documentation • Drills/exercises • Security awareness training	• Hazard and threat identification • Budget constraint • Lack of knowledge • PFSO competence	• Management support • Company security policy
2. Has the port facility established measures to prevent weapons or any other dangerous substances and devices intended for use against persons, ships, or the port, from entering the facility? (ISPS Code section A/16.3.1)	• Training on weapons recognition • Risk assessment • Drills/Exercises • Signages • Security personnel • Crew/visitor /contractor security pass • Vehicle pass • Documentation inspection criteria • Work/order manifest	• Hazard and threat identification • Assessment methodology • PFSO Competence • Budget constraint • Consequences management policy	• Management support • Company security policy

3. Has the port facility established evacuation procedures in case of security threats or breaches of security? (ISPS Code section A/16.3.5)	• Evacuation site • Staff awareness • Drills/Exercises • Security awareness training	• Threat identification • Site limitation • PFSO competency • Emergency response plan	• Management support • Company security policy
4. Has the port facility established procedures for response to an activation of a ship security alert system? (ISPS Code section A/16.3.14)	• Established contact point • Organizational structure • Job description • Drills/Exercises	• External contact • Emergency response plan • PFSO competency	• Management support • Company security policy
5. Has the port facility established the role and structure of the security organization? (ISPS Code paragraph B/16.8.1)	• Job description • Established contact point • Control and command centre • Reporting / Chain of command	• Human Resource structure • PFSO Competency • Employment terms	• Management support • Company security policy
6. Has the port facility established the duties and responsibilities for personnel with security roles? (ISPS Code paragraph B/16.8.2)	• Job description • Security training • Organizational structure • Line of reporting • Annual performance evaluation	• Documented HRM terms of employment • Organizational framework • Training budget	• Management support • Company security policy
7. Has the port facility established the training requirements for personnel with security roles? (ISPS Code sections A18.1, A/18.2, A/18.3 and paragraph B/16.8.2)	• Training need analysis • Training record book • Training schedule • Training feedback • Training evaluation	• Training budget • HRM training framework • Auditing • Hazard and threat identification	• Management support • HR planning • Company security policy
8. Has the port facility established the performance measures needed to assess the individual effectiveness	• Training need analysis • Training evaluation • Drills / exercises	• Training budget • HR development plan	• Management support • Company security policy

of personnel with security roles? (ISPS Code paragraph B/16.8.2)	• Annual performance management	• PFSO competency	
9. Has the port facility established their security organizations link with other national or local authorities with security responsibilities? (ISPS Code paragraph B/16.8.3)	• Organizational structure • Established contact point • Exercises	• Communication link • PFSO competency • Organizational hierarchy	• Management support • Company security policy
10. Has the port facility established procedures and practices to protect security-sensitive information held in paper or electronic format? (ISPS Code paragraph B/16.8.6)	• Physical site • Control of main keys • Spare keys management • Access record • Access list • Security awareness training	• Site location • Facility • PFSO Competency • Hazard and threat identification	• Management support • Company security policy
11. Has the port facility established procedures to assess the continuing effectiveness of security measures and procedures? (ISPS Code paragraph B/16.8.7)	• Drills/exercises • Review procedures • Internal audit • Review schedule • Security awareness training	• Assessment methodology • PFSO competency • Performance measurement	• Management support • Company security policy
12. Has the port facility established procedures to assess security equipment, to include identification of, and response to, equipment failure or malfunction? (ISPS Code paragraph B/16.8.7)	• Equipment performance criteria • Test record • Test schedule • Spares • Maintenance contract/record • Maintenance schedule	• Security risk methodology • PFSO competency • Security budget • Company maintenance policy	• Management support • Company security policy
13. Has the port facility established procedures governing submission and assessment of reports relating to possible breaches of	• Reporting form • Designated person – name • Job specification	• Feedback handling • Local community • Confidentiality	• Management support • Company security policy

security or security concerns? (ISPS Code paragraph B/16.8.8)	• Organization structure – external link • Established contact point		
14. Has the port facility established procedures to maintain and update records of dangerous goods and hazardous substances, including their location within the port facility? (ISPS Code paragraph B/16.8.11)	• Designated location on map • Dangerous good/ Hazardous substances records • Shippers contact link • Reporting procedures • Job specification • Patrol record / parameter	• Allocation for dangerous goods storage • Port design • Port business • PFSO knowledge	• Management support • Company security policy
15. Has the port facility established a means of alerting and obtaining the services of waterside patrols and search teams, to include bomb and underwater specialists? (ISPS Code paragraph B/16.8.12)	• Job specification • Patrol points • Patrol route • Patrol schedule • External contact point • External security contract agreement • Organizational structure	• Company HR policy • PFSO competency • Threat identification • Training budget	• Management support • Company security policy
16. Has the port facility established procedures for assisting, when requested, Ship Security Officers in confirming the identity of those seeking to board the ship? (ISPS Code paragraph B/16.8.13)	• Job specification • Contact point • Request form/record • Staff identification card • Communication pack • Stevedore manifest	• Training budget • Communication policy • Staff identification criteria • Hazards and threat identification	• Management support • Company security policy
17. Has the port facility established the procedures for facilitating shore leave	• Crew/Agent contact • Crew pass	• Crew shore leave policy/ restriction	• HSE policy • Administration requirement

