Risk Steering Committee

DHS Risk Lexicon

2010 Edition

September 2010

Homeland Security

This page is intentionally left blank.

This publication is presented on behalf of the Department of Homeland Security Risk Steering Committee, chaired by the Under Secretary for the National Protection and Programs Directorate and administered by the Office of Risk Management and Analysis, for the purpose described on page 1 (Project Goals and Objectives).

Pursuant to the authority vested in Under Secretary for the National Protection and Programs Directorate by the Secretary of Homeland Security in Delegation Number 17001 to lead the Department's efforts to establish a common framework to address the overall management and analysis of homeland security risk, this publication is hereby recognized and approved for official use and release until revised or superseded.

Philip A. McNamara
Executive Secretary
U.S. Department of Homeland Security

Rand Beers
Under Secretary
National Protection and Programs Directorate
U.S. Department of Homeland Security

This page is intentionally left blank.

PREFACE

The Department of Homeland Security (DHS) improves its ability to make risk-informed decisions by conducting systematic and structured assessments of homeland security risk. This ongoing effort includes the development of processes and tools, to gather, integrate, analyze, and communicate information about risk. These tools, like the DHS Risk Lexicon, aid the Homeland Security Enterprise in strategically prioritizing efforts and resources.

Clear and unambiguous communication among homeland security risk practitioners, decision makers, and stakeholders is necessary to achieve integrated risk management. The DHS Risk Lexicon supports integrated risk management by defining a single language for risk management and analysis. The DHS Risk Lexicon makes available an official set of harmonized risk-related terms and definitions.

If the Department, as a whole, adopts common definitions for risk-related terminology and uses these common definitions in written and oral communication, we will continue to improve our ability to manage homeland security risk. I ask for your continued cooperation in the adoption of these terms and definitions.

Rand Beers
Under Secretary
National Protection and Programs Directorate
Department of Homeland Security

This page is intentionally left blank.

EXECUTIVE SUMMARY

This is the second edition of the Department of Homeland Security (DHS) Risk Lexicon and represents an update of the version published in September 2008. More than seventy terms and definitions were included in the first edition of the DHS Risk Lexicon. The 2010 edition includes fifty new terms and definitions in addition to revised definitions for twenty-three of the original terms.

It was produced by the DHS Risk Steering Committee (RSC). The RSC, chaired by the Under Secretary for the National Protection and Programs Directorate and administered by the Office of Risk Management and Analysis (RMA), has produced a DHS Risk Lexicon with definitions for terms that are fundamental to the practice of homeland security risk management and analysis.

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 Departmental efforts toward integrated risk management. 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 glossaries used by other countries and professional associations. 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 COI. 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.

This page is intentionally left blank.

List of Terms

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

* New terms for 2010
Ω Definitions revised from 2008

* New terms for 2010
Ω Definitions revised from 2008

TABLE OF CONTENTS

This page is intentionally left blank.

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 Department of Homeland Security (DHS) Risk Steering Committee (RSC) initiated the DHS Risk Lexicon Project and in September 2008 published the first DHS Risk Lexicon. The DHS Risk Lexicon provides a set of terms for use by the homeland security risk community of interest (COI) and represents an important and ongoing effort to enable integrated risk management (IRM) across the Department.

The DHS Policy for Integrated Risk Management, signed by Secretary Napolitano in May 27, 2010, states that IRM is achieved, in part, by:

> ***Building a common understanding of risk management through development of a risk lexicon, risk-informed planning process, training, and standards of practice.***

Risk management and analysis supports specific homeland security missions and determines how homeland security functions can be best used to prevent, protect, mitigate, respond to, and recover from hazards to the Nation. The ability to communicate precise concepts and meanings is essential for effective risk-informed decision making. 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 DHS Risk Lexicon Project has identified and defined the terms that are essential to the practice of homeland security risk management. The DHS Risk Lexicon is intended to improve the internal management of DHS and facilitate commonplace discussions among the departmental risk community. The DHS Risk 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 publication represents the most recent collection of terms and definitions of the DHS Risk Lexicon. 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 homeland security risk COI.

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 definitions relevant to the practice of homeland security risk management and analysis. To support IRM 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.

- 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.

Project Governance

This DHS Risk Lexicon was created 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 initiatives. One of these groups is the Risk Lexicon Working Group (RLWG). The RLWG includes representatives from DHS Components and serves as the homeland security risk 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 RMA coordinates regular meetings of the RLWG and supports a variety of collection, documentation, and workshop activities to develop 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 are developed through a three-phase process:

- **Collection:** Terms are collected from across DHS and the risk community.
- **Harmonization:** Multiple, often conflicting, definitions are harmonized to produce a single meaning for each term.
- **Validation, Review, and Normalization:** Harmonized definitions are 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 are provided to the entire RLWG for comment. Comments are adjudicated and definitions are standardized for grammar and format.

