Section 8 – Threat Evaluation and Risk Assessment

It is generally agreed that risk-based decision-making is one of the best methods for completing a security assessment and to determine appropriate security measures for a ship.

Risk-based decision-making is a systematic and analytical process to:

1. Consider the likelihood that a security breach will endanger an asset, individual, or function.
2. Identify actions to reduce the vulnerability.
3. Mitigate the consequences of any security breach.

A security assessment is a process that identifies weaknesses in physical structures, personnel protection systems, processes, or other areas that may lead to a security breach, and may suggest options to eliminate or mitigate those weaknesses.

For example, a security assessment might reveal weaknesses in an organisation's security system or unprotected access points such as the pilot boarding ladder not being raised or side ports not being secured or monitored after loading stores.

To mitigate this threat, a vessel would implement procedures to ensure that such access points are secured and verified by some means.

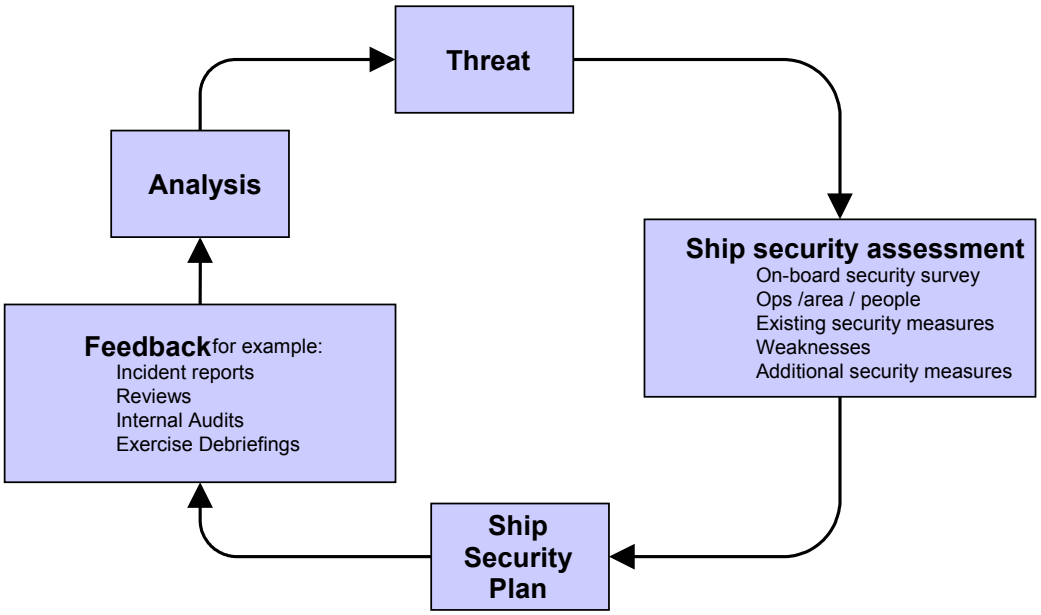
Another security enhancement might be to place locking mechanisms and/or wire mesh on doors and windows that provide access to restricted areas to prevent unauthorised personnel from entering such spaces.

Ship Security Assessments can identify vulnerabilities in vessel operations, personnel security, and physical and technical security.