for ship's crew members or personnel changes? (ISPS Code paragraph B/16.8.14)	• Crew change manifest • Shore leave record • Identification verification criteria • Ship crew list	• Safety restriction • Facilitation	• Company security policy
18. Has the port facility established the procedures for facilitating visitor access to the ship, to include representatives of seafarers welfare and labour organizations? (ISPS Code paragraph B/16.8.14)	• Registration lists • Security check list for visitor • Vehicle pass • Visitor pass	• HSE/Safety restriction • Verification criteria	• Visiting policy • Safety/HSE policy • Company security policy
Controlling access to the port facility (ISPS Code sections A/14.2.2, A/14.2.1 and A/14.3)			
19. Does the port facility's means of controlling access to the port facility meet the requirements set out in the PFSP for security level 1 and 2?	• Risk assessment's risk score • Drills and exercises • Job specification • Training record • Organization structure • Signages • Security procedures	• Threat identification • PFSO competency • Training budget	• Management support • Company security policy
20. Has the port facility identified the appropriate location(s) where security measures can be applied to restrict or prohibit access. These should include all access points identified in the PFSP at security level 1 and 2? (ISPS Code paragraphs B/16.11, B/16.19.1)	• Access barrier • Perimeter fencing • Perimeter lighting • Security patrol • Fence barrier • Road/Speed breakers • Access identification	• Check point criteria • Criticality status of facilities • PFSO competency • Threat identification • Risk assessment	• Company security policy • Management support

	• Visitor/Crew/ Contractor pass • Vehicle pass • Search criteria		
21. Does the port facility specify the type of restrictions or prohibitions, and the means of enforcement to be applied at all access points identified in the PFSP at security level 1 and 2? (ISPS Code paragraphs B/16.11 B/16.19.2, B/16.19.3)	• Access barrier • Identification system • Vehicle waiting area • Crew/Visitor retention area • Mooring gangs • Pilot responsibility • Contact point	• Threat identification • Risk assessment • Criticality criteria • PFSO competency	• Company security policy • Management support
22. Has the port facility established measures to increase the frequency of searches of people, personal effects, and vehicles at security level 2? (ISPS Code paragraph B/16.19.4)	• Crew/Visitor holding area • Vehicle holding area • Drills/Exercises • Trainings • Signages	• Threat identification • Risk assessment • Search criteria	• Company security policy • Management support • Administration requirement
23. Has the port facility established measures to deny access to visitors who are unable to provide verifiable justification for seeking access to the port facility at security level 2 (ISPS Code paragraph B/16.19.5)	• Entry criteria • Drills/exercises • Awareness & Trainings • Work/Order manifest • Organization links • Communication/Contact points • External contact point	• Information exchange • External contractors criteria • Visitor restriction	• Company security policy • Management support • Access policy
24. Has the port facility established the means of identification required to access and remain unchallenged within the port facility?	• Crew/Visitor/ Contractor/Staff pass • Vehicle Pass • Awareness & Training	• Visitor/Contractor/ Crew access criteria	• Company security policy • Access policy

(ISPS Code paragraph B/16.12)	• Drills / Exercises • Reporting point • Work/order manifest	• Access control system -- identification	• Management support
25. Does the port facility have the means to differentiate the identification of permanent, temporary, and visiting individuals? (ISPS Code paragraph B/16.12)	• Crew/Visitor/ Contractor/Staff identification tag • Registration form • Internal movement guidelines • Security awareness training • Drills and Exercises • Contact/reporting point	• Identification tag coding • Access criteria • Training criteria	• Company security policy • Access policy • Management support
26. Does the port facility have the means to verify the identity and legitimacy of passenger boarding passes, tickets, etc? (ISPS Code paragraph B/16.12)	• Crew/Visitor/contractor manifest • Contact point • Access criteria • Drills and Trainings • Crew/Passenger passes • Signages	• Access control system • Declaration of Security – Identification • Ship passengers boarding identification requirement	• Ship's passenger boarding procedures • Access control policy
27. Has the port facility established provisions to ensure that the identification systems are regularly updated? (ISPS Code paragraph B/16.12)	• Passes dateline • Access control criteria • Contact point • Entry access documentation • ID issuance record • Visitor/Crew/ Contractor data bank	• Access control system maintenance contract • Data updating procedures • Software contract	• Access control policy • Management support

28. Has the port facility established provisions to facilitate disciplinary action against those whom abuse the identification system procedures? (ISPS Code paragraph B/16.12)	• Employment terms and conditions • Employee ID and attendance procedures • Domestic inquiry • Industrial relation • HR Management • Awareness Trainings • Signages	• Terms of service • Access control criteria	• Employment policy • Management support
29. Has the port facility created procedures to deny access and report all individuals who are unwilling or unable to establish their identity or purpose for visit to the PFSO and to the national or local authorities? (ISPS Code paragraph B/16.13)	• Access/entry criteria • Drills and exercises • Trainings • External contact point • Job specification • Temporary holding areas • Access control system	• PFSO competency • Access control criteria • Threat assessment and identification • External communication procedures • Visitor/Crew/Contractor access criteria	• Access control policy • Management support
30. Has the port facility identified a location(s) for searches of persons, personal effects, and vehicles that facilitates continuous operation, regardless of prevailing weather conditions? (ISPS Code paragraph B/16.14)	• Visitor holding area • Vehicle detention area • Job specification • Search procedures • External contact point • Access manifest • Drills and Trainings	• Access control criteria • Threat assessment and identification • Availability of space • Legal requirement	• Access control policy • Management support • Legal status of the facility

