Risk Steering Committee

DHS Risk Lexicon

September 2008

Homeland Security

This document is presented on behalf of the Department of Homeland Security Risk Steering Committee, chaired by the Under Secretary of the National Protection and Programs Directorate and administered by the Office of Risk Management and Analysis, for the purpose described on page 2 (Project Goals and Objectives). This document is hereby recognized and approved for official use and release until revised or superseded.

Fred L. Schwien
Executive Secretary
U.S. Department of Homeland Security

Robert D. Jamison
Under Secretary National Protection and Programs Directorate
U.S. Department of Homeland Security

PREFACE

The Department of Homeland Security (DHS) is in the process of building an Integrated Risk Management Framework to improve its capability to make risk-informed strategic decisions using systematic and structured assessments of homeland security risk. The Integrated Risk Management Framework includes processes and tools that allow DHS to gather, integrate, analyze, and communicate information about risk such that it can be used to strategically prioritize efforts and resources throughout the DHS enterprise.

The DHS Risk Lexicon supports the Integrated Risk Management Framework by defining a single language for DHS risk management. Clear and unambiguous communication amongst risk practitioners, decision makers, and homeland security stakeholders is a key aspect the Departments integrated risk management capability. The DHS Risk Lexicon represents a significant step forward by making available an official set of definitions for risk-related terms for the Department.

The DHS Risk Lexicon is a product of the efforts of the Intra-Departmental DHS Risk Steering Committee (RSC). With membership from across the Department, the RSC was formed to leverage the risk management capabilities of DHS components, offices, and directorates to advance an integrated approach to risk management for DHS. The RSC has produced this DHS Risk Lexicon consisting of terms that are fundamental to the practice of homeland security risk management. The definitions in the DHS Risk Lexicon are intended to build a common vocabulary and language within the Department and enhance the ability of the DHS risk community to utilize risk information and assessments to set priorities for reducing the risks facing the Nation. The DHS Risk Lexicon is a dynamic document that will expand over time and be continually reviewed to ensure that terms and definitions are accurate and up to date.

To more effectively execute its mission it is imperative that the Department, as a whole, adopts common definitions for risk-related terminology and makes every effort to use these common definitions in written and oral communication within and across its Components. I ask for your continued cooperation in adopting these terms and definitions, and ensuring that the DHS Risk Lexicon provides an enduring resource to improve our ability to manage homeland security risk.

Robert D. Jamison
Under Secretary
National Protection and Programs Directorate
Department of Homeland Security

EXECUTIVE SUMMARY

The DHS Risk Steering Committee (RSC), chaired by the Under Secretary of the National Protection and Programs Directorate and administered by the Office of Risk Management and Analysis, has produced a DHS Risk Lexicon with definitions for 73 terms that are fundamental to the practice of homeland security risk management. The RSC is the risk governance structure for DHS, with membership from across the Department, formed to leverage the risk management capabilities of the DHS Components and to advance the Integrated Risk Management Framework (IRMF) for DHS. The DHS Risk Lexicon makes available a common, unambiguous set of official terms and definitions to ease and improve the communication of risk-related issues for DHS and its partners. It facilitates the clear exchange of structured and unstructured data that is essential to the exchange of ideas and information amongst risk practitioners by fostering consistency and uniformity in the usage of risk-related terminology for the Department.

The RSC created the Risk Lexicon Working Group (RLWG) to represent the DHS risk community of interest (COI) in the development of a professional risk lexicon. The RLWG's risk lexicon development and management process is in accordance with the DHS Lexicon Program. Terms, definitions, extended definitions, annotations and examples are developed through a collaborative process that is open to all DHS Components. Definitions are validated against risk lexicons used by other countries and professional associations, and taxonomy is developed that displays conceptual relationships between terms. Terms, definitions, extended definitions, annotations and examples, are then standardized grammatically according to the conventions of the DHS Lexicon Program.

All terms in the DHS Risk Lexicon were completed using this process and represent the collective work of the DHS risk community of interest. The DHS Risk Lexicon terms and definitions will be included as part of the DHS Lexicon, and future additions and revisions will be coordinated by the RSC and RLWG in collaboration with the DHS Lexicon Program.

The following terms have been defined for the DHS Risk Lexicon:

Table of Contents

List of Charts

INTRODUCTION

Risk is a key organizing principle for homeland security strategies, programs, efforts, and activities. The Department's risk management process, by which risk information is gathered, aggregated, analyzed, and communicated, must be supported by precise and unambiguous language. The DHS Risk Steering Committee (RSC) has initiated a DHS Risk Lexicon Project. The DHS Risk Lexicon provides a set of terms for use by the homeland security risk community, and represents an important milestone in building a unified approach to homeland security risk management and enabling integrated risk management for the Department.

The National Strategy for Homeland Security states:

> ***The assessment and management of risk underlies the full spectrum of our homeland security activities… We must apply a risk-based framework across all homeland security efforts in order to identify and assess potential hazards (including their downstream effects), determine what levels of relative risk are acceptable, and prioritize and allocate resources among all homeland security partners… We as a Nation must organize and help mature the profession of risk management by adopting common risk analysis principles and standards, as well as a professional lexicon (pg. 41)***

Risk management must be conducted not only at the level of specific component missions, but in the aggregate for broad DHS missions to enable the informed development and deployment of limited prevention, protection, response, and recovery capabilities to best effect homeland security risk reduction writ large. Such expansive use of risk management requires a common risk management approach, supported by a common lexicon, to be embedded into the Department's philosophy, practices, and business processes rather than to be viewed or practiced as a separate activity by each component. The ability to communicate precise concepts and meanings is essential for effective risk management. Clear communication allows information to be used consistently to support decisions about the nature, cause, and severity of risks. This ability to communicate homeland security risk information with precision is critical to support decision making at all levels throughout the Department.

The project has identified and defined the core terms that are essential to the practice of homeland security risk management. This DHS Risk Lexicon is intended to improve the internal management of the Department of Homeland

Security and facilitate commonplace discussions among the departmental risk community. The lexicon establishes a common vocabulary and language that will improve risk related communications between DHS components. However, it must be noted that other definitions may be found in guidance, regulations or statutes that will be specifically applicable in those regulatory or legal contexts. The DHS Risk Lexicon is not intended to create any right or benefit, substantive or procedural, enforceable at law or in equity, against the United States, its departments, agencies, or other entities, its officers or employees, or any other person.

This document presents the core terms and definitions of the DHS Risk Lexicon and a taxonomy that relates the concepts and meanings of the terms. Additionally, it describes the governance process for generating additional terms and maintaining the DHS Risk Lexicon. Finally, it lays out expectations for the adoption and use of the DHS Risk Lexicon within the DHS risk community.

A. Project Goals and Objectives

The purpose of the DHS Risk Lexicon Project is to establish and make available a comprehensive list of terms and meanings relevant to the practice of homeland security risk management and analysis. Accomplishing this goal improves the capability of DHS and its components to assess and manage homeland security risk. To support integrated risk management for the Department, the DHS Risk Lexicon:

- Promulgates a common language to ease and improve communications for DHS and its partners;
- Facilitates the clear exchange of structured and unstructured data, essential to interoperability amongst risk practitioners; and
- Garners credibility and grows relationships by providing consistency and clear understanding with regard to the usage of terms by the risk community across DHS and its components.

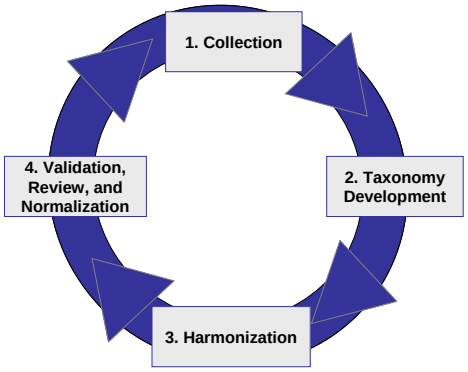
B. Project Governance

This DHS Risk Lexicon is being published by the DHS RSC. The RSC provides strategic direction for integrating risk management approaches across DHS. Working groups are created by the RSC to execute special efforts or initiatives. One of these groups is the Risk Lexicon Working Group (RLWG). The RLWG includes representatives from all DHS components and serves as the homeland

security risk community of interest (COI) in the development of a professional risk lexicon. RLWG members collectively provide the subject matter expertise necessary for the collection, normalization, and harmonization of terms and meanings in the lexicon.

The Office of Risk Management and Analysis (RMA) coordinates regular meetings of the RLWG and supports a variety of collection, documentation, and workshop activities to support the development of the DHS Risk Lexicon. RMA, in coordination with the DHS Lexicon Program, also supports the RSC in developing governance processes and procedures for the maintenance and growth of the DHS Risk Lexicon.

Definitions were developed through a four-phase process:



- **Collection:** Terms were collected from across DHS and the risk community.
- **Taxonomy Development:** Terms were organized according to the concepts they represent, facilitating consistent definitions for related terms.
- **Harmonization:** Multiple, often conflicting, definitions were harmonized to produce a single meaning for each term.
- **Validation, Review, and Normalization:** Harmonized definitions were validated against a number of non-DHS sources to ensure that the definitions produced for use in DHS are consistent with those used by the larger risk community. Proposed definitions were provided to the entire RLWG for comment. Comments were adjudicated and definitions are standardized for grammar and format.

C. Summary of Progress to Date:

Collection:

From December 2007 to March 2008, members of the RLWG collected definitions for risk-related terms from within their DHS components and offices and uploaded them into an electronic repository administered by RMA. RMA staff members worked to collect related definitions from a set of foundational policy documents that were identified in coordination with the RLWG.

Taxonomy Development:

In a series of Taxonomy Development workshops, RLWG members worked to organize terms according to their concepts and contexts. Alternative taxonomies were generated with the support of the DHS Lexicographer to ensure that they were consistent with best practices in taxonomy development. Once the RLWG reached a general consensus on a taxonomy structure, the members determined that definitions for core terms were needed to place more specialized terms into the taxonomy.

