

RISK MANAGEMENT

Capability Definition

Risk Management is defined by the Government Accountability Office (GAO) as “A continuous process of managing—through a series of mitigating actions that permeate an entity’s activities—the likelihood of an adverse event and its negative impact.” Risk Management is founded in the capacity for all levels of government to identify and measure risk prior to an event, based on credible threats/hazards, vulnerabilities, and consequences, and to manage the exposure to that risk through the prioritization and implementation of risk-reduction strategies. The actions to perform Risk Management may well vary among government entities; however, the foundation of Risk Management is constant.

Currently there are a variety of tools, processes, and offerings in practice and under development to serve the capability of Risk Management. As with the distribution of the National Infrastructure Protection Plan, the Department of Homeland Security has outlined core requirements for the management of risk, and will continue to serve this capability through additional technical assistance. As communities mature their Risk Management capability they are encouraged to look to DHS for continued guidance and updates to Threat information from the aforementioned Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) office as well as guidance on the further development of a risk analysis methodology for critical asset protection.

Outcome

Federal, State, local, tribal and private sector entities identify and assess risks, prioritize and select appropriate protection, prevention, and mitigation solutions based on reduction of risk, monitor the outcomes of allocation decisions, and undertake corrective actions. Additionally, Risk Management is integrated as a planning construct for effective prioritization and oversight of all homeland security investments.

Relationship to National Response Plan Emergency Support Function (ESF)/Annex

This capability supports the following Emergency Support Functions (ESFs):

- ESF #1: Transportation
- ESF #3: Public Works and Engineering
- ESF #4: Firefighting
- ESF #5: Emergency Management
- ESF #6: Mass Care, Housing, and Human Services
- ESF #8: Public Health and Medical Services
- ESF #9: Search and Rescue (Land-Based)
- ESF #10: Oil and Hazardous Materials Response
- ESF #12: Energy
- ESF #13: Public Safety and Security
- ESF # 14: Long-Term Community Recovery and Mitigation

Preparedness Tasks and Measures/Metrics

Activity: *Develop Risk Framework*

Definition: Develop a framework for how risk assessments and risk analysis will serve the business process of managing “risks” and a process for stakeholder buy-in. Establish a comprehensive stakeholder governing process to oversee an all-encompassing ongoing perspective of the risks posed onto the respective community. This body should include public administrators, the owners and operators of critical infrastructure and key assets within the given community, as well as key stakeholders and decision makers. Furthermore, the “framework” must consider the functional as well as spatial relationships of assets as they are often interrelated.

Critical Tasks

ComE 1.1	Ensure senior leadership communicates in writing the risk framework and intent to use risk analysis to all stakeholders
ComE 1.2	Develop actionable risk management strategy with short, medium, and long-term objectives
ComE 1.3	Develop risk analysis and risk management plans and procedures
ComE 1.3.1	Develop standards and guidelines to guide risk assessment activities
ComE 1.4	Develop and implement risk analysis training programs for state, local, and private entities
ComE 1.4.1	Conduct training in modeling and the use of analytical tools
ComE 1.4.2	Conduct risk management training for security, response, and recovery managers
ComE 1.5	Develop and implement programs to assess changes in risk and effectiveness of risk management
ComE 1.5.1	Develop system for collecting and sharing lessons learned regarding risk management

Preparedness Measures

Metric

An actionable risk management strategy that includes short, medium, and long term objectives is in place	Yes/No
Risk analysis and risk management plans are in place	Yes/No
A strategy to mitigate current risk profile has been implemented	Yes/No
Schedule and capability for updating risk analysis and risk management plans is in place	Yes/No
State, local, and private entities have been trained to conduct risk analysis	Yes/No
Monitoring program to detect changes in risk is in place	Yes/No
Program to assess program/security measures implementation is in place	Yes/No

Activity: *Assess Risks*

Definition: Assess potential targets within given system of governance as well as in relation to other systems. Identify functional as well as spatial relationships of assets and systems infrastructure and assets. This activity may be applied to assets (power generation), systems

(power supply grids), Sectors (power industry) and geographic areas (metropolitan areas). Risk management includes risks from both man made events and acts of nature.