31. Does the port facility have procedures established to directly transfer persons, personal effects, or vehicles subjected to search to the restricted holding, embarkation, or vehicle loading area? (ISPS Code paragraph B/16.14)	• Designated vehicle holding area • Designated holding area • Job specification • Drills • Trainings • External contact point • Search criteria	• Threat assessment and identification • PFSO competencies • Legal requirement	• Access control policy • Management support • Legal status of the facility
32. Has the port facility established separate locations for embarking and disembarking passengers, ship's personnel, and their effects to ensure that unchecked persons do not come in contact with checked persons? (ISPS Code paragraph B/16.15)	• Access/Entry criteria • Facilitation requirement by custom & immigration • Passenger waiting area • Check point • Holding area • Passenger barriers • Signages • Trainings and Drills • Passengers holding area	• Passenger engagement criteria • Immigration legal requirement • Threat assessment • Passengers monitoring	• Access control policy • Management support • Legal status of the facility
33. Does the PFSP establish the frequency of application of all access controls? (ISPS Code paragraph B/16.16)	• Perimeter patrol schedule • Reporting/Clocking points • Access passes • Physical barriers • Awareness trainings	• Access control criteria • Threat assessment	• Access control policy • Management support
34. Does the PFSP establish control points for restricted areas bounded by fencing or other barriers to a standard which is approved by the national government? (ISPS Code paragraph B/16.17.1)	• Perimeter fencing • Perimeter lighting • Access barrier – Gate • Training & Drills	• Maintenance schedule • Threat identification and risk assessment • PFSO competency	• Company security policy • Access control policy • Legal requirement

	• Signages • Access point classification	• Access control criteria • Training need analysis	• Management support
35. Does the PFSP establish the identification of and procedures to control access points not in regular use which should be permanently closed and locked? (ISPS Code paragraph B/16.17.7)	• Access point classification • Access identification • Patrol points • Patrol criteria • Trainings • Lighting • Perimeter fencing • Signages	• Threat identification and risk assessment • Access control criteria • PFSO competency	• Access control policy • Company security policy • Management support
Monitoring of the port facility, including anchoring and berthing area(s) (ISPS Code sections A/14.2.3 and A/14.3)			
36. Does the facility's means of monitoring the port facility, including berthing and anchorage area(s) meet the requirements set out in the PFSP for security level 1 and 2?	• Risk Assessment risk score • Threat scenario • Patrol points • Lighting • Training and Drills • Signages • Patrol schedule • Vessel reporting criteria	• Risk and threat identification • Training need analysis • PFSO competency • National requirement • Security budget	• Company security policy • Management support
37. Does the port facility have the capability to continuously monitor on land and water the port facility and its nearby approaches? (ISPS Code paragraph B/16.49)	• Risk assessment risk score • Threat scenario • Patrol point • Vessel monitoring & reporting criteria • Patrol schedule • Berth lighting	• Risk and threat identification • Training need analysis • PFSO competency • Security budget	• Company security policy • Management support

	• Training and Drills		
38. Which of the following means are employed to monitor the port facility and nearby approaches? (ISPS Code paragraph B/16.49) A. Patrols by security guards B. Patrols by security vehicles C. Patrols by watercraft D. Automatic intrusion-detection devices E. Surveillance equipment	• Patrol schedule • Risk assessment and score • Patrol point • Lighting • Vessel monitoring / reporting criteria	• Threat and risk identification • PFSO competency • Maintenance contract • Training need analysis	• Company security policy
39. If automatic intrusion-detection devices are employed, do they activate an audible and/or visual alarm(s) at a location(s) that is continuously monitored? (ISPS Code paragraph B/16.50)	• Activation criteria • Manufacturing maintenance guideline • Job specification • Trainings • Spares • Responses	• Maintenance contract • Threat and risk assessment • Training need analysis • Access control criteria • Security budget	• Security policy • Management support
40. Does the PFSP establish procedures and equipment needed at each security level? (ISPS Code paragraph B/16.51)	• Activation criteria • Manufacturing maintenance guideline • Job specification • Trainings • Maintenance contract • Spares • Responses	• Threat and risk assessment • Threat identification • PFSO competency • Training need analysis	• Security policy • Management support
41. Has the port facility established measures to increase the security measures at security level 1 and 2 (ISPS Code paragraphs B/16.51,	• Job specification • Resource allocation • Response criteria • Training	• Threat and risk assessment • Threat identification • PFSO competency	• Security policy • Management support