Harmonization:

RLWG members identified a set of core terms that form the foundation of the DHS Risk Lexicon. In a series of harmonization workshops, RLWG members produced definitions and examples for all terms contained in this report. In some cases, RLWG members produced extended definitions, annotations and examples to clarify the meaning of particularly complicated terms. The process by which each term was defined is described in more detail below, in Section I. C.

Validation, Review and Normalization:

Each of the core definitions has been validated against definitions from a variety of authoritative sources including lexicons used by other governments (e.g., Canada, Australia), professional societies (e.g., Society for Risk Analysis), and other entities within the Federal Government (Office of the Director of National Intelligence). The RSC has had an opportunity to review and comment on each of the core terms. Comments have been adjudicated and incorporated as appropriate. Definitions have also been standardized to ensure consistency with conventions used in the DHS Lexicon.

I. LEXICON PROCESS PHASES

A. Collection

The collection of terms for the DHS Risk Lexicon was coordinated through the RLWG, representing DHS components, directorates and offices. RLWG members collected terms that were relevant to the practice of homeland security risk management from within their respective Components and Offices. Data sources included management directives, glossaries, and other procedural or guidance documents. In addition, RMA staff reviewed foundational homeland security policy and doctrine to identify and collect relevant definitions, including the following documents:

- Unclassified Homeland Security Presidential Directives
- National Strategy for Homeland Security
- National Strategy for Physical Protection of Critical Infrastructure and Key Assets
- National Strategy to Secure Cyberspace
- DHS Strategic Plan, "Securing Our Homeland"
- National Response Framework
- National Incident Management System
- National Infrastructure Protection Plan
- Integrated Planning System
- Grant Guidance for the Homeland Security Grant Program, Port Security Grant Program, Transit Security Grant Program, and other homeland security grants
- Homeland Security Exercise and Evaluation Program Policy and Guidance

The preliminary term collection phase for the DHS Risk Lexicon lasted from December 3rd, 2007, when RLWG members began submitting terms to the electronic repository, to March 6th, 2008. Over 550 terms were entered in the electronic repository, representing 380 unique entries. This collection of terms was used to develop the taxonomy and identify the core terms that are included in this report.

B. Taxonomy Development

The DHS Lexicon is focused on the management of meanings and concepts, not just terms. This means that as a part of the DHS Lexicon, the DHS Risk Lexicon provides only a single definition for each term, unlike a dictionary which may offer multiple definitions for a term. To ensure that similar concepts are defined precisely and consistently, all terms and meanings are organized within a related hierarchy consisting of contexts, subjects, and other subdivisions.

Creating the taxonomy established the relationships between concepts and terms. The taxonomy differentiates fundamental and broad-reaching concepts from those that apply only to a specific instance or context. The taxonomy also allowed the RLWG to prioritize the order in which terms were harmonized.

RLWG members participated in a series of workshops to produce draft taxonomies. Participants generated several alternative taxonomies that organized terms by hazard class, mission area, or the threat, vulnerability, and consequence construct. RLWG members created the following set of criteria to determine a preferred taxonomic structure:

- Easy to understand
- Consistent with DHS policy and doctrine
- Applicable to the risk community across DHS and consistent with the external risk management community
- Consistent with the taxonomy conventions of the DHS Lexicon Program
- Organized consistently with specific concepts falling under broader and more encompassing topics

The RLWG determined that the preferred taxonomy would organize concepts in three major branches:

1. Terms that describe activities and efforts to manage homeland security risk (e.g., risk communication, risk assessment, risk analysis, risk management, risk mitigation, etc.)

2. Terms that describe activities and efforts to conduct risk analytics (e.g., risk assessment methodology, sensitivity analysis, probability, etc.)

3. Terms that describe the concept of homeland security risk and its different aspects (e.g., threat, hazard, vulnerability, consequence, etc.)

This structure provides the flexibility to differentiate between the way risks are understood and the process by which information about risks are gathered, aggregated, analyzed, and communicated. This division is consistent with the way that risk is discussed in the Department's existing risk management policy and doctrine and is consistent with the prevailing taxonomy conventions of the DHS Lexicon Program. The structures are broad enough to encompass the various contexts in which risk, risk management and risk analytics concepts are applied across DHS, and to ensure that the taxonomy is consistent with usage in outside sources and professional associations.

Based on the taxonomies, more than seventy terms were recommended for inclusion in the DHS Risk Lexicon. Each of these terms represents fundamental concepts in the proposed taxonomy and meets the majority of the following criteria:

- Relevant to all DHS Components with a role in risk management (i.e., broadly used terms)
- Used differently or inconsistently across the homeland security risk community
- Have specialized meaning in a homeland security context that is not captured by common usage or the dictionary definition
- Necessary for taxonomy development or the eventual definition of secondary / tertiary terms

The remaining terms submitted during the collection phase were categorized as either secondary or tertiary terms as they failed to meet the majority of the criteria for core terms.

C. Harmonization Process

The most critical phase in the lexicon development process is the synthesis, or "harmonization," of definitions received during the initial phase into a single, unified, definition.

RLWG members developed a protocol for harmonization that was consistent with DHS Lexicon Program procedures. This protocol allowed for a thorough examination of relevant sources to ensure that the harmonized definition produced by the RLWG was appropriate for DHS and the external homeland security risk community. During a series of Harmonization workshops, RLWG members discussed the available definitions and reached consensus on harmonized definitions for the core terms.

The RLWG members executed the following process to harmonize definitions:

1) Examine dictionary definitions to ensure that the eventual harmonized definition is compatible with dictionary definitions and common usage.

2) Examine definitions submitted during the collection phase, as well as DHS Lexicon submissions and DHS policy documents, to determine key concepts and requirements for a term's definition. Consult RLWG members for additional key concepts and requirements.

3) Determine if any submitted definitions contain all of the key concepts, or if multiple definitions can be modified or combined to create a definition that captures those key concepts.

4) Create a definition, based on key concepts and requirements, that is consistent with current usage.

D. Validation, Review and Normalization

Definitions contained in this report have been validated against other risk lexicons, reviewed by members of the RLWG, and standardized for grammar and format with the assistance of the DHS Lexicographer.

Validation:

Each of the proposed definitions was validated against non-DHS professional sources (lexicons from other countries, professional communities, and standards organizations) to ensure that the proposed DHS Risk Lexicon definitions are compatible with those used in the larger risk management community.

Validation sources included:

- Intelligence Experts Group All Hazards Risk Assessment Lexicon; Defense R&D Canada, Centre for Security Science; November, 2007.
- Australia / New Zealand Risk Management Standard 4360; prepared by Joint Technical Committee OB-007, Risk Management; August 2004.
- Society of Risk Analysis (SRA) Glossary; produced by the Committee for Definitions; estimated date, 2005.

- International Risk Governance Committee (IRGC) definitions from the white paper "Risk Governance, Towards an Integrated Approach"; authored by Ortwin Renn with annexes by Peter Graham; January, 2006.
- "International Standards Organization (ISO) Risk Management Vocabulary" ISO/ICE CD Guide 73; produced by Secretariat of ISO TMB WG on Risk Management; June, 2007.
- Draft Baseline Intelligence Community Policy Lexicon; produced by the Office of the Director of National Intelligence; anticipated publication in Fall 2008.

RMA staff, in support of the RLWG, cross-referenced each of the proposed core definitions with each validation source. Thirty eight of the seventy three terms included in the DHS Risk Lexicon were found in at least one of the validation sources. In the majority of cases, definitions for the DHS Risk Lexicon were consistent with definitions being used in the larger international risk community. When the definitions differed, it was usually attributed to differences in the communities that the definitions were intended to serve. (For example, the Society for Risk Analysis serves a much broader community of risk practitioners who may deal with financial or health risks, in contrast to the DHS Risk Lexicon, which is focused on homeland security risk.) In other cases, differences were due to the use of common words that have taken on a specific meaning in the domestic homeland security context. (Canada's Centre for Security Science definition for "critical infrastructure" focuses on interdependent networks, while the term is used more broadly in the United States homeland security paradigm.)

The validation effort demonstrated that the definitions in the DHS Risk Lexicon are consistent with the use of similar terms in related communities. DHS Risk Lexicon definitions are broad enough to accommodate communication with communities outside the domestic risk homeland security paradigm, but specific enough to be useful for practitioners within the DHS risk community of interest.

Review:

Validated DHS Risk Lexicon definitions were circulated to all members of the RLWG for comment before being submitted to the RSC for review. RLWG members reviewed definitions and examples and made revisions or comments as needed. RLWG members also had the opportunity to discuss available definitions as a group at the full RLWG meeting held on July 17, 2008.

RLWG member comments and revisions were adjudicated after the comment period ended. Comments were categorized by submitters as either "administrative," "substantive," or "critical." RMA staff adjudicated all administrative and substantive comments, and worked with submitters to ensure that critical comments were handled appropriately. On August 13, 2008, the RSC met to adjudicate outstanding comments from the Committee and the RLWG.

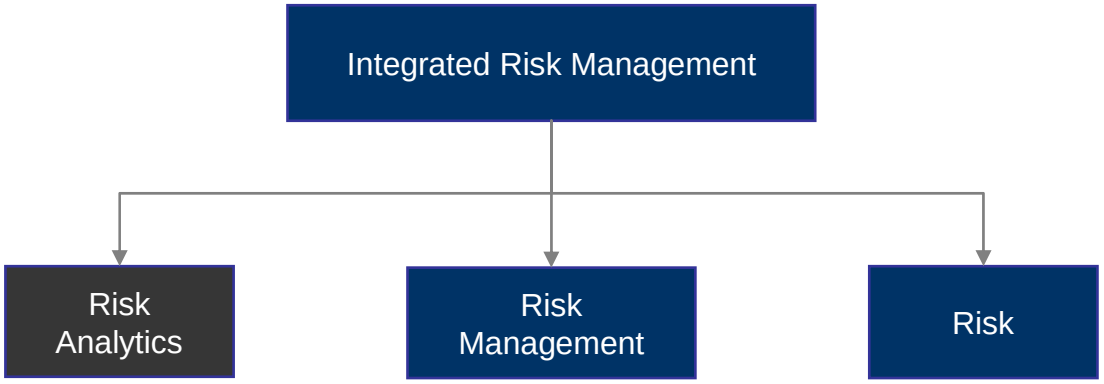
Normalization:

As a final step in producing an official definition for the DHS Risk Lexicon, definitions are vetted by the DHS Lexicographer to ensure format and grammatical consistency with the larger DHS Lexicon. They are then submitted for publication.

