Risk Management

Lesson Topics

- Risk Management
- Continuous Improvement through Lessons Learned
- Contingency Planning

Risk Management

Risk is defined as "the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences.

Risk Management

Risk management is the process for identifying, analyzing, and communicating risk and accepting, avoiding, transferring, or controlling it to an acceptable level, considering associated costs and benefits of any actions taken.

Risk Management

A widely accepted understanding of risk is depicted by the following formula:

Threat ✖ Vulnerability ✖ Consequence = Risk

Risk Management

Since you have no control over the Threat, the way to reduce risk is to reduce Vulnerability, or Consequence, or both.

Risk Management

By employing sound risk management techniques at port facilities, you can reduce the risk to those facilities.

Risk Management

Risk management practices involve an analysis of risks and identification or development of measures to reduce those risks – or in other words, develop measures to counter the threat.

Risk Management

Risk Management involves the following steps:

1. Identify Threats
2. Assess Consequences
3. Assess Vulnerabilities
4. Develop Mitigation Strategy
5. Implement Mitigation Measures

Risk Management

1. Identify Threats

- Consider attack scenarios
- Be realistic
- These should be consistent with the Port Facility Security Assessment and Port Facility Security plan
- Avoid assessing an excessive number of similar scenarios

Risk Management

2. Assess Consequences

- Determine the consequence level (e.g. High, Medium, Low) for each scenario
- The consequence level should be consistent with the type of facility (e.g. a facility that handles dangerous cargo should have a higher consequence than one that does not)

Risk Management

3. Assess Vulnerabilities

- Determine the facility's vulnerability to each attack scenario
- Assign vulnerability rating (e.g. High, Medium, Low) for each scenario
- Consider 4 factors in determining degree of vulnerability

Risk Management

Vulnerability Factors:

- Availability
- Accessibility
- Organic security
- Facility hardiness

Risk Management

Vulnerability Assessment: Availability

The facility's presence and predictability as it relates to the nature of the attack.

Risk Management

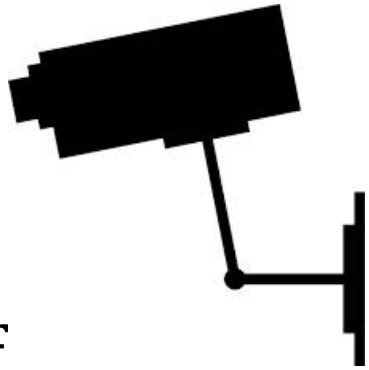
Vulnerability Assessment: Accessibility

Accessibility of the facility to the attack scenario. This relates to the physical and geographic barriers that deter the threat without organic security.

Risk Management

Vulnerability Assessment: Organic Security

- The ability of security personnel to deter the attack
- Security plans, communication capabilities, guard force, intrusion detection systems, and timeliness of outside law enforcement to prevent the attack.



Risk Management

Vulnerability Assessment: Facility Hardiness

- The ability of the facility to withstand the specific attack based on the complexity of facility design and material construction characteristics.

Risk Management

4. Develop Mitigation Strategy

- Determine which scenarios require mitigation strategies based on degree of Vulnerability and Consequence
- Document the mitigation strategies in the Port Facility Security Plan

Risk Management

5. Implement Mitigation Strategy

- Procure necessary equipment, systems, or resources
- Develop and implement processes and procedures
- Conduct training to prepare personnel to implement processes and procedures

Risk Management

Risk Management should be a continual process.

- Threats are continuously identified
- Vulnerability determinations are continually refined
- Mitigation strategies are continually refined

Risk Management

Risk Management should be a continual process.