Critical Tasks

ComE 2.1	Conduct criticality analysis (also known as screening) to identify potential targets
ComE 2.2	Conduct vulnerability assessments to assess vulnerability of potential targets to identified threats
ComE 2.3	Conduct consequence analysis of critical assets
ComE 2.4	Conduct threat assessment of potential targets
ComE 2.4.1	Conduct or obtain intelligence community threat/hazard analysis through State or local Interagency Working Groups (Joint Terrorism Task Force) to identify threats to potential targets
ComE 2.4.2	Obtain intelligence reporting and the receipt of the threat data through the Department of Homeland Security's Homeland Infrastructure Threat and Risk Analysis Center (HITRAC)
ComE 2.5	Calculate risk to potential targets based on threat, vulnerability, and consequence
ComE 2.6	Establish relative order of priorities for risk mitigation among risk portfolio
ComE 2.7	Conduct response and recovery capabilities analysis to determine capability to respond to and recover from the occurrence of identified risks

Performance Measures

Metrics

Criticality results were used to identify potential targets	Yes/No
Threat, vulnerability, and consequence results were used to assess risk for potential targets	Yes/No
A comprehensive risk assessment has been completed for potential targets identified	Yes/No
Risk assessment plans and procedures were implemented	Yes/No

Activity: *Prioritize Risks*

Definition: Rate and/or rank criticality of potential targets to mitigate or transfer associated risk (if possible) as related to given target within a system of targets

Critical Tasks

ComE 3.1	Identify potential protection, prevention, and mitigation strategies for high-risk targets
ComE 3.2	Prioritize identified strategies by risk reduction expected outcomes appreciating the various threat, vulnerabilities, and consequences that affect that community, system or asset

Performance Measures

Metrics

Risk and risk reduction results were used to prioritize risk-reduction strategies	Yes/No
Integration of a schedule and strategy to implement risk reduction strategies, including milestones, funding strategies, and opportunity costs where possible has been completed	Yes/No
Integration of a schedule and strategy for reducing the greatest risk posed to the respective stakeholder has been completed	Yes/No

Activity: *Develop Business Case*

Definition: Develop cost-benefit/cost-effectiveness analysis for consideration of applicable prescribed measures required to mitigate associated risks to an asset or system of assets; consider opportunity costs associated to one measure versus another

Critical Tasks

ComE 4.1	Develop or select methodology for cost-benefit/cost-effectiveness analysis of risk reduction solutions	
ComE 4.2	Select risk reduction solutions for implementation based on risk reduction strategies	
ComE 4.3	Allocate resources to support risk reduction solutions	
Performance Measures		Metrics
Funding priorities reflect risk assessment and prioritization of risk-reduction strategies		Yes/No
Solutions were selected and resources allocated		Yes/No
Resources were allocated and measures established to shift to a new risk reduction target		Yes/No

Activity: *Manage Risk*

Definition: Manage and monitor risk through continued assessment and analysis. Continuous consideration should be given to refresh the given threat, emerging vulnerabilities, and changing consequences to the system or assets under consideration.

Critical Tasks

ComE 5.1	Monitor the progress of solution implementation	
ComE 5.1.1	Undertake corrective actions	
Performance Measures		Metrics
Selected solutions have been verified as successfully implemented		Yes/No
Selected solutions were effective in reducing risk		Yes/No

Activity: *Conduct Risk Communication*

Definition: Develop understanding and appreciation of risk assessment, risk analysis, and risk management principles, and develop avenues for receiving information on threat, vulnerability, and consequence