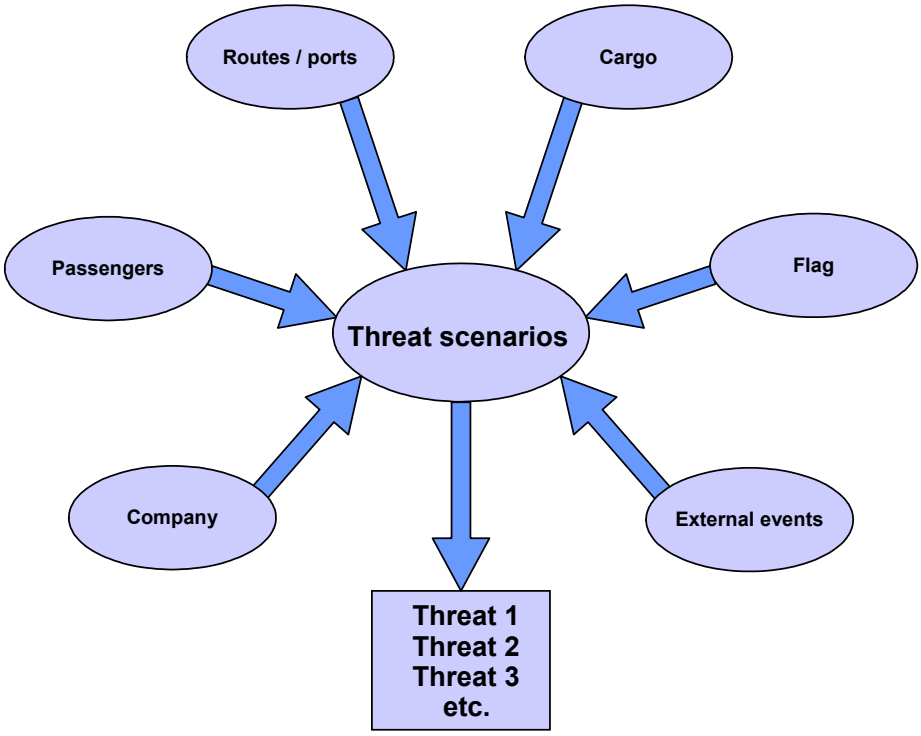
6 Steps to carrying out a Threat Evaluation and Risk Assessment

1. Establish potential threats against ship specific
2. Consequence Assessment
3. Vulnerability Assessment
4. Mitigation
5. Implementation
6. Audit, Review and Improve

An approach to a Ship Security Assessment



Establishing Threat Priorities



Ship Specific Considerations

Questions	Notes
What flag does the ship fly?	Could the nationality of the Administration increase the level of threat?
What nationality are the Ship Owners/Company?	Could the nationality of the ship owner/company increase the level of threat?
What nationalities are the crew?	Could the nationalities of the crew increase the level of threat?
What routes does the ship sail?	
Is it through areas of increased threat?	• Areas of Terrorism • Areas of Conflict • Areas of Piracy
What ports does the ship call?	• High profile city ports • Close to high densities of population • Poor security, limited protection
What cargo does the ship carry?	• Passengers • Hazardous Material
What external events are taking place?	• Civil Disorder in countries to be visited • High profile events (for example, Olympic Games)

Document Version 1.0 created on 11-Apr-03

5 Steps to carrying out a Security Threat Assessment

Step 1 – Establish potential threats against ship specific

This section is based on the approach adopted in USCG NVIC 10-02. Other approaches are available.

To begin an assessment, a vessel or company needs to consider security threat scenario(s) consisting of potential threats to a vessel under specific circumstances.

It is important that the scenario or scenarios are within the realm of possibility and, at a minimum, address known capabilities and intents.

Example Scenario

A boat containing explosives (a specific attack scenario) ramming a tanker (target) that is in a navigational choke point (specific circumstances) is one credible scenario.

It may be less credible that a hand held missile launched from a distance at a larger tanker could intentionally sink the vessel that is in the same choke point.

How many scenarios are required?

The number of scenarios is left to the judgement of the company. An initial evaluation should at least consider those scenarios provided in Table 1 – Notional List of Scenarios, with emphasis being taken to avoid unnecessarily evaluating excessive scenarios that result in low consequences.

Minor variations of the same scenario do not need to be evaluated separately unless there are measurable differences in consequences.

Table 1 – Notional List of Scenarios

Scenario	Aim	Application	Considerations
Intrude – Take Control - Seize – Hijack and …	a. Damage/destroy vessel with explosives	Intruder plants explosives	Does your ship carry special cargo for example, passengers, LNG, LPG
	b. Damage/destroy vessel through malicious acts	Intruder takes control of vessel runs it aground or collides with another vessel	To cause environmental disaster To cause shipping hazard in port approach/choke point
	c. Create a pollution or toxic release incident without destroying target	Intruder opens valves/vents to release toxic materials or release toxic material brought along Intruder overrides interlocks leading to damage/destruction	To cause environmental disaster
	d. Take hostages/kill people	Goal of the intruder is to kill people	
	e. Disable critical vessel services (for example, propulsion, steering, power)	Intruder creates damage to critical equipment so vessel is vulnerable to grounding	
External Attack by…….	a. Moving explosives adjacent to vessel: 1. From the waterside 2. On the shore side 3. Subsurface	USS Cole Style attack Frogman Car / truck bomb	
	b. Ramming a stationary target: 1. With a vessel 2. With a land based target	Intentional collision meant to damage – destroy the target	Potential to cause shipping hazard for example, port approach/choke point
	c. Stand off attack - launching or firing weapon from a distance	Firing at the vessel with a missile or rifle	Armour piercing rounds could be devastating fired at an LPG
Using the vessel as a means of transferring… ……	a. Materials to be used as a weapon in/out of the country		
Unauthorised Access			

