Name of Port :		**Date :**	**Reference:**

PORT ASSESSMENT

		Questions	Details	Notes
GENERAL INFORMATION - ASSESSORS				
	1	Date of assessment/survey		
	2	Name(s) of person(s) carrying out assessment		
	3	Relevant skills & expertise of assessors. Detail the DOT approval.		
GENERAL INFORMATION - PORT FACILITY				
	4	Name of Port Facility & adjacent users.		
	5	Port Facility Point of Contact name & phone nos		
	6	Adjacent Users Points of Contact Name & Phone nos		
	7	Name of designated/appointed PFSO & Security Officer if applicable		

Identification and evaluation of important assets and infrastructure which it is important to protect				
	8	Identify and prioritise all areas which are relevant to Port Security which may include port facilities which are already covered by Regulation (EC) No 725/2004.		
	9	Identify the specific characteristics of each sub-area, such as ;		
		Infracture		
		Location		
		Power Supply		
		Communications Systems		
		Ownership, Tenants & Users		
		Other elements considered security relevant		
	10	Having considered the above, you should now delineate your Port Boundary,		This is probably best achieved with good legible, up- to- date photographs, drawings, plans and charts. This should start from an overall view and then continue into specifics. Please remember that someone reading the assessment may not be familiar with the port area so do not assume prior knowledge.

Identification of possible threats to the assets and infrastructure and the likelihood of their occurrence, in order to establish and prioritise security measures				
	11	Identify potential threat scenarios for the entire port.		
	12	Identify potential threats scenarios for specific parts of its infrastructure		Threat Assessment is the key to a sound review of port security. However, there is a minimum security level required. In this section “likelihood of occurrence” is not intended to be interpreted as “it will never happen” rather it is intended to establish a priority in the security regime. Cargo, baggage, people or transport equipment within the port can be a direct target of an identified threat;
	13	Identify potential threats scenarios for specific parts of its infrastructure based upon their potential role as access and transit points when neighbouring areas are targeted		

	14	Identify security issues deriving from the interface between port facility and other port security measures		This is aimed at the whole port and how each part must interact effectively and in particular not cancel each other out.
	15	Identify risk variations, e.g. those based on seasonality		Factors to consider here are winter schedules or increased vulnerability at night or if the port is working or not
	16	Identify the specific consequences of a threat scenario. Consequences can impact on one or more sub-areas. Both direct and indirect consequences will be identified. Special attention will be given to the risk of human casualties.		Many of these points will have been covered in the original ISPS plan. Try to go back a step and look afresh at the whole port and see if anything has to be re-considered
	17	Identify the possibility of cluster effects of security incidents.		This would be a concerted attack on a series of areas that together might be a cause for concern. An example could be a cyber attack together with a distraction incident and then a more serious attack.

Identification, selection and prioritisation of counter-measures and procedural changes and their level of effectiveness in reducing vulnerability				
	18	Identify all organisational aspects relevant to overall port security, including the division of all security-related authorities, existing rules and procedures		An organisation chart with names numbers and then identify the linkages might suffice in many cases.
	19	Identify measures, procedures and actions aimed at reducing critical vulnerabilities. Specific attention will be paid to the need for, and the means of, access control or restrictions to the entire port or specific parts of a port, including identification of passangers, port employees or other workers, visitors and ship crews, area of activity monitoring requirements, cargo and luggage control. Measures, procedures and actions will be consistant with the percieved risk, which may vary in parts.		Variations between port areas and different ports needs to be carefully examined and justified, particularly if one facility has stringent precautions and another has little or none. The term "percieved risk" has to be carefully applied and should be read in the context of an overall threat analysis.

	20	Identify how measures, procedures and actions will be reinforced in the event of an increase of security level		This refers to the three levels of security and the assessment must give guidance to the planners as to exactly how increased security level are to be achieved. It should also cover how these increased procedures are to be maintained.
	21	Identify specific requirements for dealing with established security concerns, such as 'suspect' cargo, luggage, bunker, provisions or persons, unknown parcels, known dangers (e.g. bomb). Those requirements will analyse desirability conditions for either clearing the risk where it is encountered or after moving it to a secure area.		This is probably best covered by having standard operating procedures written down and available. These should be specific to the port or port area and not just a generic version. In the audit of the eventual plan these "drills" would be one of the points to be examined.
	22	Identify measures, procedures and action aimed at limiting and mitigating consequences		Ref 19 ?

	23	Identify task divisions allowing for the appropriate and correct implementation of the measures, procedures and actions identified.		Ref 20 ?
	24	Pay specific attention, where appropriate, to the relationship with other security plans (e.g. Port Facility Security Plans) and other existing security measures. Attention will also be paid to the relationship with other response plans (e.g. oil spill response plan, port contingency plan, medical intervention plan, nuclear disaster plan, etc.		This is self-evident but it is worthwhile to point out that “security issues” only are the subject of the directive and an accident or emergency is not a security issue of itself. A factor to be considered is the weakling of security during or after an emergency.
	25	Identify communication requirements for implementation of the measures and procedures		Up to this communications or the lack of them or their unavailability when needed was the most common problem encountered in port security.
	26	Pay specific attention to measures to protect security-sensitive information from disclosure		
	27	Identify which port personnel will be subject to background checks and/or security vetting because of their involvment in high-risk areas		
	28	Identify the need-to-know requirements of all those directly involved as well as, where appropriate, the general public		Relevant information to be disseminated at appropriate levels.

Identification of weaknesses, including human factors in the infrastructure, policies and procedures				
	29	Identify vulnerabilities of the overarching port security related to organisational, legislative and procedural aspects		
	30	Identify the vulnerabilities of each sub-area		
CHECKLIST				
Checklist :	eg	Designated port facility area	Lighting	The issues listed across were all taken into account when the assessment was being carried out.
		Fencing/barriers Security cameras	Communication systems	
		Restricted areas	Navigation systems	
		Infrastructure	Security cameras	
		Intruder detection & alarms	Passenger vehicles - ditto	
		Security patrols & manning	Luggage	
		Water approaches & patrols	Port personnel procedures	
		Berths	Training	
		Access to ships	Security levels 2 & 3	
		Ship personnel	Port facility security plan	
		Cargo	Stores	
		Passengers - boarding cards, area, checks & searches	Port facility management & committees	

SUMMARY OF RECOMMENDATIONS				