Risk Management

Lesson Topics

- Risk Management
- Continuous Improvement through Lessons Learned

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
- 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 or disaster 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

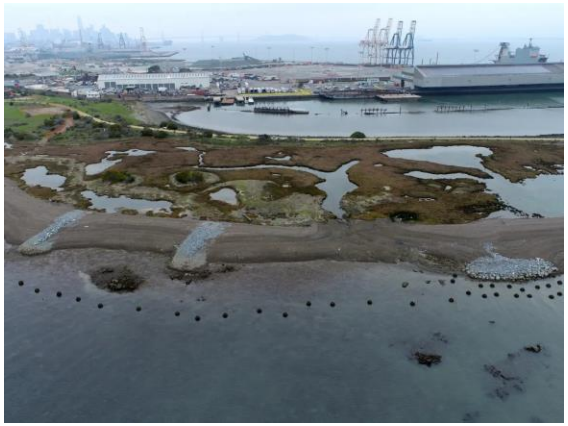
Vulnerability Assessment: Availability

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

Risk Management

Vulnerability Assessment: Accessibility

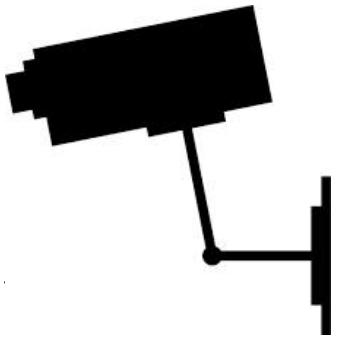
Accessibility of the facility to the attack or disaster scenario. This relates to the physical and geographic barriers that deter the threat without organic security.



Risk Management

Vulnerability Assessment: Organic Security and Facility Barriers

- The ability of facility personnel and/or facility barriers to deter the attack or disaster.
- Security & Contingency plans, communication capabilities, guard fo 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, natural or security, 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 appropriate plan (Security, Environmental, Hurricane)

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

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

Risk Management involves the following steps:

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

Continuous Improvement

Continuous Improvement

Continuous Improvement for port operations is an ongoing process of identifying, assessing, and mitigating “all hazards” risks.

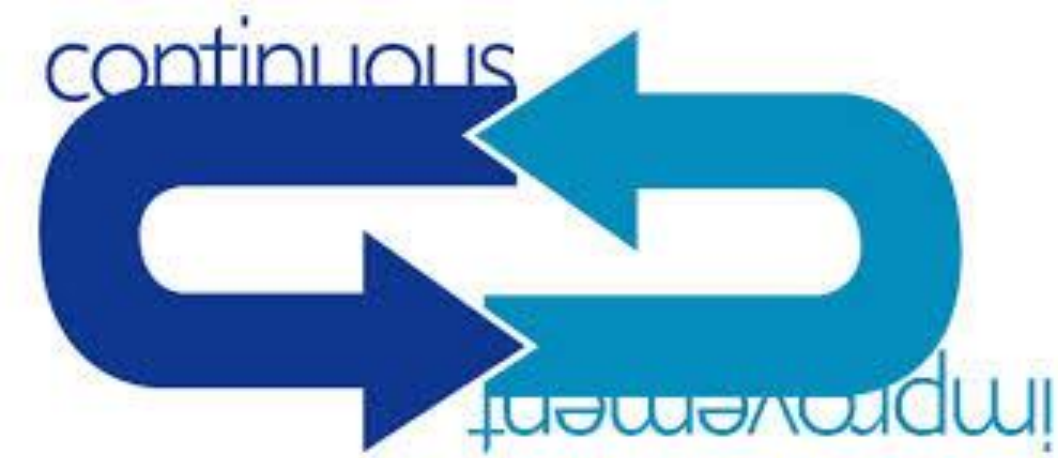
It involves constantly monitoring and evaluating risks, implementing controls and measures to minimize impact, and seeking opportunities to enhance risk management practices.