Step 2 – Consequence Assessment

Each scenario should be evaluated in terms of the potential consequences of the attack. Three elements are included in the consequence assessment:

- death and injury
- economic impact
- environmental impact.

Descriptors of the consequence components are given below.

Component	Descriptor
Death and injury	The potential number of lives that could be lost and injuries occurring as a result of an attack scenario.
Economic impact	The potential economic impact of an attack scenario.
Environmental impact	The potential environmental impact of an attack scenario.

The appropriate consequence score or "rating" should be evaluated for each scenario.

Consequence ratings and criteria with benchmarks are provided in the following Table 2 – Consequence Score.

These ratings are intended to be broad relative estimates. The appropriate rating is determined by using the consequence component that results in the highest rating.

Example Rating

If the death and injury and economic impact result in a Moderate or "1" rating but the environmental impact result is a Significant or "2" rating, then the overall consequence score would be assigned a rating of "2."

A precise calculation of these elements is not necessary.

Table 2 – Consequence Score

Assign a rating of	If the impact could be
3	**CATASTROPHIC** = Numerous loss of life or injuries, major national or long term economic impact, complete destruction of multiple aspects of the eco-system over a large area
2	**SIGNIFICANT** = Multiple loss of life or injuries, major regional economic impact, long-term damage to a portion of the eco-system.
1	**MODERATE** = Little or no loss of life or injuries, minimal economic impact, or some environmental damage.

Step 3 – Vulnerability Assessment

Each scenario should be evaluated in terms of the vessel's vulnerability to an attack. The four elements of the vulnerability score are:

- availability
- accessibility
- organic security
- vessel hardness

For each scenario, assume that the company has the greatest control over the accessibility and organic security elements. Descriptors of these two vulnerability elements follow.

Element	Descriptor
Accessibility	Accessibility of the vessel to the attack scenario. This relates to physical and geographic barriers that deter the threat independently of organic security.
Organic Security	The ability of the shipboard organisation to deter the attack. It includes security plans, communication capability, guard force, intrusion detection systems, and timeliness of outside law enforcement to prevent attack.

The company should discuss each vulnerability element for a given scenario. The initial evaluation of vulnerability is normally viewed with only existing strategies and protective measures, meant to lessen vulnerabilities, which are already in place.

After the initial evaluation has been performed, a comparison evaluation can be made with new strategies and protective measures considered.

Assessing the vulnerability with only the existing strategies and protective measures provides a better understanding of the overall risk associated with the scenario and how new strategies and protective measures will mitigate the risk.

The vulnerability score and the criteria with benchmark examples are provided in the following Table 3 – Vulnerability Score. Each scenario should be evaluated to get the individual score for each element, then sum these elements to get the total vulnerability score (step 3 in Table 5). This score should be used as the vulnerability score when evaluating each scenario in the next step.

Table 3 – Vulnerability Score

Category	Accessibility	Organic Security
3	No deterrence (for example, unrestricted access to vessel and unrestricted internal movement).	No deterrence capability (for example, no plan, no guard force, no emergency communications, outside law enforcement not available for timely prevention, no detection capability).
2	Good deterrence (for example, single substantial barrier; unrestricted access to within 100 yards of vessel).	Good deterrence capability (for example, minimal security plan, some communications, armed guard force of limited size relative to the vessel; outside law enforcement not available for timely prevention, limited detection systems).
1	Excellent deterrence (expected to deter attack; access restricted to within 500 yards of vessel; multiple physical/geographical barriers).	Excellent deterrence capability (expected to deter attack; covert security elements that represent additional elements not visible or apparent).

These definitions come directly from USCG NVIC 10-02. They are best taken as a means of comparing Vulnerability scores for Accessibility and Organic Security. As an example; it is not intended that ships deploy an "armed guard force" or employ "covert security elements" despite these terms being used in the definitions.