II. Taxonomy

The following taxonomy is intended to show conceptual relationships between terms in the DHS Risk Lexicon. The taxonomy allows the reader to understand which concepts are broad versus those that are more specific in meaning. The taxonomy is only a display of the relationships among core terms in the DHS Risk Lexicon and is not a guide for practicing risk management.

The taxonomy is divided into three major branches, shown below. The following pages display each branch of the taxonomy in detail.



Key:

Included in DHS Risk Lexicon

Serves as a taxonomy category, but is not included in the first iteration of the DHS Risk Lexicon

CHART I: RISK ANALYTICS BRANCH

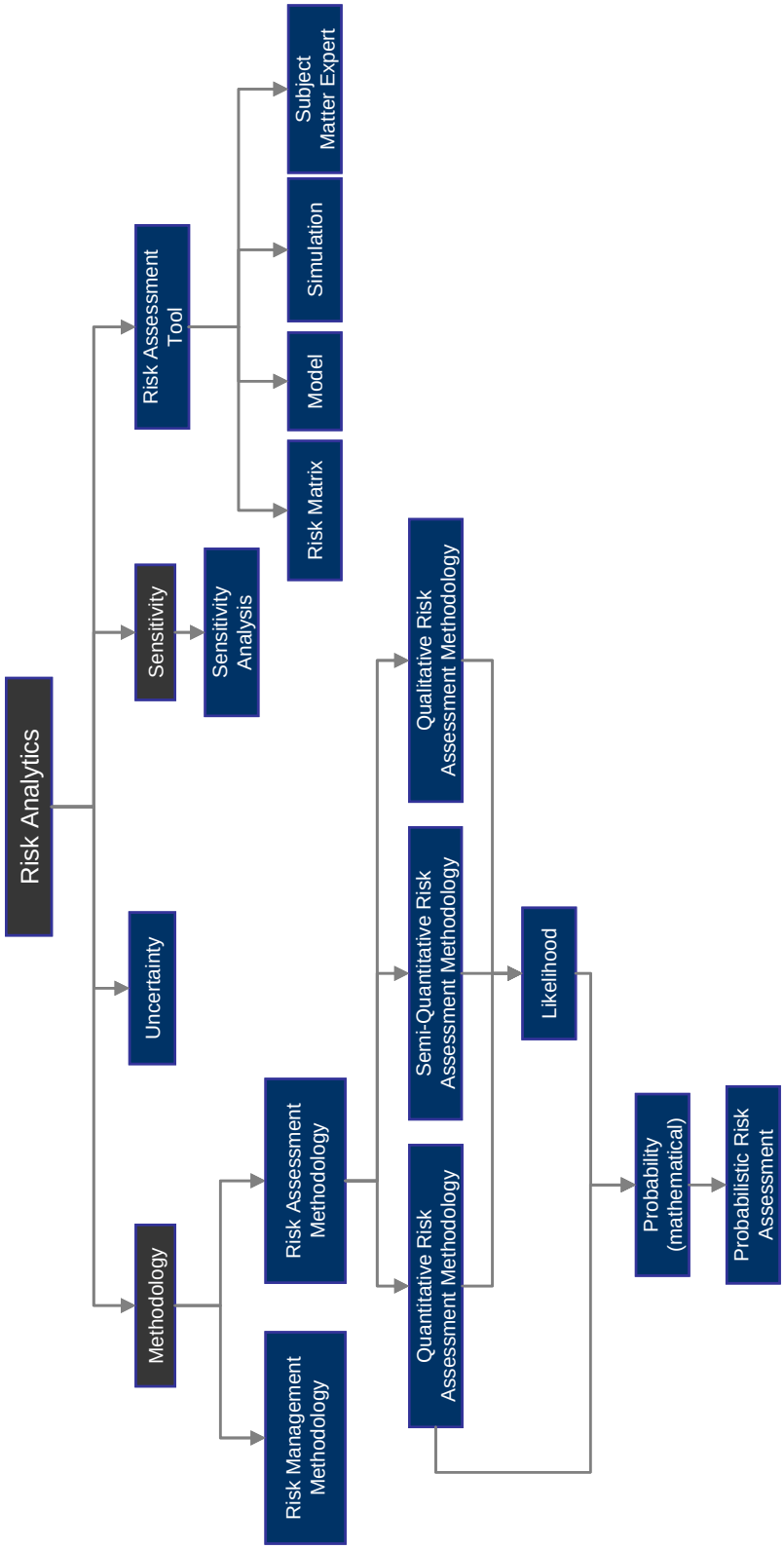


CHART II: RISK MANAGEMENT BRANCH

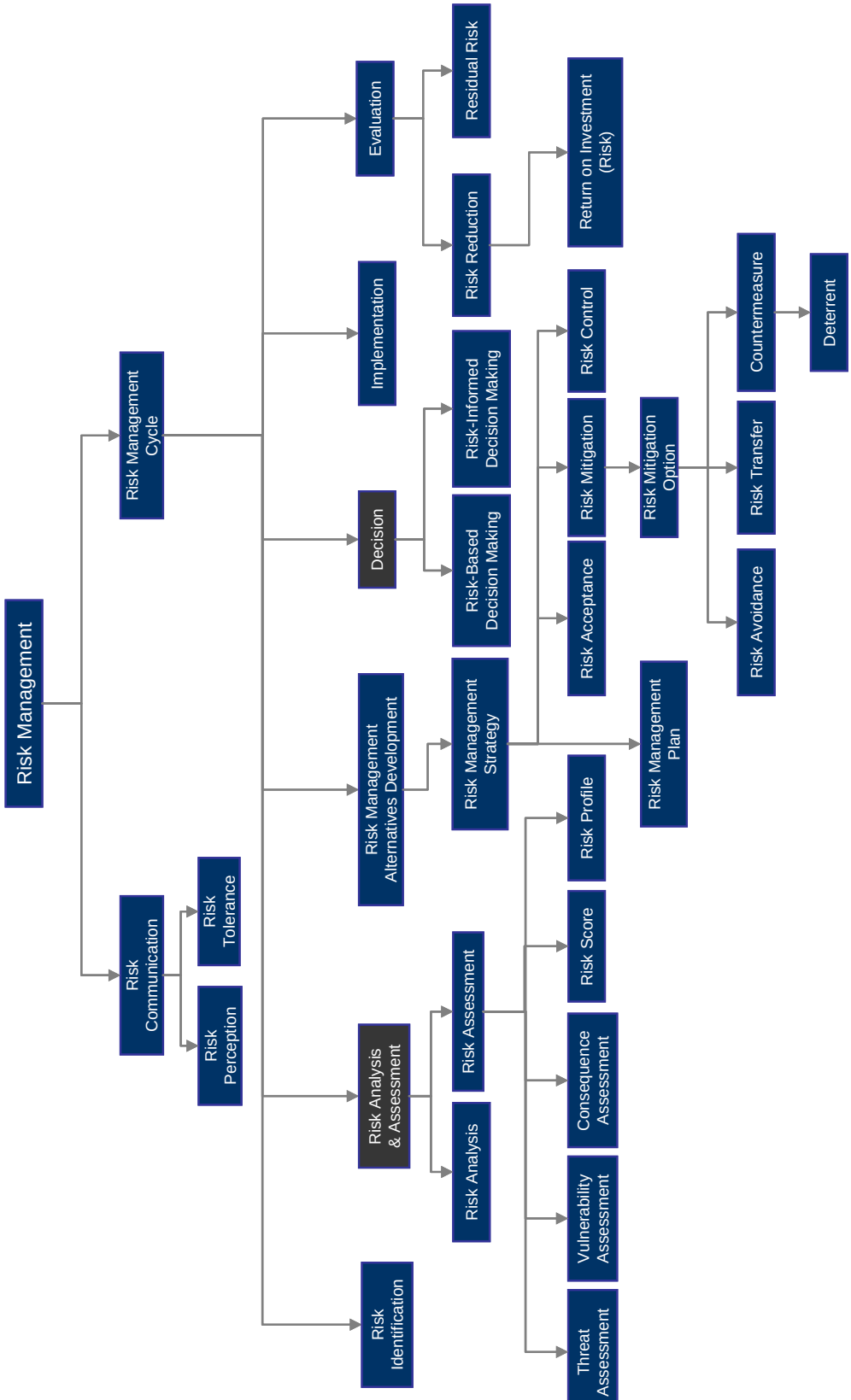
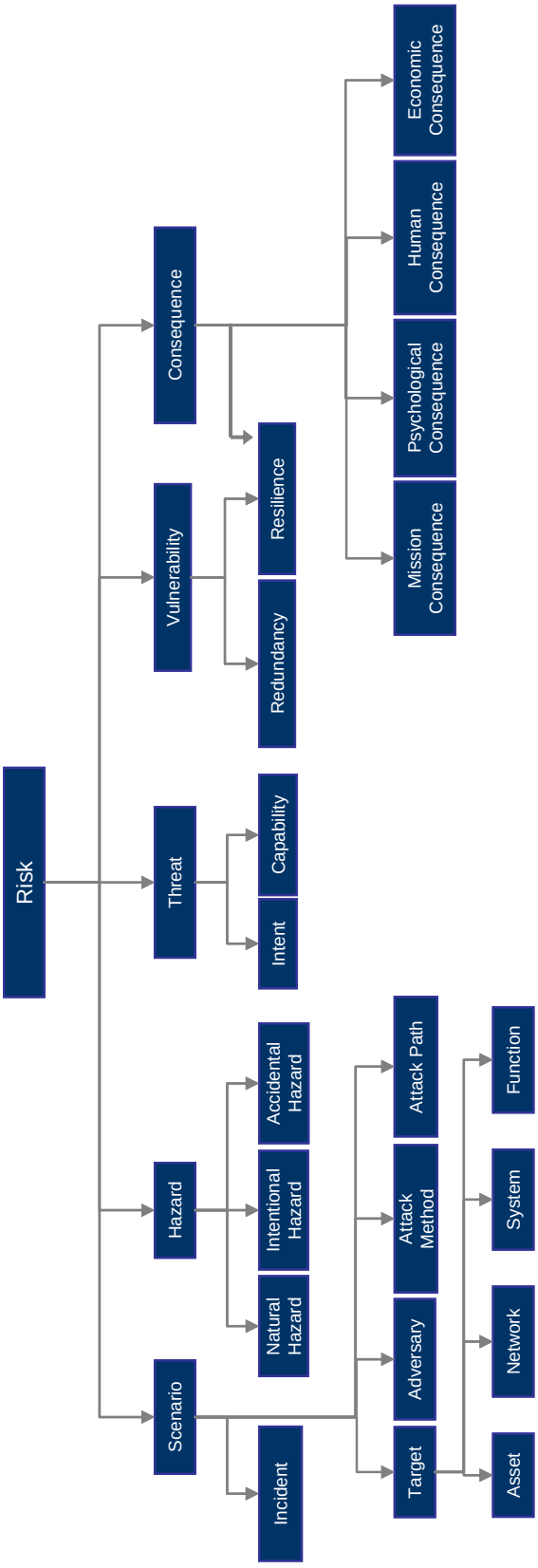