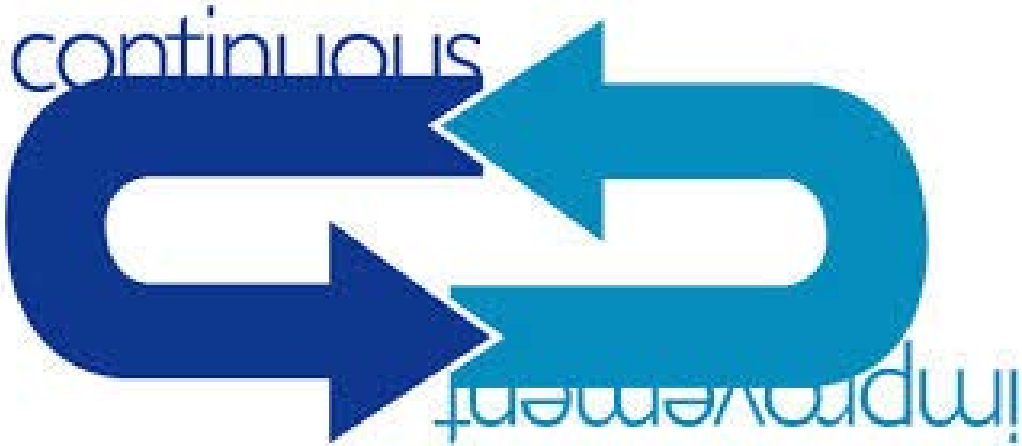
- Threats are continuously identified
- Vulnerability determinations are continually refined
- Mitigation strategies are continually refined

Continuous Improvement

Port Directors, Port Security Officers, Port Facility Security Officers, and all members of the Port Security Department should strive to conduct continuous improvement in the port security posture of port facilities.

Continuous Improvement

Candidates for improvement initiatives can be identified from lessons learned from events.



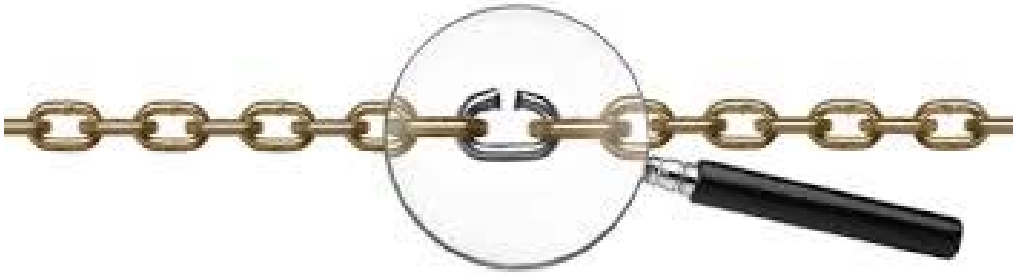
Continuous Improvement

The primary sources for lessons learned are:

- Drills
- Exercises
- Training
- Security Incidents

Continuous Improvement

All of these sources provide a means to determine areas of vulnerability as well as deficiencies in mitigation strategies.



Continuous Improvement

Lessons Learned from Drills and Exercises should be documented, categorized, and prioritized. These lessons learned could be categorized by functional area, such as access control, monitoring, communication, etc. They can also be categorized by the type of intervention or mitigation strategy needed.

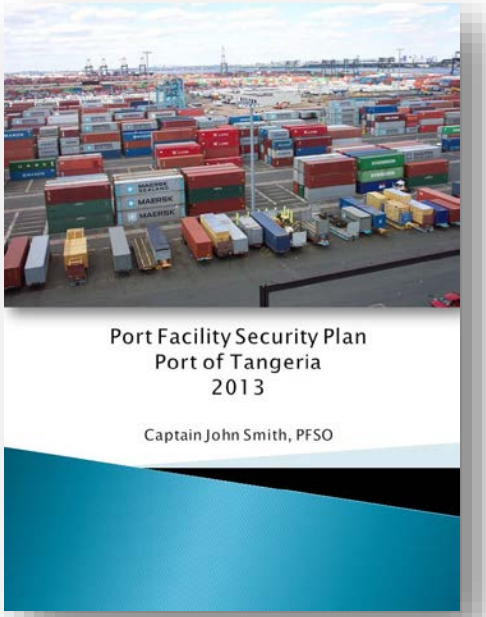
Continuous Improvement

Interventions needed based on lessons learned:

- Additional resources needed, such as additional personnel
- Equipment or systems needed, e.g. surveillance, communication, etc.

Continuous Improvement

- New or revised processes or procedures needed; these should be documented in the Port Facility Security Plan.
- Additional or revised training needed to prepare personnel.



Continuous Improvement

Training of security personnel provides an excellent opportunity to gather lessons learned.