B/16.53.1, B/16.53.2 and B/16.53.3) A. Increase intensity and coverage of lighting and surveillance equipment B. Increase frequency of foot, vehicle & waterborne patrols C. Assign additional personnel D. Surveillance	• Drills & Exercises • Communication link • Contact point	• Training need analysis	
42. Does the PFSP establish procedures and equipment necessary to ensure that monitoring equipment will be able to perform continually, including consideration of the possible effects of weather or power disruptions? (ISPS Code paragraph B/16.51)	• Manufacturer guidelines • Drills and exercises • Training • Job specification • Organizational link • Test record and log • Equipment specification	• Threat and risk assessment • Maintenance contract • Training need analysis • PFSO competency • Maintenance schedule	• Security policy • Maintenance policy • Management support
43. Does the port facility have adequate illumination, to allow for detection of unauthorized persons at or approaching access points, the perimeter, restricted areas and ships, at all times including the night hours and periods of limited visibility? (ISPS Code paragraph B/16.49.1)	• Risk score • Perimeter lighting • Maintenance contract • Drill and exercises • Training • Job specification	• Threat and risk assessment • Threat identification • Training need analysis • Maintenance schedule	• Security policy • Maintenance policy • Management support

Table 7 is the measurement tool developed for the purpose of measuring the effectiveness of the implementation of the PFSP for port facility. The table is divided into 4 columns with the column on the left taken directly from the Appendix 5 of MSC 1131 covering the 3 major parts of the PFSP and the remaining are subdivided into 3 columns coincide with the Tripod Risk Analysis model of “Active Failure”, “Pre-Condition” and “Latent failure”.

Table 7: FCF Checklist

FCF Checklist	Failure Contributory Factors
ISPS Code Requirement (MSC Cir 1131)	Active Failure Pre-Condition Latent Failure

Ensuring the performance of port facility security duties

(ISPS Code sections A/14.2.1and A/14.3)

(a)

Does the port facility's means of ensuring the performance of all security duties meet the requirements set out in the PFSP for security level 1 and 2?

(ISPS Code section A/14.2.1)

(b) Active Failure	Pre-Condition	Latent Failure
• Security threat and assessment • Acceptable risk score • Barriers in placed • Clear documentation • Drills/exercises • Security awareness training	• Hazard and threat identification • Budget constraint • Lack of knowledge • PFSO competence	• Management support • Company security policy

(c)

Evidence:

1. TRAM assessment contain percentage of acceptable risk score to indicate the level where further mitigation procedures/strategies are not required;
2. Availability of physical barrier in placed such as fencing, perimeter lighting, patrol schedule including at level 1 and 2, its frequency of patrol;
3. Confidentiality of M/PFSP including its physical location, and control of access to the plan;
4. Frequency of security inspection and check including random sampling reflected in term of percentage of vehicles check as well as type of vehicles;
5. Security awareness training for all port personnel where evidence are available through training record, schedule and modules covered;
6. Competency assessment through participation in the drill, exercises and periodical evaluation to continuously evaluate performance of all staff designated with security duties;
7. M/PFSO and support staff training ,drill and exercises;
8. Security and emergency response flow chart detailing contact list, contact point and external security assistance availability and contact including flow chart display in the control room for easy reference.

(d) Remarks:

0	1	2	3

The second column from the left of the table 7 are the indicators of the physical or documentary evidence that the port facility must have in place to ensure effectiveness of the specific initiative that required to be enforced to ensure the security integrity of the port facility. Failure to have it in place could lead to failure of effective implement of specific security measures and procedures in compliance to the requirement of the Code. Column 3 reflects the circumstances of failure to put the initiatives into place and column 4 is the probable root causes that resulted in the initiatives were left out and not being focuses on.

This tool will allow the PFSO to determine the initiatives required to ensure effectiveness of specific measures and procedures by obtain the necessary support but and also allow the PFSO determine the further initiative need to support the implementation of an effective security measures.

To facilitate ease of measurement of the security implementation, the rulers in Table 7 are converted into single A4 page, which is name as Failure Contributory Factor (FCF) Checklist. This checklist content comprises of the reference to ISPS Code Requirement based on MSC

Circular 1131, the ISPS Code descriptor with reference section of the Code including the code requirement below it and this is reference to MSC Circular 1131 (Appendix 5), and finally the three column namely active failure, pre-condition and latent failure. A total of 43 areas of security initiatives will be observed during the field research.

9.1 Effectiveness Measurement

For the purpose of determination of the level of effectiveness, a percentage compliance measurement system is devised to facilitate the Port Facility Security Officer to determine the overall level of effectiveness on the security measures and procedures implemented.

In the Failure Contributory Factor Checklist, a total of 43 areas of security initiatives and these 43 areas are grouped into 3 separate groups in the Table 8 below.

Table 8: Security Initiatives Grouping

Sr. No	**Grouping**	**Number of Security Initiatives**
1	Ensuring the performance of port facility security duties.	18
2	Controlling access to the port facility	17
3	Monitoring of the port facility, including anchoring and berthing areas	8

A point system is allocated for each security initiatives as in Table 9.

Table 9: Points Allocation Criteria

Compliance Points	Criteria for the points
0	Initiatives recorded in the PFSP but no evidence of physical/documentary support visible. Management support is absent.
1	Less than 50% of the security activities in Active Failure column are present with specific areas of concern for further improvement. Evidence available in physical/documentary forms.
2	50% and more of the security activities in Active Failure column exist and without specific area/s of concern. Evidence available in physical/documentary forms.
3	100% of the security activities in Active Failure with further enhancement initiatives.