Chart III: Risk Branch



III. DEFINITIONS

ACCIDENTAL HAZARD:

Definition: source of harm or difficulty created by negligence, error, or unintended failure

Example: The chemical storage tank in the loading area without a concrete barrier may present an accidental hazard.

ADVERSARY:

Definition: individual, group, organization, or government that conducts or has the intent to conduct detrimental activities

Example: Al-Qaeda is considered an adversary of the United States.

Annotation:

1) An adversary can be hypothetical for the purposes of training, exercises, red teaming, and other activities.

2) An adversary differs from a threat in that an adversary may have the intent, but not the capability, to conduct detrimental activities, while a threat possesses both intent and capability.

ASSET:

Definition: person, structure, facility, information, material, or process that has value

Example: Some organizations use an asset inventory to plan protective security activities.

Extended Definition: includes: contracts, facilities, property, records, unobligated or unexpended balances of appropriations, and other funds or resources, personnel, intelligence, technology, or physical infrastructure, or anything useful that contributes to the success of something, such as an organizational mission; assets are things of value or properties to which value can be assigned; from an intelligence standpoint, includes any resource – person, group, relationship, instrument, installation, or supply – at the disposal of an intelligence organization for use in an operational or support role

Annotation: In some domains, capabilities and activities may be considered assets as well. In the context of the National Infrastructure Protection Plan, people are not considered assets.

ATTACK METHOD:

Definition: manner and means, including the weapon and delivery method, an adversary may use to cause harm on a target

Example: Analysts have identified weaponization of an aircraft as an attack method that terrorists may use.

Annotation: Attack method and attack mode are synonymous.

ATTACK PATH:

Definition: steps that an adversary takes or may take to plan, prepare for, and execute an attack

Example: Part of the attack path for the car bombing involved dozens of individuals moving money, arms and operatives from the terrorist safe haven to the target area.

Annotation: An attack path may include recruitment, radicalization, and training of operatives, selection and surveillance of the target, construction or procurement of weapons, funding, deployment of operatives to the target, execution of the attack, and related post-attack activities.

CAPABILITY:

Definition: means to accomplish a mission, function, or objective

Example: Counterterrorism operations are intended to reduce the capability of terrorist groups.

Annotation: Adversary capability is one of two elements, the other being adversary intent, that is commonly considered when estimating the likelihood of terrorist attacks. Adversary capability is the ability of an adversary to attack with a particular attack method. Other communities of interest may use capability to refer to any organization's ability to perform its mission, activities, and functions.

CONSEQUENCE:

Definition: effect of an event, incident, or occurrence

Example: One consequence of the explosion was the loss of over 50 lives.

Annotation: Consequence is commonly measured in four ways: human, economic, mission, and psychological, but may also include other factors such as impact on the environment.

See Also: human consequence, economic consequence, mission consequence, psychological consequence

CONSEQUENCE ASSESSMENT:

Definition: process of identifying or evaluating the potential or actual effects of an event, incident, or occurrence

Example: The consequence assessment for the hurricane included estimates for human casualties and property damage caused by the landfall of the hurricane and cascading effects.

COUNTERMEASURE:

Definition: action, measure, or device that reduces an identified risk

Example: Some facilities employ surveillance cameras as a countermeasure.

Annotation: A countermeasure can reduce any component of risk - threat, vulnerability, or consequence.

DETERRENT:

Definition: measure that discourages an action or prevents an occurrence by instilling fear, doubt, or anxiety

Example: Fear of lethal retaliation can serve as a deterrent to some adversaries.

Annotation: A deterrent reduces threat by decreasing the likelihood of an attempted attack.

ECONOMIC CONSEQUENCE:

Definition: effect of an incident, event, or occurrence on the value of property or on the production, trade, distribution, or use of income, wealth, or commodities

Example: The loss of the company's entire trucking fleet was an economic consequence of the tornado.

Annotation: When measuring economic consequence in the context of homeland security risk, consequences are usually assessed as negative and measured in monetary units.

EVALUATION:

Definition: process of examining, measuring and/or judging how well an entity, procedure, or action has met or is meeting stated objectives

Example: After increasing the number of sensors at the port, the team conducted an evaluation to determine how the sensors reduced risks to the facility.

Annotation: Evaluation is the step in the risk management cycle that measures the effectiveness of an implemented risk management option.

FUNCTION:

Definition: service, process, capability, or operation performed by an asset, system, network, or organization

Example: A primary function of the aviation industry is the transportation of people and cargo over long distances.

HAZARD:

Definition: natural or man-made source or cause of harm or difficulty

Example: Improperly maintained or protected chemical storage tanks present a potential hazard.

Annotation:

1) A hazard differs from a threat in that a threat is directed at an entity, asset, system, network, or geographic area, while a hazard is not directed.

2) A hazard can be actual or potential.

HUMAN CONSEQUENCE:

Definition: effect of an incident, event, or occurrence that results in injury, illness, or loss of life

Example: The human consequence of the attack was 20 fatalities and 50 injured persons.

Annotation: When measuring human consequence in the context of homeland security risk, consequence is assessed as negative and can include loss of life or limb, or other short-term or long-term bodily harm or illness.

IMPLEMENTATION:

Definition: act of putting a procedure or course of action into effect to support goals or achieve objectives

Example: The implementation of the emergency evacuation plan involved the activation of additional response personnel.

Annotation: Implementation is one of the stages of the risk management cycle and involves the act of executing a risk management strategy.

INCIDENT:

Definition: occurrence, caused by either human action or natural phenomena, that may cause harm and that may require action

Example: The Department of Homeland Security plays a role in reducing the risk of a catastrophic incident in the United States.

Annotation:

1) Homeland security incidents can include major disasters, emergencies, terrorist attacks, terrorist threats, wildland and urban fires, floods, hazardous materials spills, nuclear accidents, aircraft accidents, earthquakes, hurricanes, tornadoes, tropical storms, war-related disasters, public health and medical emergencies, law enforcement encounters and other occurrences requiring a mitigating response.

2) Harm can include human casualties, destruction of property, adverse economic impact, and/or damage to natural resources.

INTEGRATED RISK MANAGEMENT:

Definition: incorporation and coordination of strategy, capability, and governance to enable risk-informed decision making

Example: DHS uses a framework of integrated risk management to ensure a unified approach to managing all homeland security risks.

INTENT:

Definition: determination to achieve an objective

Example: The content of domestic extremist websites may demonstrate an intent to conduct acts of terrorism.

Annotation:

1) Adversary intent is the desire or design to conduct a type of attack or to attack a type of target.

2) Adversary intent is one of two elements, along with adversary capability, that is commonly considered when estimating the likelihood of terrorist attacks and often refers to the likelihood that an adversary will execute a chosen course of action or attempt a particular type of attack.

INTENTIONAL HAZARD:

Definition: source of harm, duress, or difficulty created by a deliberate action or a planned course of action

Example: Cyber-attacks are an intentional hazard that DHS works to prevent.

LIKELIHOOD:

Definition: estimate of the potential of an incident or event's occurrence

Example: The likelihood of natural hazards can be estimated through the examination of historical data.

Annotation:

1) Qualitative and semi-quantitative risk assessments can use qualitative estimates of likelihood such as high, medium, or low, which may be represented numerically but not mathematically. Quantitative assessments use mathematically derived values to represent likelihood.

2) The likelihood of a successful attack occurring is typically broken into two related quantities: the likelihood that an attack occurs (which is a common mathematical representation of threat), and the likelihood that the attack succeeds, given that it is attempted (which is a common mathematical representation of vulnerability). In the context of natural hazards, likelihood of occurrence is typically informed by the frequency of past incidents or occurrences.

3) The intelligence community typically estimates likelihood in bins or ranges such as "remote," "unlikely," "even chance," "probable/likely," or "almost certain."

4) Probability is a specific type of likelihood. Likelihood can be communicated using numbers (e.g. 0-100, 1-5) or phrases (e.g. low, medium, high), while probabilities must meet more stringent conditions.

See Also: Probability (Mathematical)

MISSION CONSEQUENCE:

Definition: effect of an incident, event, operation, or occurrence on the ability of an organization or group to meet a strategic objective or perform a function

Example: The city government's inability to ensure the public's access to clean drinking water was a mission consequence of the earthquake.

Annotation: Valuation of mission consequence should exclude other types of consequences (e.g., human consequence, economic consequence, etc.) if they are evaluated separately in the assessment.