I. Lexicon Process Phases

A. Collection

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

- Unclassified Presidential Policy and Homeland Security Presidential Directive
- National Security Strategy
- Quadrennial Homeland Security Review (QHSR)
- 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
- DHS Bottom-Up Review
- 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
- Federal Emergency Management Agency (FEMA) Comprehensive Preparedness Guide 101
- FEMA State and Local Mitigation Planning (386) Series

This is the second edition of the DHS Risk Lexicon and represents an update of the version published in September 2008. Seventy-three terms were recommended for inclusion in the first edition. The 2010 Edition includes fifty new terms and revised definitions for twenty-three of the original terms. Each of these terms represent a fundamental concept of risk and meets the majority of the following criteria:

- Relevant to all DHS Components with a role in risk management (*i.e.*, broadly used terms).
- Previously 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 dictionary definition.
- Necessary for applying IRM.

B. Harmonization Process

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

RLWG members utilize a protocol for harmonization that is consistent with DHS Lexicon Program procedures. This protocol allows for a thorough examination of relevant sources to ensure that the harmonized definitions produced by the RLWG are appropriate for DHS and the external homeland security risk community. During a series of Harmonization workshops, RLWG members discuss the available definitions and reach consensus on harmonized definitions for the core terms.

The RLWG members execute 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 homeland security policy, to determine key concepts and requirements for term 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 the key concepts.

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

C. Validation, Review and Normalization

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

1. Validation:

Each of the proposed definitions is validated against non-DHS professional sources (glossaries 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 include:

- 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, 2008.
- 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, 2009.

RMA staff, in support of the RLWG, cross-referenced each of the proposed core definitions with each validation source. Fifty of the 123 terms included in the DHS Risk Lexicon are found in at least one of the validation sources. In the majority of cases, definitions for the DHS Risk Lexicon are consistent with definitions being used in the larger international risk community. When the definitions differ, it can usually be attributed to differences in the communities that the definitions are 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 are due to the use of common words that have taken on a specific meaning in the domestic homeland security context (For example, 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.).

This validation effort demonstrates 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 COI.

2. Review:

Validated DHS Risk Lexicon definitions are circulated to all members of the RLWG for comment before being submitted to the RSC for review. RLWG members review definitions and examples and make revisions or comments as necessary.

3. Normalization:

As a final step in producing official definitions for the DHS Risk Lexicon, the 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. Definitions

Absolute Risk*:

Definition: level of risk expressed with standard units of measurement that allows for independent interpretation without comparison to estimates of other risks

Sample Usage: Analysts used the absolute risk estimate for a particular scenario to determine if a mitigation measure was cost effective.

Annotation:

1) The absolute risk value of a scenario has a meaningful independent interpretation in contrast to relative risk that is meaningful only in comparison to other similarly constructed risk values.

2) Can be measured using annualized lives lost, expected economic impact, or other metrics but it is not a ratio of risks.

3) Can measure absolute level of risk pre- or post-risk reduction measures.

See Also: relative risk

Absolute Risk (Unmitigated)*:

Definition: level of risk that exists without risk controls

Sample Usage: An absolute risk value for the facility, assuming no security measures, was determined at the outset of the analysis.

Extended Definition: a hypothetical condition that would exist if risk mitigation measures were absent

Annotation:

1) The application of absolute risk to natural hazards is straightforward. It is a reasonable approximation of what the risk would be if all countermeasures were actually removed. It is commonly used as a step in calculating the risk-reduction value of existing or prospective countermeasures.

2) The use of absolute risk for crime and terrorism involves limitations. In this context, absolute risk involves imagining that no countermeasures are in place. However, it does not involve imagining the response of adaptive intelligent adversaries in this absence of countermeasures. As a result, it is a poor approximation of what the actual risk would be if the countermeasures were removed.

3) It is critical to be transparent about these assumptions when comparing any crime- or terrorism-related absolute risk (or calculation derived therein) to any other absolute risk-derived calculation.

ACCEPTABLE RISK*:

Definition: level of risk at which, given costs and benefits associated with risk reduction measures, no action is deemed to be warranted at a given point in time

Sample Usage: Extremely low levels of water-borne contaminants can be deemed an acceptable risk.

ACCIDENTAL HAZARD:

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

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

ADAPTIVE RISK*:

Definition: category of risk that includes threats intentionally caused by humans

Sample Usage: A terrorist plot to attack a public transportation system can be categorized as an adaptive risk.

Annotation: Adaptive risks can include insider threats, civil disturbances, terrorism, or transnational crime. Those threats are caused by people that can change their behavior or characteristics in reaction to prevention, protection, response, or recovery measures taken.

ADVERSARY:

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

Sample Usage: Al-Qaeda is 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.

ALTERNATIVE FUTURES ANALYSIS*:

Definition: set of techniques used to explore different future states developed by varying a set of key trends, drivers, and/or conditions

Sample Usage: Strategic analysts used alternative futures analysis to investigate the effectiveness of a proposed policy in different possible futures.

Extended Definition: includes forecasts, scenario analysis, and visioning

Annotation:

1) This type of analysis can be used to test assumptions about future conditions, as well as identify "weak signals" of trends that could be significant in the future and "wildcard events" that – while unlikely – would have high impact should they occur.