With reference to table 8 and 9 above, a percentage weightage is allocated for each security initiatives implemented and the weightage is divided according to grouping as well as overall. The purpose of dividing the initiatives in grouping to allow for better focus during improvement processes. The overall weightage calculation determination is as per table 10 below.

Table 10: Weightage Calculation

Group	Number of Security Initiatives	Maximum Points	Weightage Calculation (%)
1	18	3	Σ(Points Earned)/ (18x3) x 100 = X
2	17	3	Σ(Points Earned)/ (17x3) x 100 = Y
3	8	3	Σ(Points Earned)/ (8x3) x 100 = Z
Overall			(X + Y + Z)/3 = Overall Performance in %

10.0 Data Collection and Analysis -- Outcome of Field Test on Port A

This port specialises on handling of container cargoes including hazardous cargoes in container. This port is in existence in Malaysia for over 15 years and is one of the container ports in Malaysia that has the highest throughout per annum. The port complied with the requirement of ISPS Code since 1 July 2004 and has already undergoes 1st renewal verification by Malaysia Marine Department and next renewal verification will be in 2014. The port has dedicated security department headed by a senior manager.

The following observations were noted during the field test on the FCF Checklist applicability:

a. The lists of deliverables in the active failure, pre-condition and latent failure columns need further explanation to assist the PFSO in tracing the support documents as it do not reflect the actual operational documents practice by the port facility and the coding of the documents are based on port specific coding system;

b. The criteria for staff, visitor and ship crew are not applicable as the port facility practices issuance of pass based on duration of stay in the port facility;

c. Some of the deliverables are not applicable as for example this port do not handle passenger;

d. The checklist able to link a particular element of security equipment failure to lack of management involvement to effort to ensure immediate rectification is made on this equipment due to various level of approval are needed from separate department due to company policy of restriction the responsible department to deal directly with the vendor based on level of urgency and its criticality;

e. The port security assessment adapted the methodology recommended by the International Labour Organization's Code of Practice on Security in Port (2003) and there is no actual percentage on acceptable risk score to reflect the criticality level of each entity to be protected;

f. The checklist able to detect some critical entities being left out in the assessment such as protection for water front area.

Table 11: Level of Compliance Score for Port A

Group	Number of Security Initiatives	Maximum Points	Weightage Calculation
1	18	3	34/ (18x3) x 100 = 62.9%
2	17	3	32/ (17x3) x 100 = 62.7 %
3	8	3	14/ (8x3) x 100 = 58.3%
Overall			(62.9 + 62.7 + 58.3)/3 = 61.3% Performance in %

With reference to Table 11, overall compliance score for Port A is 61.3% where it is noted that the port fully complied with the MSC 1131 requirement for access control, restricted areas as well as the management of the security and at the same time leaving more room for improvement.

Outcome of Field Test on Port B

This is one of the oldest port in Malaysia and the port handle multiple type of cargoes ranging from break bulk cargo, containers to liquid cargoes in bulk and hazardous cargo. This port has the capacity to handle vessel on domestic voyage right up to vessel on unlimited voyage trade. The compliance to the requirement of the ISPS Code is under the purview of the Safety and Security Department under the stewardship of a Senior Manager. Full co-operation was extended by the Senior Manager for the conduct of the field studies as well as drive through visit to the entire perimeter of the port facility. The port complied with the Code requirement since 2004 and the compliance endorsement was issued by Malaysia Marine Department.

The following observations were noted during the field test on the FCF Checklist applicability:

a. The lists of deliverables in the active failure, pre-condition and latent failure columns need further explanation to assist the PFSO as the support documentations were not named as per checklist and at the same time PFSO has not access to certain support documents as it is residing at other department such as maintenance record of certain security equipment such as Close Circuit Television Camera (CCTV) as well as maintenance contract;

b. The criteria for staff, visitor and ship crew passes are issue in electronic format and coding of the passes can be accessible electronically;

c. Some of the deliverables are not applicable as for example this port do not handle passenger;

d. The checklist able to link a particular element of security equipment failure to lack of management involvement to effort to ensure immediate rectification is made on this equipment due to various level of approval are needed from separate department due to company policy

of restriction the responsible department to deal directly with the vendor based on level of urgency and its criticality. This observation is similar to the first port;

e. The port security assessment adapted the methodology recommended by the International Labour Organization's Code of Practice on Security in Port (2003) and there is no actual percentage on acceptable risk score to reflect the criticality level of each entity to be protected. This approach is very common to all ports in Malaysia as it is a recommended approach by Malaysia Marine Department;

f. The checklist able to detect some critical entities being left out in the assessment such as protection for water front area;

g. The checklist able to detect several weaknesses in the implementation of the Code especially the training provided for security personnel is very much based on the schedule training programme set up by the port and not through the actual need of the port with reference to the Training Need Analysis;

h. Vendors site were not included in the security control even-though they are located within the premise of the port facility.