Step 4 – Mitigation

The company should next determine which scenarios may require mitigation strategies (protective measures) implemented. This is accomplished by determining where the scenario falls in Table 4 based on the consequences and vulnerability assessment scores. Following are terms used in Table 4 as mitigation categories:

Mitigate means that mitigation strategies, such as security protective measures and/or procedures, may be developed to reduce risk for that scenario. An appendix to the ship security plan may contain the scenario(s) evaluated, the results of the evaluation, a description of the mitigation measure evaluated, and the reason mitigation measures were or were not chosen.

Consider means that the scenario should be considered and mitigation strategies should be developed on a case-by-case basis. The ship security plan may contain the scenario(s) evaluated, the results of the evaluation, and the reason mitigation measures were or were not chosen.

Document means that the scenario may not need a mitigation measure at this time and therefore needs only to be documented. However, mitigation measures having little cost may still merit consideration. The ship security plan may contain the scenario evaluated and the results. This will be beneficial in further revisions of the security plan, to know if the underlying assumptions have changed since the last edition of the security assessment.

Table 4 – Vulnerability and Consequence Matrix is intended as a broad, relative tool to assist in the development of the vessel security plan. "Results" are not intended to be the sole basis to trigger or waive the need for specific measure, but are tools in identifying potential vulnerabilities and evaluating prospective methods to address them.

Table 4 – Vulnerability and Consequence Matrix

		Total Vulnerability Score		
		2	3-4	5-6
Consequence Score	3	Consider	Mitigate	Mitigate
	2	Document	Consider	Mitigate
	1	Document	Document	Consider

To assist the company in determining which scenarios may require mitigation methods, the company may find it beneficial to use Table 5 – Mitigation Determination Worksheet provided below.

The vessels owner and/or operator can record the scenarios considered, the consequence score (Table 2), outcome of the each element of vulnerability (Table 3), the total vulnerability score, and the mitigation category (Table 4).

Table 5 – Mitigation Determination Worksheet

Mitigation Determination Worksheet					
Step 1	**Step 2**	**Step 3**			**Step 4**
Scenario/Description	**Consequence Score (Table 2)**	**Vulnerability Score (Table 3)**			**Mitigation Results (Table 4)**
		Accessibility	**+ Organic = Security**	**Total Score**	

Step 5 – Implementation

The true value of these assessments is realised, when:

- the company determines which scenarios require mitigation
- mitigation strategies (protective measures) are implemented to reduce vulnerabilities.

The overall desire is to reduce the risk associated with the identified scenario.

Note that generally it is easier to reduce vulnerabilities than to reduce consequences or threats when considering mitigation strategies.

To assist company in evaluating the effectiveness of specific mitigation strategies (protective measures), the company may find it beneficial to use Table 6 – Mitigation Implementation Worksheet provided below.

Table 6 – Mitigation Implementation Worksheet

Mitigation Implementation Worksheet						
Step 1	**Step 2**	**Step 3**	**Step 4**			**Step 5**
Mitigation Strategy (Protective Measures)	**Scenario(s) that are affected by Mitigation Strategy (from Step 1 in Table 5)**	**Consequence Score (remains the same)**	**Vulnerability Score (Table 3)**			**New Mitigation Results (Table 4)**
			Accessibility	**+ Organic**	**= Total Security Score**	
1.	1.					
	2.					
	3.					
2.						

The following steps correspond to each column in Table 6.

1. The company should brainstorm mitigation strategies (protective measures) and record them in the first column of Table 6.
2. Using the scenario(s) from Table 5, list all of the scenario(s) that would be affected by the selected mitigation strategy.
3. The consequence score remains the same as was recorded in Table 5 for each scenario.
4. Re-evaluate the vulnerability score (Table 3) for each element, taking into consideration the mitigation strategy, for each scenario.
5. With the consequence score and new total vulnerability score, use Table 4 to determine the new mitigation results.

In determining if a mitigation strategy should be implemented, there are two factors to consider:

- Effectiveness
- Feasibility

A strategy may be thought of as highly effective if its implementation lowers the mitigation category. For example, from "mitigate" to "consider" in Table 4.