Continuous Improvement

Port Directors, Port Security Officers, Port Operations Officers, and all members of the Port Facility should strive to conduct continuous improvement in the port facilities to remain open and ready for business.

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
- Real Incidents
- Audits / Assessments

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.

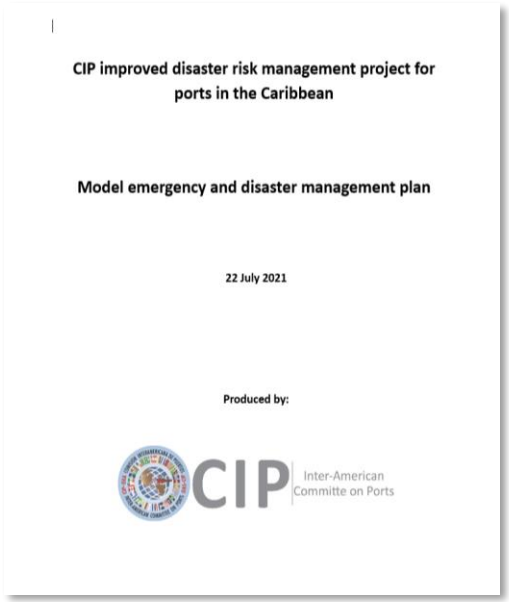
Continuous Improvement

Interventions needed based on lessons learned:

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

Continuous Improvement

- New or revised processes or procedures needed; these should be documented in the specific facility plan or regional emergency plan.
- Additional or revised training needed to prepare personnel.


CIP improved disaster risk management project for ports in the Caribbean

Model emergency and disaster management plan

22 July 2021

Produced by:

CIP Inter-American Committe on Ports

Continuous Improvement

Training of facility 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.

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

Continuous Improvement

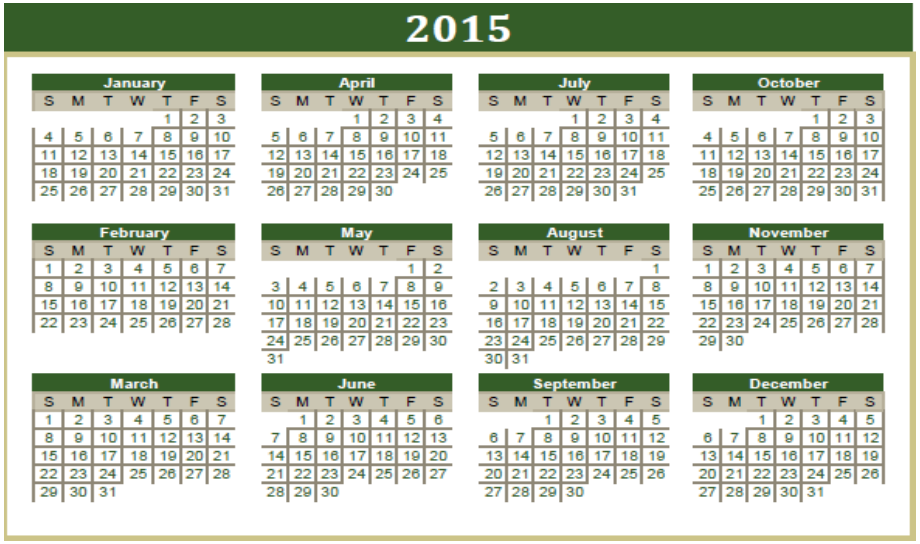
Real incidents should be analyzed to determine if areas of vulnerability could be strengthened and if additional measures could be imposed.

Continuous Improvement

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

Continuous Improvement

Safety & Security Officers and/or Operations Officers should also develop an annual work plan to address implementation of the required actions.



Summary

Continuous Improvemmt - involves constantly monitoring and evaluating risks, implementing controls and measures to minimize impact, and seeking opportunities to enhance risk management practices.

Summary

The primary sources for lessons learned to enhance continuous improvements are:

- Drills
- Exercises
- Training
- Real Incidents
- Audits / Assessments