MODEL:

Definition: approximation, representation, or idealization of selected aspects of the structure, behavior, operation, or other characteristics of a real-world process, concept, or system

Example: To assess risk for over 400 events, analysts created a model based on only the most important factors.

Annotation: See Also: simulation

NATURAL HAZARD:

Definition: source of harm or difficulty created by a meteorological, environmental, or geological phenomenon or combination of phenomena

Example: A natural hazard, such as an earthquake, can occur without warning.

NETWORK:

Definition: group of components that share information or interact with each other in order to perform a function

Example: Power plants, substations, and transmission lines constitute a network that creates and distributes electricity.

Annotation: Network is used across DHS to explain the joining of physical, cyber, and other entities for a particular purpose or function.

PROBABILISTIC RISK ASSESSMENT:

Definition: type of quantitative risk assessment that considers possible combinations of occurrences with associated consequences, each with an associated probability or probability distribution

Example: The engineers conducted a probabilistic risk assessment to determine the risk of a meltdown resulting from a series of compounding failures.

Annotation: Probabilistic risk assessments are typically performed on complex technological systems with tools such as fault and event trees, and Monte Carlo simulations to evaluate security risks and/or accidental failures.

PROBABILITY (MATHEMATICAL):

Definition: likelihood that is expressed as a number between 0 and 1, where 0 indicates that the occurrence is impossible and 1 indicates definite knowledge that the occurrence has happened or will happen, where the ratios between numbers reflect and maintain quantitative relationships

Example: The probability of a coin landing on "heads" is 1/2.

Annotation:

1) Probability (mathematical) is a specific type of likelihood estimate that obeys the laws of probability theory.

2) Probability is used colloquially as a synonym for likelihood.

PSYCHOLOGICAL CONSEQUENCE:

Definition: effect of an incident, event, or occurrence on the mental or emotional state of individuals or groups resulting in a change in perception and/or behavior

Example: A psychological consequence of the disease outbreak could include the reluctance of the public to visit hospitals for fear of infection, which may make it more difficult for experts to control the outbreak.

Annotation: In the context of homeland security, psychological consequences are negative and refer to the impact of an incident, event, or occurrence on the behavior or emotional and mental state of an affected population.

QUALITATIVE RISK ASSESSMENT METHODOLOGY:

Definition: set of methods, principles, or rules for assessing risk based on non-numerical categories or levels

Example: The qualitative risk assessment methodology allows for categories of "low risk," "medium risk," and "high risk."

QUANTITATIVE RISK ASSESSMENT METHODOLOGY:

Definition: set of methods, principles, or rules for assessing risks based on the use of numbers where the meanings and proportionality of values are maintained inside and outside the context of the assessment

Example: Engineers at the nuclear power plant used a quantitative risk assessment methodology to assess the risk of reactor failure.

Annotation: While a semi-quantitative methodology also involves the use of numbers, only a purely quantitative methodology uses numbers in a way that allows for the consistent use of values outside the context of the assessment.

REDUNDANCY:

Definition: additional or alternative systems, sub-systems, assets, or processes that maintain a degree of overall functionality in case of loss or failure of another system, sub-system, asset, or process

Example: A lack of redundancy in access control mechanisms is a vulnerability that can result in a higher likelihood of a successful attack.

RESIDUAL RISK:

Definition: risk that remains after risk management measures have been implemented

Example: While increased patrols lessened the likelihood of trespassers, residual risk remained due to the unlocked exterior doors.

RESILIENCE:

Definition: ability to resist, absorb, recover from or successfully adapt to adversity or a change in conditions

Example: The county was able to recover quickly from the disaster because of the resilience of governmental support systems.

Extended Definition:

1) ability of systems, infrastructures, government, business, and citizenry to resist, absorb recover from, or adapt to an adverse occurrence that may cause harm, destruction, or loss of national significance

2) capacity of an organization to recognize threats and hazards and make adjustments that will improve future protection efforts and risk reduction measures

Annotation: Resilience can be factored into vulnerability and consequence estimates when measuring risk.

RETURN ON INVESTMENT (RISK):

Definition: calculation of the value of risk reduction measures in the context of the cost of developing and implementing those measures

Example: Although the installation of new detection equipment was expensive, the team concluded that the return on investment for the new equipment was positive because of the significant reduction in risk.

RISK:

Definition: potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences

Example: The team calculated the risk of a terrorist attack after analyzing intelligence reports, vulnerability assessments, and consequence models.

Extended Definition: potential for an adverse outcome assessed as a function of threats, vulnerabilities, and consequences associated with an incident, event, or occurrence

Annotation:

1) Risk is defined as the potential for an unwanted outcome. This potential is often measured and used to compare different future situations.

2) Risk may manifest at the strategic, operational, and tactical levels.

RISK ACCEPTANCE:

Definition: explicit or implicit decision not to take an action that would affect all or part of a particular risk

Example: After determining that the cost of mitigation measures was higher than the consequence estimates, the organization decided on a strategy of risk acceptance.

Annotation: Risk acceptance is one of four risk management strategies, along with risk avoidance, risk control, and risk transfer.

RISK ANALYSIS:

Definition: systematic examination of the components and characteristics of risk

Example: Using risk analysis, the community identified the potential consequences from flooding.

Annotation: In practice, risk analysis is generally conducted to produce a risk assessment. Risk analysis can also involve aggregation of the results of risk assessments to produce a valuation of risks for the purpose of informing decisions. In addition, risk analysis can be done on proposed alternative risk management strategies to determine the likely impact of the strategies on the overall risk.

RISK ASSESSMENT:

Definition: product or process which collects information and assigns values to risks for the purpose of informing priorities, developing or comparing courses of action, and informing decision making

Example: The analysts produced a risk assessment outlining risks to the aviation industry.

Extended Definition: appraisal of the risks facing an entity, asset, system, network, geographic area or other grouping

Annotation: A risk assessment can be the resulting product created through analysis of the component parts of risk.

RISK ASSESSMENT METHODOLOGY:

Definition: set of methods, principles, or rules used to identify and assess risks and to form priorities, develop courses of action, and inform decision-making

Example: The Maritime Security Risk Analysis Model (MSRAM) is a risk assessment methodology used to assess risk at our Nation's ports.

RISK ASSESSMENT TOOL:

Definition: activity, item, or program that contributes to determining and evaluating risks

Example: A checklist is a common risk assessment tool that allows users to easily execute risk assessments in a consistent way.

Annotation: Tools can include computer software and hardware or standard forms or checklists for recording and displaying risk assessment data.

RISK AVOIDANCE:

Definition: strategies or measures taken that effectively remove exposure to a risk

Example: He exercised a strategy of risk avoidance by refusing to live in an area prone to tornados.

Annotation: Avoidance is one of a set of four commonly used risk management strategies, along with risk control, risk acceptance, and risk transfer.

RISK COMMUNICATION:

Definition: exchange of information with the goal of improving risk understanding, affecting risk perception and/or equipping people or groups to act appropriately in response to an identified risk

Annotation: Risk communication is practiced for both non-hazardous conditions and during incidents. During an incident, risk communication is intended to provide information that fosters trust and credibility in government and empowers partners, stakeholders, and the public to make the best possible decisions under extremely difficult time constraints and circumstances.

Example: As part of risk communication efforts, DHS provides information regarding the current threat level to the public.

RISK CONTROL:

Definition: deliberate action taken to reduce the potential for harm or maintain it at an acceptable level

Example: As a risk control measure, security guards screen suitcases and other packages to reduce the likelihood of dangerous articles getting inside of office buildings.

RISK IDENTIFICATION:

Definition: process of finding, recognizing, and describing potential risks

Example: During the initial risk identification for the facility's risk assessment, explosives and seismic events were chosen as scenarios to consider because of their potentially high consequences.

RISK MANAGEMENT:

Definition: process of identifying, analyzing, assessing, and communicating risk and accepting, avoiding, transferring or controlling it to an acceptable level at an acceptable cost

Annotation: The primary goal of risk management is to reduce or eliminate risk through mitigation measures (avoiding the risk or reducing the negative effect of the risk), but also includes the concepts of acceptance and/or transfer of responsibility for the risk as appropriate. Risk management principles acknowledge that, while risk often cannot be eliminated, actions can usually be taken to reduce risk.

RISK MANAGEMENT ALTERNATIVES DEVELOPMENT:

Definition: process of systematically examining risks to develop a range of options and their anticipated effects for decision makers

Example: After completing the risk management alternatives development step, the analysis team presented the mayor with a list of risk management options.

Annotation: The risk management alternatives development step of the risk management process generates options for decision-makers to consider before deciding on which option to implement.

RISK MANAGEMENT CYCLE:

Definition: sequence of steps that are systematically taken and revisited to manage risk

Example: Using the risk management cycle, the organization was able to understand and measurably decrease the risks it faced.

RISK MANAGEMENT METHODOLOGY:

Definition: set of methods, principles, or rules used to identify, analyze, assess, and communicate risk, and mitigate, accept, or control it to an acceptable level at an acceptable cost

Example: The risk management methodology recommended by the Government Accountability Office consists of five steps.

RISK MANAGEMENT PLAN:

Definition: document that identifies risks and specifies the actions that have been chosen to manage those risks

Example: Businesses often have a risk management plan to address the potential risks that they might encounter.

RISK MANAGEMENT STRATEGY:

Definition: course of action or actions to be taken in order to manage risks

Example: Mutual Aid Agreements are a risk management strategy used by some emergency response authorities to increase their capacity to respond to large scale incidents.

Extended Definition: proactive approach to reduce the usually negative impacts of various risks by choosing within a range of options that include complete avoidance of any risk that would cause harm or injury, accepting the risk, controlling the risk by employing risk mitigation options to reduce impacts, or transferring some or all of the risk to another entity based on a set of stated priorities

RISK MATRIX:

Definition: tool for ranking and displaying components of risk in an array

Example: The security staff devised a risk matrix with the likelihoods of various threats to the subway system in the rows and corresponding consequences in the columns.