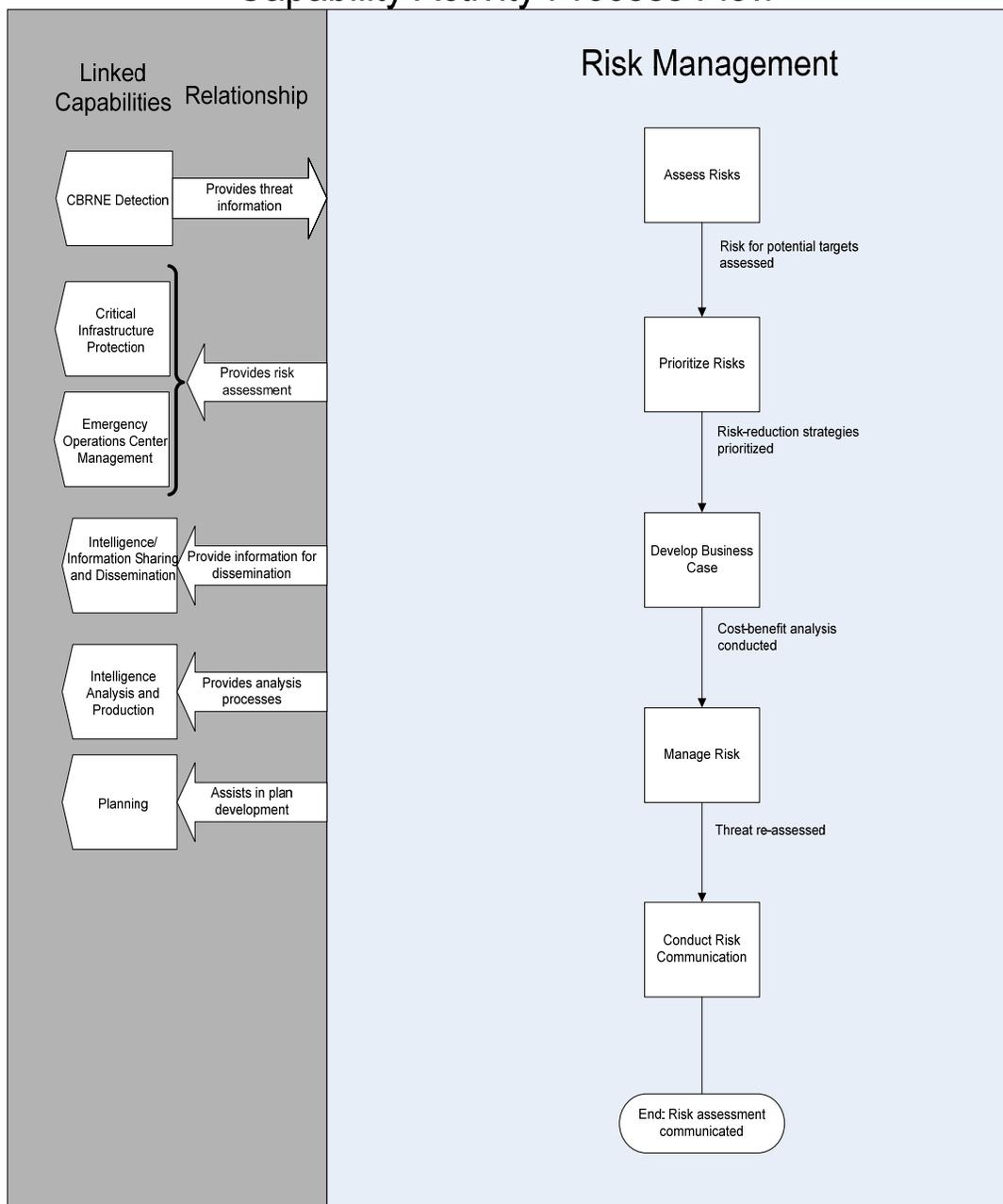
Critical Tasks

ComE 6.1	Share the assessment of sector-specific infrastructure risk with interdependent entities within appropriate sectors	
Performance Measures		Metrics
Risk management strategy is communicated regularly with stakeholders (monthly or quarterly reporting)		Yes/No

Linked Capabilities

Linked Capability	Relationship to Capability
CBRNE Detection	CBRNE Detection provides potential threat information used in the risk assessment process of Risk Management
Critical Infrastructure Protection	Critical Infrastructure Protection uses the risk assessment process to prioritize protection decisions
Emergency Operations Center Management	Risk Management provides risk assessments to Emergency Operations Center Management
Intelligence and Information Sharing and Dissemination	Risk Management provides information for Intelligence and Information Sharing and Dissemination
Intelligence Analysis and Production	Risk Management provides analysis processes to Intelligence Analysis and Production
Planning	Risk Management is a key step in the all-hazards planning process.