A strategy may be thought of as partially effective if the strategy will lower the overall vulnerability score when implemented by itself or with one or more other strategies. For example, if a mitigation strategy lowers the vulnerability score from "5-6" to "3-4" while the consequence score remains at "3" and the mitigation category stays at "mitigate".

If a mitigation strategy, when considered individually, does not reduce the vulnerability then multiple strategies may be considered in combination. Considering mitigation strategies as a whole may allow the vulnerability to be reduced.

A strategy may be thought of as **feasible** if it can be implemented with little operational impact or funding relative to the prospective reduction in vulnerability.

A strategy may be thought of as **partially feasible** if its implementation requires significant changes or funding relative to the prospective reduction in vulnerability.

A strategy may be thought of as **not feasible** if its implementation is extremely problematic or is cost prohibitive.

The company should keep in mind that some strategies may be deployed commensurate with various security threat levels established.

Feasibility of a mitigation strategy may vary based on the *MARSEC level,* therefore some strategies may not be warranted at *MARSEC Level 1,* but may be at *MARSEC Levels 2* or 3.

USCG NVIC 10-02 uses *MARSEC Level 1, 2 & 3*. These are directly equivalent to Security Level 1, 2 & 3 which are adopted in the ISPS Code.

For example, using divers to inspect the underwater pier structures and ship's hulls may not be necessary even if there is a specific threat and/or an increase in *MARSEC level.* Mitigation strategies should ultimately ensure that a level of security is maintained to achieve the objectives discussed in NVIC 10-02.

Example Vulnerability Mitigation Measure

A company may implement security patrols by hiring additional personnel to detect and prevent unauthorized persons from entering spaces below the main deck on a passenger ferry.

This measure would improve organic security and may reduce the overall vulnerability score from a "high" to a "medium".

This option, however, is specific for this scenario and also carries a certain cost.

Another option might be to secure all access points to spaces below the main deck. This may reduce the accessibility score from "high" to "medium".

This option does not require additional personnel and is a passive mitigation measure. Similarly, other scenarios can be tested to determine the most effective strategies.

The vessel owner an/or operator should develop a process through which overall security is continually evaluated by considering consequences and vulnerabilities, how they may change over time, and what additional mitigation strategies can be applied.

Example

Bulk Carrier carrying iron ore, running Peru, South America to South Africa.
Bahamas Flag, Dutch Owned, Crew 5 Dutch, 12 Philippino.

Step 1 – Establish potential threats against ship specific

Flag: Bahamas – No Specific Risk.

Owner: Dutch – No Specific Risk.

Crew: Dutch/Philippines – No Specific Risk.

Passengers: None – No Specific Risk.

Route: Peru to South Africa via Magellan Straights, bunkering in Punta Arenas - High Risk

External Events: Civil unrest in Argentina – High Risk.

Threats: Route taking into consideration civil unrest in Argentina and that the ship is required to bunker in Punta Arenas.

Intruders take control of ship for money, organisation/belief/propaganda.

Intentions	Likelihood
To take hostages for ransom or kill crew for publicity	Possible
To plant explosives onboard in order to sink ship	Possible
To take over ship and cause environmental disaster	Unlikely

External attack to sink ship in port or in port approach choke point.

Intentions	Likelihood
To ram vessel with boat laden with explosives	Unlikely
To drive truck laden with explosives along side in port	Unlikely
To launch missile attack against vessel from a distance	Unlikely
To place explosives subsurface using divers in port	Unlikely
Use the vessel to transport weapons, ammunition or people	Possible

Step 2 – Consequence Assessment

Refer to Table 2 - Consequence Score. It is only necessary to score the threats with the highest likelihood.

Considerations to include	Consequence Score
All crew killed	Significant
Could the cargo represent environmental disaster	Moderate
Could the loss of ship cause economic disaster	Moderate

Consequence score will remain **Significant** throughout.

Mitigation Determination Worksheet					
Step 1	**Step 2**	Step 3			Step 4
Scenario/Description	**Consequence Score (Table 2)**	Vulnerability Score (Table 3) Accessibility + Organic = Total Security Score			Mitigation Results (Table 4)
Intruders take control of ship in order to take hostages and/or kill crew **during passage**.	**2**				
Intruders take control of ship in order to place explosives and sink ship **during passage**.	**2**				
Intruders take control of ship in order to take hostages and/or kill crew **when bunkering**.	**2**				
Intruders take control of ship in order to place explosives and sink ship **when bunkering**.	**2**				
Intruders take control of ship to transport weapons or people.	**1**				

Step 3 – Vulnerability Assessment

Refer to Table 3 - Vulnerability Score.