Annotation: A risk matrix is typically displayed in a graphical format to show the relationship between risk components.

RISK MITIGATION:

Definition: application of measure or measures to reduce the likelihood of an unwanted occurrence and/or its consequences

Example: Through risk mitigation, the potential impact of the tsunami on the local population was greatly reduced.

Annotation: Measures may be implemented prior to, during, or after an incident, event, or occurrence.

RISK MITIGATION OPTION:

Definition: measure, device, policy, or course of action taken with the intent of reducing risk

Example: Medical professionals advised the risk mitigation option of inoculations to reduce the risk of a disease outbreak.

RISK PERCEPTION:

Definition: subjective judgment about the characteristics and/or severity of risk

Example: The fear of terrorist attacks may create a skewed risk perception.

Annotation: Risk perception may be driven by sense, emotion, or personal experience.

RISK PROFILE:

Definition: description and/or depiction of risks to an asset, system, network, geographic area or other entity

Example: A risk profile for a hydroelectric plant may address risks such as structural failure, mechanical malfunction, sabotage, and terrorism.

Annotation: A risk profile can be derived from a risk assessment; it is often used as a presentation tool to show how risks vary across comparable entities.

RISK REDUCTION:

Definition: decrease in risk through risk avoidance, risk control or risk transfer

Example: By placing vehicle barriers outside the facility, the security team achieved a significant risk reduction.

Annotation: Risk reduction may be estimated both during the decision and evaluation phases of the risk management cycle.

RISK SCORE:

Definition: numerical result of a semi-quantitative risk assessment methodology

Example: By installing a surveillance system, the chemical plant was able to reduce its risk score when the next assessment was conducted.

Extended Definition: numerical representation that gauges the combination of threat, vulnerability, and consequence at a specific moment

Annotation: The application of risk management alternatives may result in a change of risk score.

RISK TOLERANCE:

Definition: degree to which an entity is willing to accept risk

Example: After a major disaster, a community's risk tolerance may decrease significantly.

RISK TRANSFER:

Definition: action taken to manage risk that shifts some or all of the risk to another entity, asset, system, network, or geographic area

Example: A risk transfer may occur after increasing security at one facility because it might make an alternate facility a more attractive target.

Annotation: Risk transfer may refer to transferring the risk from asset to asset, asset to system, or some other combination, or shifting the responsibility for managing the risk from one authority to another (for example, responsibility for economic loss could be transferred from a homeowner to an insurance company).

RISK-BASED DECISION MAKING:

Definition: determination of a course of action predicated primarily on the assessment of risk and the expected impact of that course of action on that risk

Example: After reading about threats and vulnerabilities associated with vehicle explosives downtown, the Mayor practiced risk-based decision making by authorizing the installation of vehicle barriers.

Annotation: Risk-based decision making uses the assessment of risk as the primary decision driver, while risk-informed decision making may account for multiple sources of information not included in the assessment of risk as significant inputs to the decision process in addition to risk information. Risk-based decision making has often been used interchangeably with risk-informed decision making.

RISK-INFORMED DECISION MAKING:

Definition: determination of a course of action predicated on the assessment of risk, the expected impact of that course of action on that risk, as well as other relevant factors

Example: The Mayor practiced risk-informed decision making in planning event security by considering both the results of the risk assessment and logistical constraints.

Annotation: Risk-informed decision making may take into account multiple sources of information not included specifically in the assessment of risk as inputs to the decision process in addition to risk information, while risk-based decision making uses the assessment of risk as the primary decision driver.

SCENARIO (RISK):

Definition: hypothetical situation comprised of a hazard, an entity impacted by that hazard, and associated conditions including consequences when appropriate

Example: The team designed a scenario involving a car bomb at the power plant to help assess the risk of vehicle-borne improvised explosive devices.

Annotation: A scenario can be created and used for the purposes of training, exercise, analysis, or modeling as well as for other purposes. A scenario that has occurred or is occurring is an incident.

SEMI-QUANTITATIVE RISK ASSESSMENT METHODOLOGY:

Definition: set of methods, principles, or rules to assess risk that uses bins, scales, or representative numbers whose values and meanings are not maintained in other contexts

Example: By giving the "low risk, "medium risk," and "high risk" categories corresponding numerical values, the assessor used a semi-quantitative risk assessment methodology.

Annotation: While numbers may be used in a semi-quantitative methodology, the values are not applicable outside of the methodology, and numerical results from one methodology cannot be compared with those from other methodologies.

SENSITIVITY ANALYSIS:

Definition: process to determine how outputs of a methodology differ in response to variation of the inputs or conditions

Example: The sensitivity analysis showed that the population variable had the largest effect on the output of the model.

Annotation:

1) When a factor considered in a risk assessment has uncertainty, sensitivity analysis examines the effect that the uncertainty has on the results.

2) A sensitivity analysis can be used to examine how individual variables can affect the outputs of risk assessment methodologies.

3) Alternatively, sensitivity analysis can show decision makers or evaluators the impact or predicted impact of risk management alternatives.

SIMULATION:

Definition: model that behaves or operates like a given process, concept, or system when provided a set of controlled inputs

Example: The scientists designed a simulation to see how weather impacted the plume of smoke.

Annotation: See Also: model

SUBJECT MATTER EXPERT:

Definition: individual with in-depth knowledge in a specific area or field

Example: A subject matter expert was consulted to inform team members on improvised nuclear devices.

Annotation: Structured techniques for the elicitation of expert judgment are key tools for risk assessment. Subject matter experts are also used to supplement empirical data when needed, or to provide input on specialized subject areas for the purposes of designing and executing risk assessments.

SYSTEM:

Definition: any combination of facilities, equipment, personnel, procedures, and communications integrated for a specific purpose

Example: The collection of roads, tunnels, and bridges provided the country with the foundation for a useful transit system.

TARGET:

Definition: asset, network, system or geographic area chosen by an adversary to be impacted by an attack

Example: Analysts identified mass gatherings as one potential target of an attack.

THREAT:

Definition: natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment and/or property

Example: Intelligence suggested that the greatest threat to the building was from explosives concealed in a vehicle.

Annotation: Threat as defined refers to an individual, entity, action, or occurrence; however, for the purpose of calculating risk, the threat of an intentional hazard is generally estimated as the likelihood of an attack (that accounts for both the intent and capability of the adversary) being attempted by an adversary; for other hazards, threat is generally estimated as the likelihood that a hazard will manifest.

THREAT ASSESSMENT:

Definition: process of identifying or evaluating entities, actions, or occurrences, whether natural or man-made, that have or indicate the potential to harm life, information, operations and/or property

Example: Analysts produced a threat assessment detailing the capabilities of domestic and foreign terrorist organizations to threaten particular infrastructure sectors.

UNCERTAINTY:

Definition: degree to which a calculated, estimated, or observed value may deviate from the true value

Example: The uncertainty in the fatality estimate for the chemical attack was due to the unpredictable wind direction in the affected area.

Annotation:

1) Uncertainty may stem from many causes, including the lack of information.

2) The concept of uncertainty is useful in understanding that likelihoods and consequences can oftentimes not be predicted with a high degree of precision or accuracy.

VULNERABILITY:

Definition: physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard

Example: Installation of vehicle barriers may remove a vulnerability related to attacks using vehicle-borne improvised explosive devices.

Extended Definition: characteristic of design, location, security posture, operation, or any combination thereof, that renders an asset, system, network, or entity susceptible to disruption, destruction, or exploitation

Annotation: In calculating risk of an intentional hazard, the common measurement of vulnerability is the likelihood that an attack is successful, given that it is attempted.

VULNERABILITY ASSESSMENT:

Definition: process for identifying physical features or operational attributes that render an entity, asset, system, network, or geographic area susceptible or exposed to hazards

Example: The team conducted a vulnerability assessment on the ship to determine how it might be exploited or attacked by an adversary.

Annotation: Vulnerability assessments can produce comparable estimates of vulnerabilities across a variety of hazards or assets, systems, or networks.

IV. Governance Structure for DHS Lexicon

The Lexicon Section of the Office of the DHS Executive Secretariat (DHS ESEC) is responsible for the management of controlled vocabulary for DHS. Lexicon Section works with various COIs (e.g., law enforcement, immigration, data, training, risk, etc.) to ensure that appropriate meanings are assigned to terms and that a controlled vocabulary is maintained. Its mission is to provide a consistent methodology and structure to be used in the development of topical glossaries and an official Lexicon for the Department. These include specific glossaries supporting Advanced Distributed Learning system lesson modules as well as broader ones related to subject areas such as law enforcement, training and education, and risk management. The RSC, through the RLWG, represents the risk COI for the management of risk-related terms, and the DHS ESEC and the RSC work together to manage the maintenance and growth of the DHS Risk Lexicon.

A. The DHS Executive Secretariat

The DHS ESEC ensures that executive correspondence, communications, and reports are efficient, purposeful, coordinated, and controlled. Working closely with its counterparts throughout DHS, ESEC assures correct and timely production and transmission of official materials.

B. Risk Steering Committee

RMA leads the development, implementation, and sharing of integrated risk management approaches to support the management of homeland security risk. The RSC is the risk governance structure for the Department, formed to ensure that risk management is carried out consistently and compatibly throughout DHS. The RSC is made up of three tiers: Tier I, which is comprised of Component Heads; Tier II, which is comprised of individuals at the sub component; and Tier III, which is comprised of Action Officers. The RSC is a forum to exchange information, identify analytical guidelines, and vet and approve standards and integrated approaches to risk management across DHS. The RSC also oversees a number of working groups, one of which is the RLWG.

The RLWG supports the RSC in developing the DHS Risk Lexicon. The RLWG is responsible for building the DHS Risk Lexicon and managing the meanings contained within it. RLWG members collectively provide the subject matter

expertise necessary for the collection, harmonization, and normalization of terms and meanings. These activities are coordinated through regular meetings of the RLWG and are supported and facilitated by RMA and the DHS Lexicon Section.