Capability Activity Process Flow



Resource Element Description

Resource Elements	Components and Description
Local law enforcement	Personnel with skills, ability, and training to promulgate local risk assessment and risk management strategies, with a focus on risk management, and to participate in risk communication activities
Urban Area Working Groups	Personnel with skills, ability, and training to promulgate local risk assessment and risk management strategies, with a focus on risk management, and to participate in risk communication activities
Regional Transit Security Working Groups	Personnel with skills, ability, and training to promulgate local risk assessment and risk management strategies, with a focus on risk management, and to participate in risk communication activities
Area Maritime Security Committees	Personnel with skills, ability, and training to promulgate local risk assessment and risk management strategies, with a focus on risk management, and to participate in risk communication activities
Owners and Operators of Critical Infrastructure/Key Resources (CI/KR)	Personnel with skills, ability, and training to promulgate emergency operations plans (EOPs) as part of local and regional risk management strategies, and to participate in risk communication activities
State Administrative Agencies (SAAs)	Personnel with skills, ability, and training to promulgate State-wide risk assessment and risk management strategies; to participate in risk communications activities; and to use risk reduction tools to evaluate alternate risk management strategies
Federal law enforcement and homeland security community	Personnel with skills, ability, and training to promulgate national risk assessment and risk management strategies; to participate in risk communications activities; and to create, disseminate, and use risk reduction tools to evaluate alternate risk management strategies
Joint Terrorism Task Forces (JTTFs)	Task forces formed at the local level and composed of persons from various government and private entities (e.g., law enforcement, public health, local businesses, key infrastructure representatives, emergency management, and other first responders).
National intelligence community	Personnel with skills, ability, and training to support national risk assessment and Risk Management strategies and to participate in risk communications activities. Training and formal education are keys to having a sound Risk Management background. Various levels of government will require varying levels of experience or capabilities
Risk analysis/risk management tools	Tools to facilitate risk analysis/risk management
Cost estimating tools	Tools to estimate costs of risk management decisions
Geographical Information System (GIS) data collection tools	Tools to facilitate the collection of geographically-specific data

Planning Assumptions and Definitions

- Risk assessments can be conducted in a relative manner. Calculated threat and risk ratings will not represent absolute probabilities, unless accurate probability data is readily available, but rather will be measured relative to other threats.

Target Capabilities List

- Scenario-based risk assessment will be used to evaluate threat, vulnerability, and consequence. For purposes of consistency the National Planning Scenarios should be used.
- Input will be sought from the national intelligence community, including JTTFs, to establish viable threats and the relative likelihood of those threats. To seek alignment with the National Infrastructure Protection Plan would be to use the threat analysis generated by DHS/ Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) in coordination with the intelligence community. This would provide a more authoritative and more consistent threat input.
- Scenario-specific threat assessments will include evaluation of target value, weapon availability, attack simplicity, as well as past history and specific intelligence information. Target values will require expert opinion and should be coordinated with the intelligence community and/or Federal stakeholders. Furthermore, the "intent" and "capability" of the adversary must be applied to assess terrorist threat. This approach is consistent with the DHS/NIPP threat analysis approach.
- Vulnerability analysis will measure the likelihood that specific scenarios could be executed successfully based on an evaluation of physical features, security capabilities, and response capabilities that serve to prevent an attack from being successful.
- Consequence analysis will measure the expected outcome of specific scenarios based on analysis of the susceptibility to attack of the asset given the functional characteristics of the targets, likely cascading impacts to interdependent assets, and the availability of response and recovery capabilities.
- Prevention, response, and recovery assessments will also be based on the same set of scenarios.
- Total systemic risk will be calculated as an integration of risk across all targets and scenarios within a jurisdiction.
- Appropriate protection, prevention, and mitigation solutions will be evaluated using risk-reduction tools. Threat, vulnerability, and consequence will be re-evaluated based upon implementation of solutions. Initial risk calculations serve as a benchmark against which risk reduction is measured.
- Criticality assessments will be based on critical target factors that represent the mission of targets to the Federal, State, local, and tribal entities. Considerations should be provided to the factors of human health impact, economic impact, national strategic mission impact, and psychological impact as aligned to Homeland Security Presidential Directive-7.
- Life cycle costs for identified solutions will be evaluated, including implementation costs such as training and recurring costs such as personnel and maintenance, and discounted to produce a net present cost. Where available and known, costs to upgrade will be included.
- Resources will be allocated through cost-benefit analysis, comparing total risk reduction and costs.
- From an actionable perspective, all communities of interest are responsible for risk communication. Risk communication may include but should not be limited to intelligence data, potential terrorism target selection or infrastructure selection, and anomalies which may result in prevention and or deterrence. Furthermore, there are tactical, strategic, and operational responsibilities for each respective community of interest.
- Federal, State, and local governments and the private sector all have a role in managing risk. Each should develop an understanding and appreciation of the principles of risk assessment, analysis and management. Each should develop a framework that integrates risk management in their business, and include a process for stakeholder buy-in and governance.
- There are current departmental activities aligned to develop a national baseline for risk management architecture. The Department of Homeland Security has defined the framework as the appreciation for consequence, threat, and vulnerability. Given this foundation and the work of the Department, a target architecture should be forthcoming. The National Infrastructure Protection Plan (to be released) provides a framework for the foundations of risk management. Specifically, Chapter 3 and Appendix 3 of the National Infrastructure Protection Plan.