2) Alternative futures analysis can also test the robustness of alternative strategies, policies, or capabilities by evaluating the effectiveness of each, and evaluating trade-offs or complementarities among them, in a variety of potential future states ranging from the highly challenging to the visionary.

3) Similar methods can be used to develop a statement of vision to motivate an organization to create the future it prefers in light of changes taking place in the environment.

ASSET:

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

Sample Usage: 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

Sample Usage: 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

Sample Usage: 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.

BASELINE RISK*:

Definition: current level of risk that takes into account existing risk mitigation measures

Sample Usage: Risk analysts for the locality calculated a baseline risk value before analyzing the risk reduction potential of two alternative strategies.

Annotation: Often, the word "risk" is used to imply "baseline risk" with the unstated understanding that the reference is the current circumstances. It should not be confused with risk as a measurement, which can change with the substitution of different variables.

BAYESIAN PROBABILITY*:

Definition: the process of evaluating the probability of a hypothesis through 1) the specification of a prior probability and 2) modification of the prior probability by incorporation of observed information to create an updated posterior probability

Sample Usage: The analyst applied Bayesian probability techniques to incorporate new evidence and update her estimate of the threat probability.

Annotation: This concept is also referred to as Bayesian probabilistic inference. Bayesian probability evaluates likelihoods as probabilities rather than frequencies.

See Also: subjective probability, probability, and frequentist probability

BAYESIAN PROBABILITY (SUBJECTIVE PROBABILITY)*:

Definition: see subjective probability (synonym)

Sample Usage: An analyst may use Bayesian probability to estimate likelihood based on a degree of belief.

BREAK-EVEN ANALYSIS*:

Definition: variant of cost-benefit analysis that estimates the threshold value at which a policy alternative's costs equal its benefits

Sample Usage: Break-even analysis showed that the proposed security policy would have to reduce the probability of attack by two orders of magnitude for its benefits to equal its costs; since this was judged unlikely, the proposed security policy was rejected.

Annotation: Analysts have applied this technique to homeland security by calculating the minimum threat probability required for the risk reduction benefits of a security policy to exceed the costs. If decision makers believe the actual threat is greater than the calculated break-even threat level, then the expected benefits of the policy exceed the costs. The technique also may be applied to other uncertain parameters in the analysis.

See Also: return on investment (risk)

CAPABILITY:

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

Sample Usage: 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 are 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 COIs may use capability to refer to any organization's ability to perform its mission, activities, and functions.

CONDITIONAL PROBABILITY*:

Definition: see probability (annotation, 7)

Sample Usage: An individual has a higher conditional probability of developing a fever if they contract influenza.

CONSEQUENCE:

Definition: effect of an event, incident, or occurrence

Sample Usage: 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 (health), economic consequence, mission consequence, psychological consequence, indirect consequence, and direct consequence

CONSEQUENCE ASSESSMENT Ω:

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

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

See: Appendix A for 2008 definition

COST-EFFECTIVENESS ANALYSIS (CEA)*:

Definition: analytic technique that compares the cost of two or more alternatives with the same outcome. Alternatively: analytic technique that evaluates an alternative by how much it delivers per unit cost, or how much has to be spent per unit benefit

Sample Usage: Cost-effectiveness analysis supported selection of a new screening technology for detecting contraband items because its cost per item detected is less than that of the current screening method.

COST-BENEFIT ANALYSIS (CBA)*:

Definition: analytic technique used to compare alternatives according to the relative costs incurred and the relative benefits gained

Sample Usage: Cost-benefit analysis allowed risk practitioners to make recommendations between two different screening systems.

Extended Definition: typically measured in monetary terms

Annotation: The analysis can incorporate discounting calculations to take into account the time value of money.

COUNTERMEASURE Ω:

Definition: action, measure, or device intended to reduce an identified risk

Sample Usage: Some facilities employ surveillance cameras as a countermeasure.

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

See: Appendix A for 2008 definition

CRITICALITY*:

Definition: importance to a mission or function, or continuity of operations

Sample Usage: The criticality of the asset was determined based upon the number of people to whom it provided service.

CRITICALITY ASSESSMENT*:

Definition: product or process of systematically identifying, evaluating, and prioritizing based on the importance of an impact to mission(s), function(s), or continuity of operations

Sample Usage: A criticality assessment determined that the county's chemical plants required greater attention than previously determined.

DECISION ANALYSIS*:

Definition: techniques, body of knowledge, and professional practice used to provide analytical support for making decisions through a formalized structure

Sample Usage: Decision analysis can be used to more effectively allocate resources to various risk reduction measures.

Annotation: Decision analysis can be used in the context of risk analysis to evaluate complex risk management decisions. Decision analysis can be applied to strategic, operational, and tactical decisions.

DETERRENT Ω:

Definition: measure that discourages, complicates, or delays an adversary's action or occurrence by instilling fear, doubt, or anxiety

Sample Usage: Robust countermeasures can serve as a deterrent to some adversaries, causing them to change, delay, or abandon their plans.

Annotation:

1) A deterrent reduces threat by decreasing the likelihood that an attack (or illegal entry, etc.) will be attempted.