Table 12: level of Compliance Score for Port B

Group	Number of Security Initiatives	Maximum Points	Weightage Calculation (%)
1	18	3	30/ (18x3) x 100 = 55.6%
2	17	3	34/ (17x3) x 100 = 66.7%
3	8	3	17/ (8x3) x 100 = 70.8%
Overall			(55.6 + 66.7 + 70.8)/3 = 64.4% Performance in %

With reference to Table 12, overall compliance score for Port B is 64.4% where it is noted that the port fully complied with the MSC 1131 requirement for access control, restricted areas as well as the management of the security and at the same time leaving more room for improvement.

11.0 Failure Contributory Factor Checklist Review

The field test carryout on the use of FCF Checklist noted that the checklist failed to facilitate the PFSO to carryout self-assessment of the effectiveness of the implementation of the security measures and procedures required under the Code even-though the checklist able to detect weaknesses in the implementation. The ability to detect these weaknesses lies most of the time on the knowledge acquired by the researcher based on his working experience in the field which is not the objective of this research.

The FCF Checklist must be able to facilitate the PFSO in carryout the self-assessment without the aids of external party and it should be able to provide relationship or link to the requirement under the Code. For the purpose the FCF Checklist was further enhanced by incorporating additional guidance note at the beginning of the checklist and the Criteria for FCF was included as an accompany document which will allow the PFSO to use as reference to the compliance to the Code.

For the FCF Checklist, it is further divided to 4 sections named as (a), (b), (c) and (d). These sub-divisions is to allow the PFSO to cross reference between the guideline and individual table. The sub-section (a) is remained the same which is the measurement criteria set out in MSC Circular 1131. The sub-section (b) comprises the 3 column which contain the bullet points checklist on the support documents, measures, processes and procedures in Active Failure column follow by the Pre-Condition column which contained the bullet points checklist on the contributory factor the lead to the Active Failure and finally the Latent Failure column which reflect possible root cause to the failure to effectively implement the measures and procedures as stipulated in the Code. The sub-section (c) is a new sub-section incorporate into the checklist, this sub-section provide further elaboration on the nature of the support documentations needed during the self-assessment process by the PFSO. This additional sub-section was incorporated to remove the difference in the coding or naming of the support documents which may varies with difference port facility. It is self-explanatory and do not need further guidance to the PFSO. The sub-section (d) is blank so as to provide space for the PFSO to insert remarks of any observations or additional action required as after audit follow-up action/s.

12.0 Conclusion

The conclusion is that the initial FCF Checklist is able to detect weaknesses in the effective implementation of the security measures and procedures covering for access control and restricted areas. Due to varying practices in these ports under the study, the checklist points caused some level of mis-interpretation by the PFSOs. Modifications are made to further facilitate the effectiveness of the checklist so as to allow the PFSOs to carry out the assessment unaided.

Nevertheless it is still vital that certain level of basic knowledge on the assessor such as the requirement of the Code itself and, knowledge and understanding on the individual port operations and its linkage would further facilitate in the execution of the checklist.

The main challenge encountered during the data gathering processes is the confidentiality nature of the PFSP which do not reflect the port specific checklist of the FCF Checklist. It is the researcher's view that if the FCF Checklist could be made port specific, it will be able to further detect weakness in the specific area thus placed better focuses on root cause determination and better manage corrective action.

In conclusion, the SPMS system can be used to measure the completeness of the security threats for a port facility and its success depend mainly in the Port Facility Security Officer and his/her assessment team to take into consideration the totality of the port facility operation and not solely focuses on nature of threat alone but the associate entities that critical to the port operation.

The FCF Checklist able to support the PFSO in carryout his/her security measures and procedures depend mainly on his/her ability to proactively determine it weaknesses as well as opportunities for improvement.

References:

Artley W and Stroh S. (2001), Establishing an Integrated Performance Measurement System (Volume 2), Oak Ridge Institute for Science and Education, Retrived 18.11.2008, http://www.orau.gov/pdm/pdmhand book/volume%202/pdf.

Brooks M. R and Pelot R., *Port Security: A Risk Based Prespective*, Maritime Safety, Security and Piracy., Informa Law, Mortimer House, London., 2008., pg 196, 198, 201to 204;

Baumgartner M., *Performance Measurement in ATM*? A Necessity or A Hindrance to Efficient ATCD Work?, International federation of Air traffic Controller association, USA, Sept. 2006, Pg.4;

Bellamy L. J. et al.,*Storybuilder – A Tool for the Analysis of Accident Report*, Reliability Engineering and System Safety 92 (2007) 735-744, The Netherland, www.elsevier.com. ,June 2006;

Biringerl B. & Danneels J. J., *Risk Assessment Methodology for Protecting Our Critical Physical Infrastructures***,** 1Systems Analyst, Systems Analysis and Development, Dept. 5845, Sandia National Laboratories, Albuquerque, NM 871 85-0759

Bridges W & Clark T., *Key Issues with Implementing LOPA (Layer of Protection Analysis) – Perspective from One of the Originators of LOPA*, 5th Global congress on Process Safety, American Institute of Chemical Engineerings, New York, New York, 2009, Pg 5;

Brooks M. R. and Pelot R., *Port Security: A Risk Based Perspective*, Chapter 11 Maritime Safety, Security and Piracy, Informa Law Mortimer House, London, 2008, Pg 196;