Mitigation Determination Worksheet					
Step 1	**Step 2**	**Step 3**			**Step 4**
Scenario/Description	**Consequence Score (Table 2)**	**Vulnerability Score (Table 3)**			**Mitigation Results (Table 4)**
		Accessibility	**+ Organic**	**= Total Security Score**	
Intruders take control of ship in order to take hostages and/or kill crew **during passage**.	**2**	3	2	**5**	
Intruders take control of ship in order to place explosives and sink ship **during passage**.	**2**	3	2	**5**	
Intruders take control of ship in order to take hostages and/or kill crew **when bunkering**.	**2**	3	2	**5**	
Intruders take control of ship in order to place explosives and sink ship **when bunkering**.	**2**	3	2	**5**	
Intruders take control of ship to transport weapons or people.	**1**	3	2	**5**	

Step 4 – Mitigation

Refer to Table 4 - Vulnerability and Consequence Matrix.

Mitigation Determination Worksheet					
Step 1	**Step 2**	**Step 3**			**Step 4**
Scenario/Description	**Consequence Score (Table 2)**	**Vulnerability Score (Table 3)**			**Mitigation Results (Table 4)**
		Accessibility	**Organic Security**	**= Total Score**	
Intruders take control of ship in order to take hostages and/or kill crew **during passage**.	**2**	3	2	**5**	**Mitigate**
Intruders take control of ship in order to place explosives and sink ship **during passage**.	**2**	3	2	**5**	**Mitigate**
Intruders take control of ship in order to take hostages and/or kill crew **when bunkering**.	**2**	3	2	**5**	**Mitigate**
Intruders take control of ship in order to place explosives and sink ship **when bunkering**.	**2**	3	2	**5**	**Mitigate**
Intruders take control of boat to transport weapons or people.	**1**	3	2	**5**	**Consider**

When entering port, Port Facility Security Measures along with the Security Level will need to be taken into consideration.

Step 5 - Implementation

Refer to Table 6 - Mitigation Implementation Worksheet.

Mitigate by increasing security measures from "normal" to "additional" (Additional measures may be procedural, operational or additional security equipment).

Typical increased security measures may include:

Procedural: Monitoring and securing of access points. Instigating or increasing security patrols

Operational: Look at the passage plan with a view to avoiding areas of heightened risk. Such an approach is not always possible due to commercial considerations.

Security Equipment: Monitoring equipment such as CCTV and access control equipment such as Key Pad Entry systems

This has reduced the accessibility in the vulnerability score from 3 to 2.

Mitigation Determination Worksheet						
Step 1	**Step 2**	**Step 3**	**Step 4**			**Step 5**
Mitigation Strategy (Protective Measures)	**Scenario(s) that are affected by Mitigation Strategy (from Step 1 in Table 5)**	**Consequence Score (remains the same)**	**Vulnerability Score (Table 3)**			**New Mitigation Results (Table 4)**
			Accessibility	**+ Organic Security**	**= Total Score**	
Accessibility: Deterrence increased by implementing increased security measures. Organic Security: Deterrence increased by implementing increased security measures	**At Sea** **1. Scenario 1**	**2**	**2**	**2**	**4**	**Consider**
	2. Scenario 2	**2**	**2**	**2**	**4**	**Consider**
Accessibility: Deterrence increased by implementing increased security measures Organic Security: Deterrence increased by implementing increased security measures. Port Facility Security Measures and their Level of security will affect the Accessibility score in the Vulnerability table.	**When Bunkering** **3. Scenario 3**	**2**	**1**	**2**	**3**	**Consider**
	4. Scenario 4	**2**	**1**	**2**	**3**	**Consider**
	5. Scenario 5	**1**	**1**	**2**	**3**	**Document**

In the above example the maximum mitigation result has been reduced from **Mitigate** to **Consider**. The addition security measures implemented to achieve this reduction should form part of the ship security plan. How the measures are implemented and controlled will form part of the security procedures attached to the ship security plan.