2) One form of deterrent is a prospective punitive action intended to discourage the adversary from acting (*e.g.*, massive nuclear retaliation, Mutual Assured Destruction during the Cold War, or prison for conventional crimes). Another form of deterrent is a measure or set of measures that affects the adversary's confidence of success (*e.g.*, fences, border patrols, checkpoints).

3) A deterrent may cause an adversary to abandon plans to attempt an attack (or illegal entry, etc).

4) A deterrent may cause the adversary to react by "threat shifting" in any of several domains: shift in time (delay); shift in target; shift in resources (additional resources); and/or a shift in plan or method of attack.

5) Resilience, in terms of both critical economic systems and infrastructure and in societal resilience (*e.g.*, the famed British "stiff upper lip" of WWII, advance preparation for effective consequence reduction response operations, etc.), also has a potential deterrent value achieved when terrorist groups perceive that the strategic impact they seek through a particular attack or type of attack will not be achieved.

See Also: threat shifting

DIRECT CONSEQUENCE*:

Definition: effect that is an immediate result of an event, incident, or occurrence

Sample Usage: Property damage and loss of life were among the direct consequences resulting from the hurricane.

Annotation:

1) Direct consequences can include injuries, loss of life, on-site business interruption, immediate remediation costs, and damage to property and infrastructure as well as to the environment.

2) The distinction between direct and indirect consequences is not always clear, but what matters in risk analysis is a) capturing the likely effects – be they designated as direct or indirect – that should be part of the analysis, b) clearly defining what is contained as part of direct consequences and what is part of indirect consequences, and c) being consistent across the entire analysis. Such consistency and clarity is important for comparability across scenarios and risk analyses.

See: primary consequence

See Also: indirect consequence

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

Sample Usage: The loss of the company's 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.

ENTERPRISE RISK MANAGEMENT*:

Definition: comprehensive approach to risk management that engages organizational systems and processes together to improve the quality of decision making for managing risks that may hinder an organization's ability to achieve its objectives

Sample Usage: An organization uses enterprise risk management processes to holistically consider the risks associated with personnel turnover.

Annotation: Enterprise risks may arise from internal and external sources. Examples of internal sources include issues such as financial stewardship, personnel reliability, and systems reliability.

Where internal risks threaten successful mission execution, enterprise risk management seeks to ensure that internal systems and processes are tailored to minimize the potential for mission failure. Examples of external factors include, but are not limited to, global, political, and societal trends. An organization will modify its enterprise risk management approach to take these risks into account.

EVALUATION:

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

Sample Usage: 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.

EVENT TREE*:

Definition: graphical tool used to illustrate the range and probabilities of possible outcomes that arise from an initiating event

Sample Usage: Analysts used an event tree to diagram possible outcomes from a terrorist attack.

Annotation:

1) Event trees use forward logic; they begin with an initiating event and work forward in time to determine the possible outcomes.

2) The probabilities used in event trees are *conditional probabilities* because they are based on the assumption that the initiating event has already occurred. (See Probability annotation for a description of conditional probability.)

3) As an example, consider Figure A. The initiating event is an *Attack Attempted*. From the initiating event, the tree branches into a sequence of random variables, called events. The branching point at which a new random event is introduced is called a node and is depicted by a circle.

The first of these random events is *Personnel Action to Stop Attack*. The *Personnel Action to Stop Attack* is successful with probability $1\text{-}P_1$ and fails to stop the attack with probability P_1. If *Personnel Action to Stop Attack* is successful, then the branch leads to the final outcome of Unsuccessful Attack, No Damage (Scenario A). If *Personnel Action to Stop Attack* is not successful, then the branch leads to the next node representing the random event of whether the *Security Equipment to Stop Attack* is successful or not with probabilities of $1\text{-}P_2$ and P_2 respectively. If the *Security Equipment to Stop Attack* is successful then the branch leads to the final outcome of Unsuccessful Attack, No Damage (Scenario B). If *Security Equipment to Stop Attack* fails then the branch leads to the final outcome of Successful Attack, Damage to System (Scenario C).

Assuming that P_1 equals 10% or 0.1 and P_2 equals 30% or 0.3, then the conditional probabilities of a Successful and Unsuccessful Attack, given that the initiating event occurs and an attack is attempted, are calculated as follows:

Probability of Successful Attack given that an attack is attempted:

= Probability of Scenario C

= Probability that *Personnel Action to Stop Attack* fails and *Security Equipment to Stop Attack* fails.

$= P_1 \times P_2$

$= 0.1 \times 0.3$

$= 0.03$

Therefore, the conditional probability of a Successful Attack, given the attack is attempted, is 3%.

Probability of Unsuccessful Attack given that an attack is attempted:

= Probability of Scenario A or Scenario B occurring

= Probability that *Personnel Action to Stop Attack* is successful or *Security Equipment to Stop Attack* is successful.

$= (1 - P_1) + [P_1 \times (1 - P_2)]$

$= 0.9 + (0.1 \times 0.7)$

$= 0.97$

Therefore, the conditional probability of an Unsuccessful Attack, given that the attack is attempted, is 97%.