V. MAINTENANCE OF THE DHS RISK LEXICON

The DHS Risk Lexicon will continue to grow and mature even after this publication of terms and definitions. Institutionalizing the use of a common risk language requires a set of processes to ensure that the DHS Risk Lexicon remains relevant to the practice of homeland security risk management as the Department's approaches to an integrated risk management framework matures. The DHS Risk Lexicon must be constantly maintained and updated to adequately support the risk community of interest and to reflect the Department's most current thinking on risk.

Maintenance processes ensure that:

- Definitions and examples for terms in the DHS Risk Lexicon remain up-to-date and relevant to practitioners of homeland security risk management
- New terms are added to the DHS Risk Lexicon to ensure effective communication and cooperation amongst risk practitioners for both new and established methods and concepts
- Definitions in the DHS Risk Lexicon are validated against other similar Federal and interagency efforts as they become available to promote consistency throughout the community for the use of risk-related terms
- An up-to-date version of the DHS Risk Lexicon of terms is available throughout the Department
- A procedure exists to notify the risk community of interest of additions or edits to the DHS Risk Lexicon

The DHS Risk Lexicon is maintained through an ongoing and cooperative effort involving both the RLWG and the DHS Lexicon Section. In its role representing the risk management community of interest, the RLWG oversees the introduction of additional terms as well as revisions to published terms.

To establish the DHS Risk Lexicon, the RLWG has convened monthly meetings and numerous smaller workshops and sessions since its creation in December 2007. From the date of this publication, the RLWG will oversee the maintenance and growth of the Lexicon through quarterly meetings, with additional sessions as needed. Meeting schedules are coordinated by RMA in support of the RSC.

The RLWG supports the growth and maintenance of the DHS Risk Lexicon through the following functions:

A. Maintenance of Existing Terms:

Revisions to existing terms and definitions are coordinated through and adjudicated by the RLWG and the DHS Lexicon Section. Requested revisions shall be recorded on the comment form provided in Appendix B of this document and submitted via the RSC Tier-III / RLWG representative from the Component of the individual requesting the revision. The Component representative should send the completed comment form to Lexicon@dhs.gov and to RMAexecsec@hq.dhs.gov

The DHS Lexicon Program welcomes all comments and proposed revisions to the DHS Risk Lexicon, and has delegated the RLWG, as the risk COI for the Department, to adjudicate those comments. As comments are received on existing terms, RMA, in support of the RSC, will compile and record all requests for revision and will liaise with the individual Component who submitted the comment. Substantive and critical comments shall be discussed during the first scheduled RLWG meeting following the submission of the comment form. Administrative comments shall be adjudicated on a case-by-case basis and may or may not be brought to the attention of the RLWG. A Component is encouraged to participate in the RLWG meeting at which their comment is reviewed; if the individual is not a member of the RLWG, he or she may attend at the discretion of the Component RSC Tier-III / RLWG representative.

If the RLWG accepts a proposed revision, RMA shall recommend the change to the DHS Lexicon Section of DHS ESEC. The revision is then entered into the official revision process that governs the DHS Lexicon. If the DHS Lexicon Section accepts the revision, RMA shall ensure that the changes are reflected in official DHS Risk Lexicon documentation.

B. Addition of New Terms:

To be included in the DHS Risk Lexicon, terms must relate specifically to the practice of homeland security risk management. New terms may be submitted through a Component's RSC Tier-III / RLWG representative or through the DHS Lexicon Section. Proposed additional terms submitted to DHS ESEC will be forwarded to the RLWG. The RLWG coordinates the addition of terms into the DHS Risk Lexicon on the submitter's behalf, although the submitter is welcome to participate as appropriate in the process. Submitters can send

single terms or lists of terms to Lexicon@dhs.gov with a copy (Cc) to RMAexecsec@hq.dhs.gov, or submit terms through their Component's RSC Tier-III representative.

The DHS Lexicon Section and RMA staff will compare all proposed additional terms against the existing repository. Any terms that are unique and only used by a single Component or small group will be formatted and added to the repository. If the term or a similar term already exists in the repository, the definitions shall be harmonized and validated by the RLWG as described in Section I of this document.

Each proposed additional term and definition shall be discussed individually at the first scheduled RLWG meeting following the submission of the term. If the RLWG accepts the proposed addition, RMA shall recommend the addition of the term to the DHS Lexicon Section of DHS ESEC to ensure that the changes are reflected in official DHS Risk Lexicon documentation.

C. Consistency with Related Federal/Interagency Efforts:

Ensuring that DHS Risk Lexicon definitions are generally consistent with related definitions used throughout the Federal interagency supports the broader goal of effective communication and coordination of risk-related efforts throughout the Federal Government. RMA continually collects information on risk-related lexicons and glossaries as they become available throughout the Federal government. In addition, RMA will survey the RSC and RLWG membership every six months to determine if they are aware of any new risk-related glossaries or efforts. As glossaries and lexicons are identified, they shall be used as validation sources and compared to existing DHS Risk Lexicon definitions using the process described in Section I. D. of this report (Validation, Review and Normalization). RMA shall conduct outreach to other Federal Government entities as appropriate to ensure consistency with the definitions in the DHS Risk Lexicon.

D. Availability:

The most current version of the DHS Risk Lexicon is available through the DHS Executive Secretariat homepage on DHS Online. DHS Online can be accessed through https://dhsonline.dhs.gov/portal/jhtml/community.jhtml.

RMA works with the Lexicon Section of DHS ESEC to ensure that the DHS intranet website references the most up-to-date version of the DHS Risk Lexicon. Those interested in obtaining a copy of the most current version can also contact RMA or their representative on the RSC Tier-III / RLWG.

E. Notification of Updates:

RMA coordinates notifications of updates to the DHS Risk Lexicon through the RSC. Committee members are provided with a record of any changes to established definitions or additions to the DHS Risk Lexicon during regular meetings of the RSC Tier-III. RSC members are responsible for informing individuals within their Components of changes that may affect how they use terms found in the DHS Risk Lexicon.

VI. USE OF THE DHS RISK LEXICON

The DHS Risk Lexicon must be used throughout DHS for it to accomplish the goal of facilitating the clear exchange of structured and unstructured data, essential to the interoperability of terms amongst risk practitioners. The requirement to institutionalize the use of the DHS Risk Lexicon is supported by multiple areas of effort, including:

- Ensuring that official terms and meanings from the DHS Lexicon are incorporated into institutional doctrine
- Socializing the existence of the DHS Risk Lexicon with the current community of risk practitioners and supporting them as they adopt its definitions for use within their Components
- Incorporating DHS Risk Lexicon definitions into training and education materials relevant to the practice of homeland security risk management
- Promoting the use of consistent risk-related language in documents and communications throughout DHS through the RSC & ESEC

As part of its mission to build an institutionalized IRM framework for DHS, RMA monitors efforts to create or revise foundational policy documents. Leveraging partnerships throughout the Department, RMA advocates for the inclusion of DHS Risk Lexicon definitions in cornerstone Departmental documents that support the Homeland Security Management System and the use of risk throughout DHS.

To advocate for the adoption of the DHS Risk Lexicon across the risk COI, RMA works with RSC representatives to reinforce awareness with practitioners at the Component level. RMA also advocates for the use of the DHS Risk Lexicon and the definitions contained within it through partnerships with other DHS Components and their activities, including support to grant programs and the Program Planning Budget and Execution (PPBE) process, planning activities, methodology support, and other related efforts. RMA will incorporate the definitions contained in the DHS Risk Lexicon into materials it produces, including analytic guidelines, standards, and other documents.

RMA is currently identifying training opportunities within DHS that relate to the practice of homeland security risk management. RMA is also working with RSC members to identify training opportunities within their Components and Offices and advocates for the inclusion of DHS Risk Lexicon definitions in training and education materials as appropriate.

VII. APPENDICES

APPENDIX A: COMMENT/REVISION FORM

DHS Risk Lexicon Comment Form Return to Lexicon@dhs.gov and RMAexecsec@hq.dhs.gov				
Submitted Category **C - Critical** **S - Substantial** **A - Administrative**	**Submitter's Name, Position, Email, Phone**	**Text to be Changed**	**Reasoning for Proposed Change**	**Recommended Solution Language**

Appendix B: Lexicon Contact Information

DHS Lexicon
DHS Lexicographer
United States Department of Homeland Security
Office of the Secretary
Office of the Executive Secretariat
DHS Lexicon Section

(202) 447-3518 (NAC)
lexicon@dhs.gov

DHS Risk Lexicon
Office of Risk Management and Analysis
United States Department of Homeland Security
National Protection and Programs Directorate

rmaexecsec@hq.dhs.gov

Appendix C: Common DHS Acronyms for Risk methodologies and Programs

This appendix provides acronyms for risk methodologies, programs and other terms frequently used in DHS, along with a brief description of each.

ADRA:

Long Form: Air Domain Risk Assessment

Description: A Transportation Security Administration risk assessment methodology established to rank risk to generic United States air domain assets (airports, airplanes, navigation towers, general aviation, charter, etc.) from acts of terrorism.

BZPP:

Long Form: Buffer Zone Protection Program

Description: A DHS-administered grant program designed to help local law enforcement and owners and operators of critical infrastructure and key resources increase security in the "buffer zone" – the area outside of a facility that can be used by an adversary to conduct surveillance or launch an attack.

C/ACAMS:

Long Form: Constellation/Automated Critical Asset Management System

Description: A system that provides a capability for State and local users to build and manage inventories of local infrastructures, conduct vulnerability assessments of those infrastructures, develop incident response plans, and build and generate a wide range of reports.

CAPRA:

Long Form: Critical Asset and Portfolio Risk Analysis

Description: A methodology developed at the University of Maryland for use by the Maryland Emergency Management Agency for input into their Critical Asset Database.

CARVER:

Long Form: Criticality, Accessibility, Recuperability, Vulnerability, Effect and Recognizability

Description: A mnemonic composed of the above terms, that when applied to security risk management, are used to characterize assets.