- The work within this target capability is focused on “terrorism risk,” as it is that adversarial relationship that this target capability is designed for under the disciplines of homeland security. It is intended to establish the fundamental equations that define terrorism risk and to standardize terminology for conduct of a terrorism risk assessment. However, the ability to plan for catastrophic events such as natural disasters should be considered equally within the greater scheme of risk management.
- Although estimates can be made as to the potential goals of terrorist groups, the targets that they might select, and the types of weapons that they might use, the actions of terrorists do not absolutely conform to any set of rules or statistics. Because relatively few attacks have occurred in the United States, historical data using trend analysis cannot predict future events and may be of only limited use in predicting even the *type, time, or location* of attacks that might be launched.
- Because of the human element, there is a linkage between terrorism risks at different potential targets. Unlike most forms of risk, where the likelihood of the event occurring at any given location is independent, with terrorism the likelihood of the event occurring is very much dependent on actions that occur at other potential targets. If security measures are increased at one target (target hardening), the relative likelihood of attack can increase at other potential targets (soft targets). This happens because additional security measures could direct resources away from one target and towards others with lower levels of deterrence.
- Similarly, the relative value of a potential target can also have a major effect on the likelihood of attack. Terrorist target sites will meet certain goals for an attack, including casualties, economic disruption, or symbolic importance. A larger relative value for one potential target over another makes it more likely that the site might be attacked. Changes in the relative value of other sites could have the effect of changing the risk of terrorism at a particular site, even if no change occurred at the site itself.
- Standard algorithms and terminology for evaluating risk must be modified to deal with the effects of the human-element and of the linkages between targets.
- Target attractiveness measures the features of a particular asset that may make it more or less likely to be targeted by terrorists for a particular form of attack. Evaluation of target attractiveness should include an evaluation of two sets of features: *target value* and *deterrence*. *Target value* evaluates those features of an asset that make it more likely that an asset will be attacked; features that make the asset attractive as a target. These may include: potential for casualties, potential for economic disruption, and symbolic importance. *Deterrence* evaluates those features that make a target less likely to be attacked. These features primarily include visible security and known response capabilities.
- In instances where frequency of attack can be reasonably evaluated using statistical analysis or some other direct form of estimate, that metric can be directly used for target attractiveness.
- The Consequence of a terrorist attack is a product of the *criticality* of the target and the *impact* that an attack would have on that *criticality*.
 - $\text{Consequence} = (\text{Criticality}) \times (\text{Impact})$
- *Criticality* is broadly defined as the particular aspects or features of an asset that would make someone want to protect the asset against an attack. Generally, *criticality* is defined using a set of ‘Critical Asset Factors’. These factors define the specific features of an asset that could make it important to protect that asset from attack. Examples of typical critical asset factors include:
 - Loss of Life
 - Economic losses
 - Disruption of Government Services
 - Degradation of Critical Infrastructures and Key assets