Notice that the Probability of Successful Attack plus the probability of Unsuccessful Attack equals one because there are no alternative outcomes.

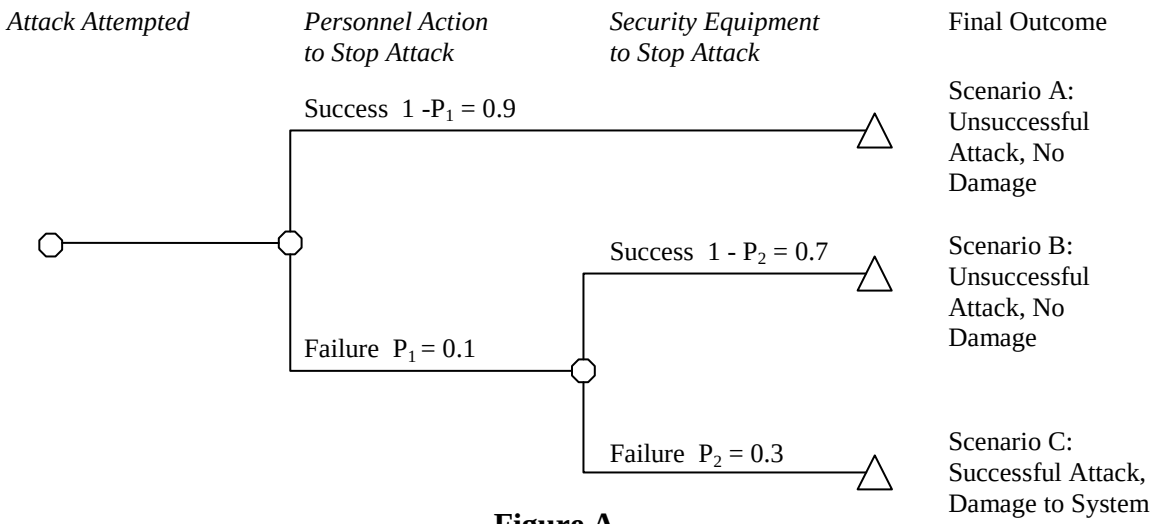

Figure A

Event trees differ from fault trees by starting with an initiating event and moving forward in time to determine possible final outcomes. Fault trees start with an outcome and work backwards in time to determine the range of events that may have caused the outcome.

See Also: fault tree, probability

FAULT TREE*:

Definition: graphical tool used to illustrate the range, probability, and interaction of causal occurrences that lead to a final outcome

Sample Usage: A fault tree for machinery was used to diagram the possible points of failure.

Annotation:

1) Fault trees use inductive (backwards) logic; they begin with a final occurrence and work backwards in time to determine the possible causes.

2) A fault tree can be used to quantitatively estimate the probability of a program or system failure by visually displaying and evaluating failure paths.

3) Fault trees can identify system components that lack redundancy or are overly redundant.

4) As an example, consider Figure B. The final outcome, labelled here as *Damage to System* is shown at the top of the fault tree. All of the events that could lead to *Damage to System* are diagrammed in the tree beneath the final outcome. Each event either does or does not occur, and the events are interconnected by logical functions OR and AND.

Notice that one event that could result in *Damage to System* is if a *Successful Attack* occurs. *Successful Attack* is one of the final states depicted in the Event Tree example. The occurrence of a *Successful Attack* depends on 1) an attack being attempted, 2) the failure of *Personnel Action to Stop Attack*, AND 3) the failure of *Security Equipment to Stop Attack*. If the probability of an attack being attempted is P_0, then the probability of a *Successful Attack* is the probability that all three of these conditions are met, equal to $P_0 \times P_1 \times P_2$.

However, *Damage to System* can also occur if *Natural Disaster* occurs, which happens with probability of P_3. Assuming that P_0 equals 5% or .05, P_1 equals 10% or 0.1, P_2 equals 30% or 0.3, and P_3 equals 20% or 0.2, then the overall probability of *Damage to System* is calculated as follows:

Probability of Damage to System = Probability that *Natural Disaster* occurs OR *Successful Attack* occurs.

= 1 - [Probability that *Natural Disaster* does not occur AND *Successful Attack* does not occur]

$= 1 - [(1 - P_3) \times (1 - P_0 \times P_1 \times P_2)]$

$= 1 - [0.8 \times (1 - 0.0015)]$

$= 0.2012$

Therefore, the probability of *Damage to the System* from all possible hazards is approximately 20%.