CFIUS:

Long Form: Committee on Foreign Investment in the United States

Description: An inter-agency committee of the United States Government, chaired by the Secretary of the Treasury, that reviews the national security implications of foreign investments in U.S. companies or operations.

CIKR:

Long Form: Critical Infrastructure and Key Resources

Description: Critical Infrastructure are the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof. Key Resources are publicly or privately controlled resources essential to the minimal operations of the economy and government.

CIII:

Long Form: Critical Infrastructure Interdependencies Integrator

Description: A Monte Carlo simulation tool developed in conjunction with Argonne National Laboratory that measures the time and cost of asset recovery and restoration for critical infrastructure. This acronym is sometimes displayed as CI^3.

CIKR CRM:

Long Form: Critical Infrastructure and Key Resources Common Risk Model

Description: An Office of Infrastructure Protection quantitative scenario risk assessment methodology designed to enable defensible cross-sector comparisons and comparisons of risk to combinations of infrastructure

within a jurisdiction, sector, or attack type. The methodology is designed to support return-on-investment evaluations of potential risk management alternatives.

CIMS:

Long Form: Critical Infrastructure Modeling System

Description: A system created by the Idaho National Laboratory as a high level model designed to identify interdependencies that exist across multiple infrastructure sectors.

CIPDSS:

Long Form: Critical Infrastructure Protection Decision Support System

Description: An Office of Infrastructure Protection system for analysis of cross-sector critical infrastructure consequences.

CR:

Long Form: Comprehensive Review

Description: A cooperative, government-led analysis of CIKR to determine facilities' risk of a potential terrorist attack, the consequences of such an attack, and the integrated prevention and response capabilities of the owner and operator, local law enforcement, and emergency response organizations.

CTMS:

Long Form: CREATE Terrorism Modeling System

Description: The Homeland Security Center for Risk and Economic Analysis of Terrorism Events (CREATE) methodology and software system for assessing risks of terrorism within the framework of economic analysis and structured decision making.

CTMS / TMS:

Long Form: CREATE Terrorism Modeling System / Terrorism Magnitude Scale

Description: A base-10 logarithmic scale, produced in the CTMS. It measures human, financial, and symbolic consequences of the scenarios the CTMS produces.

ECIP Assessment:

Long Form: Enhanced Critical Infrastructure Protection Assessment

Description: An assessment conducted to identify vulnerabilities and enhance security in collaboration with Federal, State, local and private sector stakeholders.

FAIT:

Long Form: Fast Analysis Infrastructure Tool

Description: Created by the National Infrastructure Analysis Center under DHS direction, the tool produces regional economic analysis, asset descriptions, and other important information on assets for the National Infrastructure Analysis Center's internal analysts.

HAZUS:

Long Form: Hazards United States

Description: Developed by the Federal Emergency Management Agency, a nationally applicable standardized methodology and software program that estimates potential losses from earthquakes, hurricane winds, and floods.

HIRA:

Long Form: Hazard Identification and Risk Assessment

Description: A DHS methodology designed to identify hazards and associated risk to persons, property, and structures.

IEISS:

Long Form: Interdependent Energy Infrastructure Simulation System

Description: Created by Los Alamos National Laboratories as a tool to study the interdependency relationships within and among energy subsectors including the benefits of investment to infrastructure.

IRAPP:

Long Form: Infrastructure Risk Assessment Partnership Program

Description: A framework for working with state authorities to develop, evaluate and support the implementation of CIKR risk assessment and risk management decision support processes in a state/local environment.

JSERA:

Long Form: Joint Special Events Risk Assessment

Description: An Office of Infrastructure Protection risk assessment methodology that provides operationally relevant risk and risk-informed analysis capable of assisting partners with decision making related to special events.

MAST:

Long Form: Maritime Security and Strategic Toolkit

Description: A tool designed to enhance Area Maritime Security Plans and allow ports to better integrate their security efforts into the broader Urban Areas Security Initiative planning construct.

MD SHARPP:

Long Form: Mission, Demography, Symbolism, History, Accessibility, Recognizability, Population and Proximity

Description: A mnemonic conceived as a numeric assessment in which each of the criteria are evaluated and combined to produce an overall score. In security risk management this score is typically applied to key assets.

MSRAM:

Long Form: Maritime Security Risk Assessment Model

Description: A United States Coast Guard model designed to identify and prioritize risks to ports, waterways, and associated facilities.

MTI:

Long Form: Methodology Technical Implementation

Description: A program within the Infrastructure Information Collection Division that collaborates with the Sector Specific Agencies, Sector Coordinating Councils, and Government Coordinating Councils of each of the CIKR sectors to integrate risk and vulnerability assessment methodologies into automated tools to enable the identification, analysis, and management of sector-specific security risks.

NEXT GENERATION ABEL:

Long Form: Next Generation Agent Based Economic Laboratory

Description: A high resolution macroeconomic model created by the Sandia National Laboratory that measures economic factors, feedbacks, and downstream effects of infrastructure interdependencies.

NISAC:

Long Form: National Infrastructure Simulation and Analysis Center

Description: An Office of Infrastructure Protection organization, including elements of Los Alamos and Sandia National Laboratories, created to develop and implement advanced modeling, simulation, and analysis capabilities to identify dependencies and interdependencies in the Nation's CIKR and potential cross-sector consequences of disruption to CIKR functioning.

NMSRA:

Long Form: National Maritime Strategic Risk Assessment

Description: A United States Coast Guard all-mission risk assessment that informs budget and planning guidance.

NTSRA:

Long Form: National Transportation Sector Risk Assessment

Description: A Transportation Security Administration risk assessment established to evaluate threats, vulnerabilities, and consequences of selected terrorist attack scenarios, identify needs for more detailed analysis, inform planning decisions, and establish a baseline for other

periodic analyses and analytical activities related to transportation security.

OCTAVE:

Long Form: Operationally Critical Threat, Asset, and Vulnerability Evaluation

Description: An information system analysis tool designed for large organizations and sponsored by the U.S. Department of Defense.

PAWSA:

Long Form: Ports and Waterways Safety Assessment

Description: A United States Coast Guard risk assessment methodology designed to identify major waterway safety hazards, estimate risk levels, and evaluate potential mitigation measures.

RAMCAP:

Long Form: Risk Analysis and Management for Critical Asset Protection

Description: A risk methodology that uses a common risk framework for owners and operators of the nation's critical infrastructure to assess terrorist risk to their own assets and systems.

RAPID:

Long Form: Risk Assessment Process for Informed Decision Making

Description: An Office of Risk Management and Analysis program aimed at developing a strategic-level process to gauge future risks across the full range of DHS responsibilities to inform the DHS's annual Planning, Programming, Budgeting, and Execution cycle of resource allocation decisions.

RMAT:

Long Form: Risk Management Assessment Tool

Description: A Transportation Security Administration agent based model for analyzing and making decisions about risk reduction options based on threat, vulnerability, and consequence data.

RSAT:

Long Form: Risk Self Assessment Tool

Description: A tool, formerly known as the Vulnerability Identification Self Assessment Tool (VISAT), used within the Commercial Facilities Sector, public assembly subsector, to conduct risk assessments at individual venues. RSAT (sometimes displayed as R-SAT) assists owner-operators with the identification of vulnerabilities and risks and provides recommendations for improving a venue's overall security posture.

SAV:

Long Form: Site Assistance Visit

Description: Facility vulnerability assessment jointly conducted by DHS in coordination and cooperation with Federal, State, and local officials, and CIKR owners and operators.

SEAR:

Long Form: Special Events Assessment Rating

Description: An Office of Operations Coordination effort to provide a single Federal interagency resource to assess and categorize the risk to domestic special events that do not rise to the level of a National Special Security Event.

SHIELD:

Long Form: Strategic Hazard Identification Evaluation for Leadership Decisions

Description: Collaboration between the Office of National Capital Region Coordination and the Office of Risk Management and Analysis to create a regional risk management model.

SHIRA:

Long Form: Strategic Homeland Infrastructure Risk Assessment

Description: An annual collaborative process conducted in coordination with the infrastructure protection and intelligence communities to assess and analyze the risks to the Nation's critical infrastructure and key resource sectors from natural and manmade hazards.

SNJTK:

Long Form: Special Needs Jurisdiction Tool Kit

Description: A methodology developed by the Office for Domestic Preparedness (later the Office of Grants and Training, the functions of which have been reassigned to the Federal Emergency Management Agency) designed to address jurisdictions with special needs, or specifically, jurisdictions with unique and complex circumstances where it is necessary to compare relative risk levels across dissimilar assets and critical infrastructure.

SNJTK / CAF:

Long Form: Special Needs Jurisdiction Tool Kit / Critical Asset Factor

Description: A primary component of the SNJTK that represents characteristics of assets that would result in significant negative impact to the organization if an asset were lost.

STAR:

Long Form: Strategic Threat and Action Report

Description: A precursor to SHIRA that provided decision makers with a comparative assessment of risks to the Nation and the actions taken to manage those risks.

TRAGIS:

Long Form: Transportation Routing Analysis Geographic Information System

Description: A model created by the Oak Ridge National Laboratory used to illustrate highway, rail, and waterway routes across the Nation and to determine optimal routes for normal and abnormal states of infrastructure operation.

TRAM:

Long Form: Transit Risk Assessment Methodology

Description: A Federal Emergency Management Agency process that leverages past assessments of vulnerability with threat and consequence information to create a roadmap for making funding allocation decisions.

TRAVEL:

Long Form: Transportation Risk Assessment and Vulnerability Evaluation Tool

Description: A Transportation Security Administration tool that is used in facilitated, on-site assessments of transportation assets.

VISAT:

Long Form: Vulnerability Identification Self-Assessment Tool

Description: VISAT will be renamed as RSAT as of January 2009; for information please see RSAT entry above.

WISE:

Long Form: Water Infrastructure Simulation Environment

Description: A tool created by the Los Alamos National Laboratories that is similar to the IEISS, which studies the interdependency relationships within and between the water sectors in-depth and models the benefits of investment to this infrastructure.