Continuous Improvement

Based on the performance of personnel during training, lessons learned related to areas of weak performance should be documented.

Continuous Improvement

In some cases, poor performance during training may be the result of inadequate resources or processes in place, and these too provide valuable lessons learned.

Continuous Improvement

Security incidents at your or other port facilities provide an excellent means to identify lessons learned.

- Improper procedures
- Inadequate policy
- Faulty or inadequate equipment
- Performance problems

Continuous Improvement

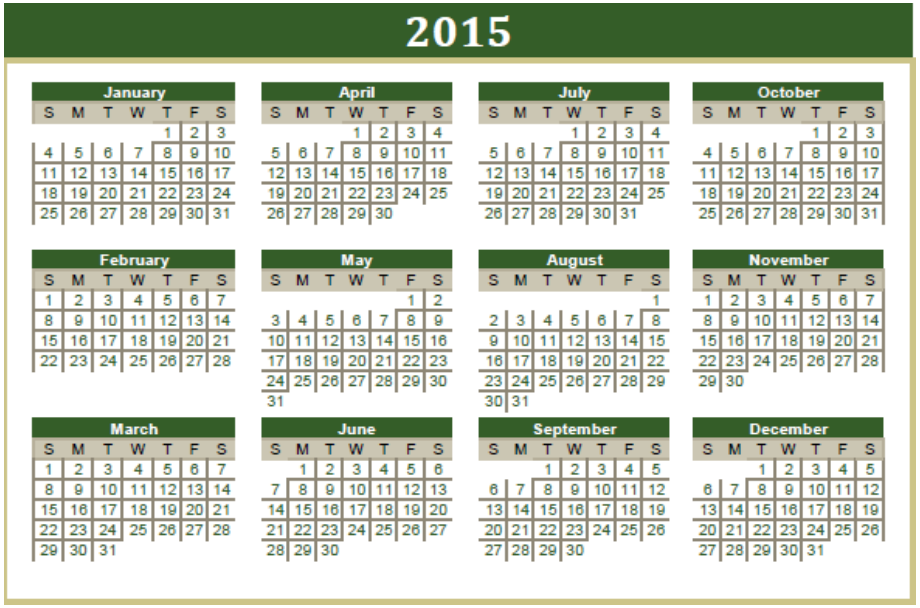
These incidents should be analyzed to determine if areas of vulnerability could be strengthened and if security measures could be improved.

Continuous Improvement

Security Officers should maintain a record of lessons learned accompanied by identified actions to overcome the deficiencies noted.

Continuous Improvement

Security Officers should also develop an annual work plan to address implementation of the required actions.



Contingency Planning

What is a contingency plan?

A contingency plan, or crisis management plan, is a set of actions that you intend to take to deal with a crisis, emergency, or disaster situation.

Contingency Planning

A contingency plan, developed in advance of an incident, can ensure a positive and successful response to an evolving situation.

Contingency Planning

The objective of a contingency plan is to recover from a situation as soon as possible and return to normal operations.

Contingency Planning

What kinds of incidents benefit from a contingency plan?

- Terrorist incidents
- Other security incidents
- Natural disasters
- Emergency situations of all kinds
- Infrastructure damage or malfunction

Contingency Planning

A good place to start when deciding the kinds of contingency plans that will be necessary is the Port Facility Security Assessment.

Contingency Planning

Incidents identified as likely in the Port Facility Security Assessment are good candidates for contingency plans.

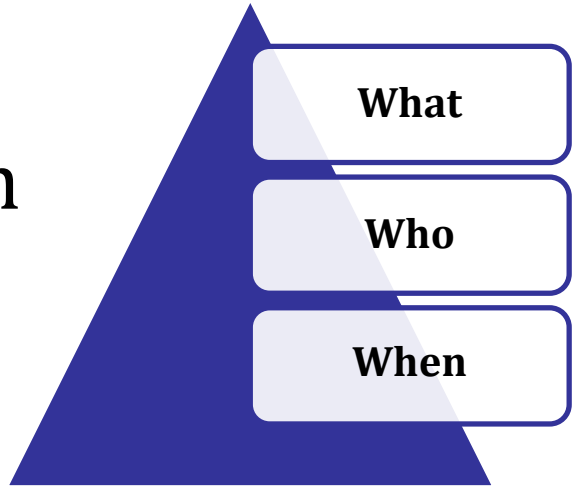
Contingency Planning

A review of past incidents at the port facility is another good way to determine the need for contingency plans.