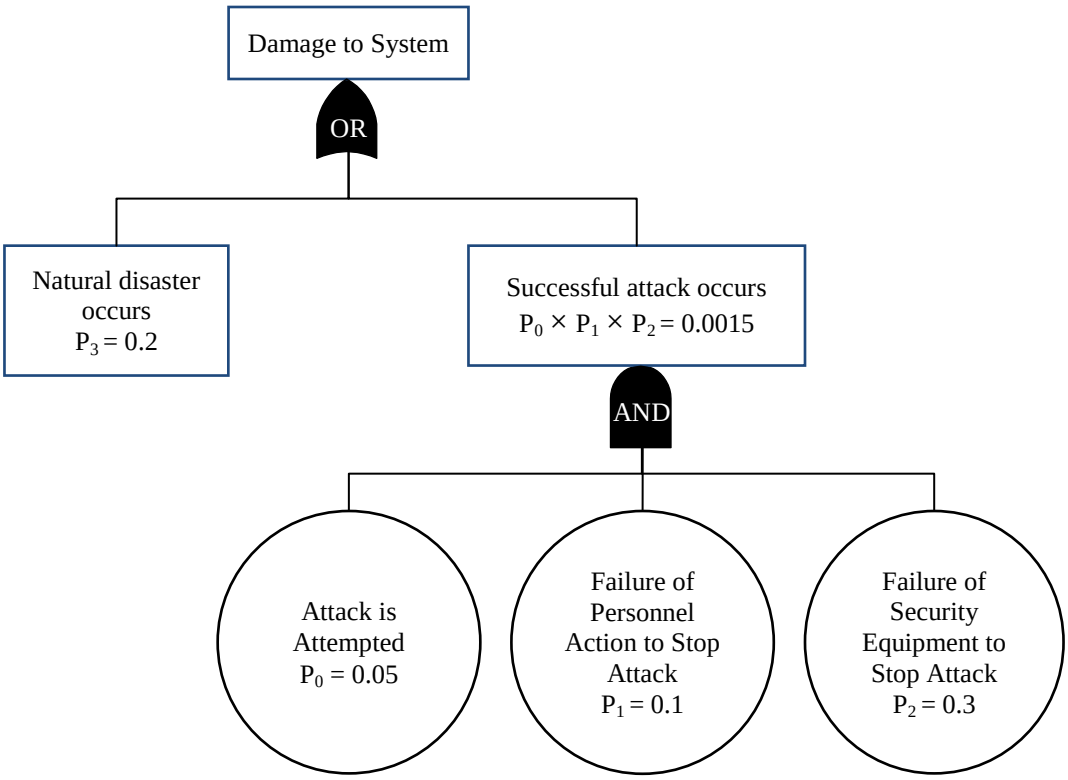

Figure B

See Also: event tree, probability

FREQUENCY*:

Definition: number of occurrences of an event per defined period of time or number of trials

Sample Usage:

1) The frequency of severe hurricanes in the Atlantic Ocean has been observed to be on average four per year.

2) The frequency of the number three when Bob rolled a six-sided die was one time in six rolls.

FREQUENTIST PROBABILITY*:

Definition: interpretation or estimate of probability as the long-run frequency of the occurrence of an event as estimated by historical observation or experimental trials

Sample Usage:

1) Based on empirical evidence from repeated experimental trials, the frequentist probability of getting a three when rolling a fair six-sided die is 1/6 or 16.7%.

2) Based on historical evidence, scientists can provide a frequentist probability of experiencing a category 5 hurricane in a given year.

Annotation:

1) Within the frequentist probability interpretation, precise estimation of new or rarely occuring events, such as the probability of a catastrophic terrorist attack, is generally not possible.

2) Frequentist probabilities generally do not incorporate "degree of belief" information, such as certain types of intelligence information.

See Also: probability, Bayesian probability, and subjective probability

FUNCTION Ω:

Definition: service, process, capability, or operation performed by an entity, asset, system, network, or geographic area

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

GAME THEORY*:

Definition: branch of applied mathematics that models interactions among agents where an agent's choice and subsequent success depend on the choices of other agents that are simultaneously acting to maximize their own results or miminize their losses

Sample Usage: Analysts used game theory to model terrorist behavior in response to potential security measures.

Annotation:

1) Game theory can be used in the context of risk analysis to model strategic decisions and interactions of agents with conflicting interests to predict likely decision outcomes.

2) A basic application of game theory involves two players and two strategy alternatives.

HAZARD:

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

Sample Usage: Improperly maintained or protected 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.

HORIZON SCANNING*:

Definition: process of identifying future trends, drivers, and/or conditions that may have an effect on future events, incidents, or occurrences

Sample Usage: In alternative futures analysis of potential attacks on transportation systems, horizon scanning indicated that future availability of technology for adversaries could provide more options for carrying out an attack.

HUMAN CONSEQUENCE (HEALTH) Ω:

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

Sample Usage: 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

Sample Usage: 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

Sample Usage: DHS 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.

INDIRECT CONSEQUENCE*:

Definition: effect that is not a direct consequence of an event, incident, or occurrence, but is caused by a direct consequence, subsequent cascading effects, and/or related decisions

Sample Usage: In the following months, decreased commerce and tourism were among the indirect consequences resulting from the hurricane.

Annotation:

1) Examples of indirect consequences can include the enactment of new laws, policies, and risk mitigation strategies or investments, contagion health effects, supply-chain economic consequences, reductions in property values, stock market effects, and long-term cleanup efforts,

2) Accounting for indirect consequences in risk assessments is important because they may have greater and longer-lasting effects than the direct consequences.

3) Indirect consequences are also sometimes referred to as ripple, multiplier, general equilibrium, macroeconomic, secondary, and tertiary effects.