Cambon J., Guarinori F. & Groenweg J., *Towards A New Tool for Measuring Safety Management Systems Performance*, Centre for Safety Research, University of Leidan, Netherlands, 2008;

CCPS. (1993), *Guidelines for Auditing Process Safety Management Systems*., American Institute of Chemical Engineers, Wiley Interscience, New York, New York 10017, US;

Centre for Chemical Process Safety, *Guidelines for Auditing Process Safety Management System*, American Institute of Chemical Engineers, Wiley Interscience Inc, New York, 1993, Pg. 6;

Certo S. C., *Modern Management*, Prentice Hall, New Jersey, USA, 2000

Clifton A., *Accident Investigation Using EEFTA*, Proceedings of the 18th International System Safety conference 2000, The Boeing Company, Seattle, Washington, 2000

Eliana F., *Risk Assessment and Risk Management under the Cartagena Protocol on Biosafety, AAssPPaacc JJ.. MMooll.. BBiiool.l .B Bioitoetcehcnhonl.o 2l.0 V0o9l. 16 (3), 2008 Running title 1 Vol. 17 (3) : 97-98*

FATF Secretariat**.,** *Money Laundering & Terrorist Financing Risk Assessment Strategies*, FATF Secretariat, OECD, 2 rue André Pascal 75775 Paris Cedex 16, France, 18 June 2008

Fletcher W J., *The application of qualitative risk assessment methodology to prioritize issues for fisheries management*, ICES Journal of Marine Science, 62: 1576e1587 (2005) : WA Marine Research Laboratories, Department of Fisheries, PO Box 20, North Beach 6920, WA, Australia

General Accounting Office**,** *Information Security Risk Assessment GAO Practices of Leading Organizations A Supplement to GAO's May 1998 Executive Guide on Information*, GAO, November 1999, USA

Gordon R., Flin R and Mearns K., *Designing and evaluating a human factors investigation tool (HFIT) for accident analysis*, Industrial Psychology Research Centre, University of Aberdeen, Scotland 2005

Hale A . and Baram M., *Safety Management, The Challenge of Change*, Elsevier Science Ltd, UK, 1998;

Hopkin P., *Holistic Risk Management in Practice*, Witherby & Co. Ltd, London, 2002

Hughes P & Ferrett E, *Safety Measurement*, Introduction to Health and Safety At Work, Elsevier Limited, London, 2003, Pg 102;

Hayward, B.J., Lowe, A.R., & Branford, K., *Creating Safer Systems: Proactive Integrated Risk Assessment Technique*, Paper presented at the 28th Conference of the European Association for Aviation Psychology, Valencia, Spain, 27-31 October 2008;

Hurst S. & Lewis S., *Lessons Learned from Real World Application of Bow-Tie Method*, Risktec Solutions Limited, United Kingdom, www.risktec.co.uk., February 2005;

International Labour Organization, *Code of Practice on Security in Ports*., IMO-ILO Tripartite Meeting of Experts on Security, Safety and Health in Ports., Geneva, 2003, page 28 to 36;

International Maritime Organization, ISPS Code., International Ship & Port Facility Security Code and SOLAS Amendments 2002, IMO, 2003 London. Page 6,7, 20 & 21;

International Maritime Organization, *Appendix 2, Interim Guidance on Voluntary Self-Assessment by SOLAS Contracting Governments and By Port Facilities*., MSC/Circ. 1131., IMO, London, 14 December 2004., Pg 5 to 14;

ISO., *ISO 28000 Specification for Security Management Systems for the Supply Chain*., ISO 28000:2007(E), International Organization for Standardization, Geneva, 2007., Retrieved 07.07.2008., www.sname.org;

. ISO., *ISO 28001 Security Management Systems for the Supply Chain – Best practices for implementating supply chain security, assessments and plans – Requirements and guidance*., Draft International Standard ISO/Dis 28001, International Organization for Standardization, Geneva, 2007., Retrieved 07.07.2008., www.sname.org;

ISO., *ISO 20858 Ships and marine technology – Maritime port facility security assessments and security plan development*., Draft International Standard ISO/DIS 20858, International Organization for Standardization, Geneva, 2007., Retrieved 07.07.2008., www.sname.org;

ISO., *ISO 28004 Security Management Systems for the Supply Chain – Guidelines for the implementation of ISO 28000*., ISO 28004:2007(E), International Organization for Standardization, Geneva, 2007., Retrieved 07.07.2008., www.sname.org;
ISO., *ISO 19011 Guidelines for quality and/or environmental management systems auditing*., International Organization for Standardization, Geneva, 2002., retrieved 08.07.2008., www.iso.staratel.com;

Isoraite M, Analysis of Transport Performance Measurement System, 5th international Conference RelStat, Mykolas Romous, University of Lithuania, Lithuania, 2005, Pg. 1- 5;

International Maritime Organization., *ISPS Code 2003 Edition*, 4 Albert Embankment, London SE1 7SR., Arkle Print Ltd., Northampton, United Kingdom., pg 19—21, 76—85;

International Maritime Organization. (2004), *Interim Guidance on Voluntary Self-Assessment by SOLAS Contracting Governments and by Port Facility – MSC/Circ. 1131*., IMO, London;