- Symbolic and Psychological Impact
- Cascading impacts on interdependent assets
- Once the risk has been determined, the likelihood of an attack being successful can be assessed. In determining the susceptibility of an attack or “vulnerability to attack” it is assumed that the asset has been targeted, that the terrorists have the required weapon(s) and equipment, and that the attack will take place. The susceptibility then measures the probability that the attack would achieve its desired result given the constraints that are in place at the target, including physical constraints, operational constraints, and security measures.
- There are a number of methods that can be used to calculate or estimate *susceptibility*. These range from simple ratings of security capabilities to complex, simulation-based evaluations of detailed attack scenarios. The most appropriate method will depend on the type of asset and the goals of the risk assessment. In general, however, an appropriate assessment of susceptibility would include an evaluation of physical features, security capabilities, and response capabilities that serve to prevent an attack from being successful. These activities can also be categorized as those that serve to deny, detect, delay, or defend against the attack, and are addressed by other capabilities in the TCL.

Planning Factors from an In-Depth Analysis of a Scenario with Significant Demand for the Capability

Risk assessment does not focus on single incidents but rather assesses risk across a number of viable threats and critical assets.

Target Capability Preparedness Level

Resource Element Unit	Type of Element	Number of Units	Unit Measure (number per x)	Lead	Capability Activity supported by Element
Local law enforcement	Personnel	As Needed		Local	Develop Risk Framework Assess Critical Infrastructure Risks Manage Risk Conduct Risk Communication
Urban Area Working Groups	Personnel	As Needed		Local	Develop Risk Framework Assess Critical Infrastructure Risks Manage Risk Conduct Risk Communication
Regional Transit Security Working Groups	Personnel	As Needed		Local (Intrastate region)	Develop Risk Framework Assess Critical Infrastructure Risks Manage Risk

Resource Element Unit	Type of Element	Number of Units	Unit Measure (number per x)	Lead	Capability Activity supported by Element
					Conduct Risk Communication
Area Maritime Security Committees	Personnel	As Needed		Local (Intrastate region)	Develop Risk Framework Assess Critical Infrastructure Risks Manage Risk Conduct Risk Communication
Owners and operators of critical infrastructure/ key resources (CI/KR)	Personnel	As Needed		State/Local/Private Sector	Develop Risk Framework Conduct Risk Communication Assess Critical Infrastructure Risks and Manage Risk Analyze Interdependencies of Assets (Functional, Spatial)
State Administrative Agencies	Personnel	As Needed		State	Assess Critical Infrastructure Risks Prioritize Risks Develop Business Case Manage Risk Conduct Risk Communication
Federal law enforcement and homeland security community	Personnel	As Needed		Federal (DHS)	Develop Business Case Manage Risk Conduct Risk Communication
Joint Terrorism Task Forces (JTTFs)	Personnel	As Needed		Federal (DOJ, DHS)	Develop Business Case Manage Risk Conduct Risk Communication
National intelligence community	Personnel	As Needed		Federal	Develop Business Case Manage Risk Conduct Risk Communication

Resource Element Unit	Type of Element	Number of Units	Unit Measure (number per x)	Lead	Capability Activity supported by Element
Risk analysis/risk management tools	Equipment	As Needed		Federal/State/ Local	Assess Risk
Cost estimating tools	Equipment	As Needed		Federal/State/ Local	Develop Business Case Manage Risk
Geographical Information System (GIS) data collection tools	Equipment	As Needed		Federal/State/ Local	Assess Risk

References

1. National Infrastructure Protection Plan. Department of Homeland Security.
2. Homeland Security Presidential Directive/HSPD-8, "National Preparedness". December 2003. <http://www.whitehouse.gov/releases/2003/12/20031217-6.html>
3. National Response Plan (NRP). Department of Homeland Security, December 2004.
4. National Incident Management System (NIMS). Department of Homeland Security. March 2004. <http://www.dhs.gov/interweb/assetlibrary/NIMS-90-web.pdf>
5. Walker, David M. "Strategic Budgeting: Risk Management Principles Can Help DHS Allocate Resources to Highest Priorities," United States Government Accountability Office, Testimony Before the Subcommittee on Management, Integration, and Oversight, Committee on Homeland Security, House of Representatives, GAO-05-824T, June 29, 2005: <http://www/gao.gov/new.items/d05824t.p>