4) The distinction between direct and indirect consequences is not always clear but what matters in risk analysis is a) capturing the likely effects – be they designated as direct or indirect – that should be part of the analysis, b) clearly defining what is contained as part of direct consequences and what is part of indirect consequences, and c) being consistent across the entire analysis. Such consistency and clarity is important for comparability across scenarios and risk analyses.

5) Induced consequences are occasionally estimated separately from indirect consequences but should be contained within indirect estimates.

See: secondary consequence

See Also: direct consequence

INTEGRATED RISK MANAGEMENT Ω:

Definition: structured approach that enables the distribution and employment of shared risk information and analysis and the synchronization of independent yet complementary risk management strategies to unify efforts across the enterprise

Sample Usage: DHS uses an integrated risk management framework to promote a unified approach to managing all homeland security risks.

INTENT Ω:

Definition: a state of mind or desire to achieve an objective

Sample Usage: 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

Sample Usage: Cyber attacks are an intentional hazard that DHS works to prevent.

JOINT PROBABILITY*:

Definition: see probability (annotation, 8)

Sample Usage: The probability of developing a fever from influenza is equal to the joint probability of someone contracting influenza and developing a fever.

LIKELIHOOD Ω:

Definition: chance of something happening, whether defined, measured or estimated objectively or subjectively, or in terms of general descriptors (such as rare, unlikely, likely, almost certain), frequencies, or probabilities

Sample Usage: 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, multiplicative 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

LIKELIHOOD (STATISTICAL)*:

Definition: conditional probability of observing a particular event given the hypothesis under consideration is true

Sample Usage: Analysts evaluated the likelihood of a breach in the border fence given their observations of population increases in area cities.

Annotation:

1) Likelihood is used colloquially as a synonym for probability.

2) In statistical usage there is a clear distinction between probability and likelihood: whereas probability allows us to predict unknown outcomes based on known parameters, likelihood allows us to estimate unknown parameters based on known outcomes.

3) The probability of a successful attack occurring can be broken into two related quantities: the probability that an attack occurs (which is a common mathematical representation of threat), and the probability that the attack succeeds, given that it is attempted (which is a common mathematical representation of vulnerability). In the context of natural hazards, probability of occurrence is typically informed by the frequency of past incidents or occurrences. These probabilities are often colloquially referred to as likelihoods.

See: Appendix A for 2008 definition

See Also: likelihood

MARGINAL PROBABILITY*:

Definition: see probability (annotation, 10)

Sample Usage: Analysts estimated the marginal probability of a water system contamination, irrespective of the source or type of contaminate.

MITIGATION* (FROM DHS LEXICON):

Definition: ongoing and sustained action to reduce the probability of, or lessen the impact of, an adverse incident

Extended Definition: actions may be implemented prior to, during, or after an incident occurrence

Sample Usage: Through the use of mitigation measures, the impact of the tsunami on the local population was greatly reduced.

Annotation: Mitigation measures may include zoning and building codes, floodplain buyouts, and analysis of hazard-related data to determine where it is safe to build or locate temporary facilities. Mitigation can include efforts to educate governments, businesses, and the public on measures they can take to reduce loss and injury. Technical measures can include the development of technologies that result in mitigation and can be used to support mitigation strategy.

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

Sample Usage: The inability to ensure the public's access to clean drinking water could be 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 Ω:

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

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

See Also: simulation

NATURAL HAZARD:

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

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

NET ASSESSMENT*:

Definition: multidisciplinary strategic assessment process used to provide a comparative evaluation of the balance of strengths and weaknesses

Sample Usage: A key aspect of net assessment involves analyzing technological influences on the security environment.

Annotation: Net assessment often involves the combined use of business principles, scenarios, crisis gaming and path gaming, conflict situations, and other tools.

NETWORK Ω:

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

Sample Usage: 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.

NORMALIZED RISK*:

Definition: measure of risk created by mathematically adjusting a value in order to permit comparisons

Sample Usage: The risk assessment report displayed the normalized risk of the three biological agents to facilitate comparison and avoid sharing sensitive information.

Annotation:

1) Typically, normalized risk divides the risk of each scenario by the sum of the risk across the set of scenarios under consideration. For example, if you are considering the expected number of fatalities from three different biological agents A, B and C, then the total risk posed by these biological agents is the sum of the risk posed by each of them. If agent A has expected fatalities of 10,000, Agent B has 7,000, and Agent C has 3,000, then the total risk is 20,000 fatalities and the normalized risks are 0.5 for Agent A, 0.35 for Agent B, and 0.15 for Agent C. This particular way of normalizing risk is commonly referred to as "normalizing to 1" because now the risk from all the scenarios in the considered set sums to 1.

2) Risk can be normalized by dividing by an existing sample space value. For example, if there were 100 car accidents this year and 800 last year, then normalizing these values with respect to the total vehicle trips each year permits a more appropriate comparison of the risk of last year versus this year. If there were 10,000 vehicle trips this year then 100/10,000, or 1% of all trips ended in accidents, whereas if last year there were 100,000 vehicle trips then 800/100,000, or 0.8% of all trips ended in accidents. Without normalization it would appear that it was more risky to drive last year, but in reality the opposite is the case.