IMO. (2008), *Maritime Security*., Supplement No.1 2008, IMO60, IMO News, Issue 1, 2008, International Maritime Organization., pg XI – Supplementary;

International Maritime Organization. (2004), *SOLAS Consolidated Edition 2004*., The Bath Press, United Kingdom;

International Labour Organization, *Code of Practice on Security in Ports*., IMO-ILO Tripartite Meeting of Experts on Security, Safety and Health in Ports., Geneva, 2003, page 28 to 36;

International Maritime Organization. (2004), *Interim Guidance on Voluntary Self-Assessment by SOLAS Contracting Governments and by Port Facility – MSC/Circ. 1131*., IMO, London;

International Maritime Organization (2003), *ISPS Code 2003 Edition*, 4 Albert Embankment, Arkle Print Ltd., Northampton, United Kingdom;

Jones S, *Maritime Security, A Practical Guide*, The Nautical Institute, London, 2006, Pg. 3;

Kuo, C., *Managing Ship Safety*, LLP Ltd. September 1998;

Kuo C., *Safety management and its Application*, The Nautical Institute, London 2007;

Lehtinen E and Wahlstrom B. (2002), Safety Performance Measurement In Process Industries, Technical Research Centre of Finland, Retrived 18.11.2008, http://www.bewas.fi/PMA_170pdf.

Legal Research Board., The Merchant Shipping Ordinance 1952., International Law Book Services, Golden Book Centre Sdn Bhd., 2007, pg 265;

McNaught F., Effectiveness of the International Ship and Port Facility Security (ISPS) Code in addressing the Maritime Security Threat; GEDDES PAPER 2005, Royal Australian Navy, Australia, 2005, pg. 5 – 6;

Manule F. A., *On the Practice of Safety*, Vol. 55, John, Wiley & Son Inc, USA, 2003, Pg 437, 445;

Parker J. C., Managing Risk in Shipping, The Nautical Institute, London, 1999;

Redinger C. F. and Levine S. P., Occupational Health and Safety Management System Performance Measurement – A Universal Assessment Instrument, American industrial Hygiene Association, USA, 1999, Pg. 33;

Ross C. W., Computer System for OSHM, Marcel Dekker Inc., USA, 1991, Pg. 204;
Nelemans R, Wiezer N, Vaas F, Gort J, Groeneweg J ., *TRIPOD SIGMA. RESULTS OF A PRO-ACTIVE WORK STRESS-SURVEY*., TNO Work & Employment, University of Leiden, Centre for Safety Research TNO paper | APA/NIOSH Conference 2003

Reason J., et al, TRIPOD, A principled basis for accident prevention, 1988;

Sklet S., *Methods for accident investigation*, Norwegian University of Technology, 2002;

Sullivan J. P. (2002), *Unconventional Weapons Response Handbook*, First edition, Jane's, Jane's Information Group, Virginia, USA;

Servik P. & Wetzel R., *Application Performance Measurement: The State of the Art,* Business Communication Review, USA, Feb 2004, Pg.1;

Sutarji K, *Efficiency Measurement of Malaysia's Maritime Enforcement Agency*, Penerbitan Universiti Kebangsaan Malaysia, Bangi, 2009, Pg 61;

Steen J. V., Safety Performance Measurement, European process safety Centre, Institution of Chemical Engineer, UK, 1996, Pg. 3-4;

Stranks J., A Manager's guide to Health & Safety at Work, Kogen Page Limited, London, 2001, Pg 54;
Turnbull K. F., US and International Approaches to Performance Measurement for Transportation: A Conference, Transport research Board, USA, Dec 2008, Pg. 45;

Srinivas G. S., *Risk Assessment Model for Assessing NBFCs' (Asset Financing) Customers* International Journal of Trade, Economics and Finance, Vol. 1, No. 1, June, 2010 2010-023X;

Turksema R. & Postma K., *Tripod Beta and Performance Audit*, International Seminar on Performance Auditing, Oslo, 25 May 2007;

Walewski J., Gibson G E., *INTERNATIONAL PROJECT RISK ASSESSMENT: METHODS, PROCEDURES, AND CRITICAL FACTORS***,** A Report of the Center Construction Industry Studies The University of Texas at Austin In Cooperation with and Additional Guidance Provided by: Construction Industry Institute Project Team 181 International Project Risk Assessment Austin, Texas September 2003

UK P & I Club., *GETTING TO GRIPS WITH THE HUMAN FACTOR* The puzzle that is safety management and total incident prevention – an insight
US Department of Transport, *Recommended Security Guidelines for Facilities*., Navigation and Vessel Inspection Circular no. 11-02., United State Coast Guard, 2003, Washington DC, USA, COMDTPUB P16700.4., Enclosure 5 page 1 to 8;

USCG., *Risk Management Within Coast Guard - Risk Based Decision Making Guidelines*., United State Coast Guard, 2006, Washington DC, USA, Retrived 05.07.2006, http://www.uscg.mil/hq/gm/risk;

US Department of Transport, *Recommended Security Guidelines for Facilities*., Navigation and Vessel Inspection Circular no. 11-02., United State Coast Guard, 2003, Washington DC, USA, COMDTPUB P16700.4., Enclosure 5 page 1 to 8;