Contingency Planning

In its most basic form, a contingency plan explains:

1. What actions need to be taken
2. Who needs to take them
3. When they need to be taken



Contingency Planning

Contingency Planning

Other types of information that are typically present in contingency plans include:

- Notification procedures: who needs to notify whom and when, and how often
- Authorities and responsibilities, e.g. Who is in charge of the response?

Contingency Planning

- Coordination mechanisms
- Communication procedures, including telephone numbers, radio frequencies, e-mail addresses, etc.
- Availability of necessary equipment and resources

Contingency Planning

Contingency Plans describe specific actions to be taken in response to a situation. These actions should be detailed enough for personnel to clearly understand what is required. Actions should ALWAYS be assigned to someone in advance and spelled out in the contingency plan.

Contingency Planning

Coordination:

When contingency plans require the actions of other organizations or agencies, the contingency plan must be developed, reviewed, and agreed to by these organizations and agencies.

Contingency Planning

Everyone involved must agree to the provisions in the contingency plan and agree to follow the detailed actions prescribed for them.

Contingency Planning

Practice:

A contingency plan is only as good as the people who are responsible for carrying out its provisions. The best way to ensure people are familiar with the contingency plan is to practice, practice, practice!

Contingency Planning

Drills, exercises, and coordination meetings will help people to become familiar with the contingency plan and comfortable and confident about its contents and required actions.

Contingency Planning

Format:

Any format may be used for a contingency plan, however, the “who, what, when, where, and how” of the response must always be included.

Contingency Planning

Sample Format:

1. Introduction
2. Responsibility
3. Organization
4. Notification and Reporting
5. Response

Contingency Planning

1. Introduction:

- Purpose
- Objectives
- Scope
- Definitions
- References

Contingency Planning

2. Responsibility:

- Of each of the agencies or organizations involved
- Of special resources or teams
- Authority for each agency, organization, team, or individual
- Designation and authority of the person in charge of the response

Contingency Planning

3. Organization:

- Conceptual organization for the response
- Reporting relationships – who reports to whom
- Coordinating relationships – who needs to work with whom

Contingency Planning

4. Notification and Reporting:

- Requirements for notification of agencies, organizations, and individuals
- Details on communication techniques, including formats for reports as required
- Frequency of reporting

Contingency Planning

5. Response:

- Actions to be taken
- Sequence of actions
- Responsibility for actions
- Timing of actions
- Relationship of actions
- Actions may be categorized by phases of the response

Contingency Planning

Planning (Optional)

Sometimes a contingency plan may contain a section detailing the planning responsibilities for developing the contingency plan. This could also include responsibility for reviewing and revising the plan at prescribed intervals.

Contingency Planning

Preparedness (Optional)

Sometimes a contingency plan may contain a section detailing a schedule for exercising the plan through drills and exercises.

Lesson 5 Activity

Application of Risk Management Principles to Determine Mitigation Strategies

Summary

Risk management is the process for identifying, analyzing, and communicating risk and accepting, avoiding, transferring, or controlling it to an acceptable level, considering associated costs and benefits of any actions taken.

Summary

A widely accepted understanding of risk is depicted by the following formula:

Threat ✖ Vulnerability ✖ Consequence = Risk

Summary

Risk Management involves the following steps:

1. Identify Threats
2. Assess Consequences
3. Assess Vulnerabilities
4. Develop Mitigation Strategy
5. Implement Mitigation Measures

Summary

The primary sources for lessons learned are:

- Drills
- Exercises
- Training
- Security Incidents

Summary

In its most basic form, a contingency plan explains:

1. What actions need to be taken
2. Who needs to take them
3. When they need to be taken

Summary

Other types of information that are typically present in contingency plans include:

- Notification procedures: who needs to notify whom and when, and how often
- Authorities and responsibilities, e.g. Who is in charge of the response?

Summary

- Coordination mechanisms
- Communication procedures, including telephone numbers, radio frequencies, e-mail addresses, etc.
- Availability of necessary equipment and resources