NON-ADAPTIVE RISK*:

Definition: category of risk that includes threats caused by natural and technological hazards

Sample Usage: The suspected path of a tornado can be categorized as a non-adaptive risk.

Annotation: Threats from non-adaptive risks are caused by physical characteristics and dimensions that do not change in reaction to measures taken.

OPERATIONAL RISK*:

Definition: risk that has the potential to impede the successful execution of operations

Sample Usage: Given that none of the security guards had the flu vaccine, influenza posed an operational risk to provision of security for the facility.

See Also: strategic risk

PRIMARY CONSEQUENCE*:

Definition: see direct consequence (synonym)

Sample Usage: Property damage and injuries were among the primary consequences resulting from the flood.

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

Sample Usage: The engineers conducted a probabilistic risk assessment to determine the risk of an accident resulting from a series of compounding failures.

Annotation:

1) 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.

2) For some types of risk, like those involving human volition, the probability of occurrence of an event may not be independent of the consequences and, in fact, may be a function of the consequences.

PROBABILITY Ω:

Definition: numerical value between zero and one assigned to a random event (which is a subset of the sample space) in such a way that the assigned number obeys three axioms: (1) the probability of the random event "A" must be equal to, or lie between, zero and one; (2) the probability that the outcome is within the sample space must equal one; and (3) the probability that the random event "A" or "B" occurs must equal the probability of the random event "A" plus the probability of the random event "B" for any two mutually exclusive events

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

Annotation:

1) Probability can be roughly interpreted as the percent chance that something will occur. For example, a weather forecaster's estimate of a 30 percent chance of rain in the Washington, DC area is equivalent to a probability of 0.3 that rain will occur somewhere in Washington, DC.

2) A probability of 0 indicates the occurrence is impossible; 1 indicates that the occurrence will definitely happen.

3) Probability is used colloquially as a synonym for likelihood, but in statistical usage there is a clear distinction.

There are many concepts in probability that are used regularly in the field of risk analysis. This extension provides an elaboration on some of these concepts.

4) The probability that event A occurs is written as P(A).

5) Event A and event B are *mutually exclusive* if they cannot occur at the same time. For example, a coin toss can result in either heads or tails, but both outcomes cannot happen simultaneously.

6) Event A and event B are *statistically independent* if the occurrence of one event has no impact on the probability of the other. Examples of two events that are independent are the systems designed to prevent an attack as described the Fault Tree example and Event Tree example. The probability that the Personnel Action to Stop Attack is successful is not affected by whether the Security Equipment to Stop Attack is successful and vice versa. Two events that may not be independent are the collapse of a bridge and the occurrence of a major earthquake in the area. Clearly the probability of a bridge collapse can be affected by the occurrence of a major earthquake. However, the two events may also be independent: a bridge can survive an earthquake and a bridge can collapse in the absence of any earthquake.

7) *Conditional probability* is the probability of some event A, given the occurrence of some other event B, written as $P(A|B)$. An example is the conditional probability of a person dying (event A), given that they contract the pandemic flu (event B).

8) *Joint probability* is the probability of two events occurring in conjunction - that is, the probability that event A and event B both occur, written as) or P(AB) and pronounced A intersect B. The probability of someone dying from the pandemic flu is equal to the joint probability of someone contracting the flu (event A) and the flu killing them (event B). Joint probabilities are regularly used in Probabilistic Risk Assessments and Event Trees.

9) Conditional and joint probabilities are related by the following formula:

$$P(A|B) = P(AB)/P(B) \qquad (1)$$

If events A and B are statistically independent then

$$P(A|B) = P(A)$$

and the relationship (1) above becomes

$$P(A) \times P(B) = P(AB)$$

Consequently, for statistically independent events, the joint probability of event A and event B is equal to the product of their individual probabilities. An example of the joint probability of two independent events is given in the Event Tree example. If the probability that Personnel Action to Stop Attack fails equals P(A) and the probability that Security Equipment to Stop Attack fails equals P(B) then

Probability of Successful Attack $= P(AB)$

$= P(A) \times P(B)$

$= 0.1 \times 0.3$

= 0.03

as calculated in the Event Tree example (see Figure A on page 14).

10) *Marginal probability* is the unconditional probability of event A, P(A). It is the probability of A regardless of whether event B did or did not occur. If B can be thought of as the event of a random variable X having a given outcome, then the marginal probability of A can be obtained by summing (or integrating, more generally) the joint probabilities over all outcomes for X.

Suppose,

for example, that event A is the occurrence of an illegal person entering the country and X is the random variable of where he entered the country. Then there are two possible outcomes of X: either he entered through an official point of entry (event B), or he did not (event B' pronounced B-not). Then the probability of the person entering the country, P(A), is equal to the sum of the joint probabilities of him entering by traveling through a point of entry plus the probability of him entering by not traveling through a point of entry. P(A) = P(AB) + P(AB'). This is called marginalization.

See Also: frequentist probability, subjective probability, Bayesian probability, and likelihood

See: Appendix A for 2008 definition

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

Sample Usage: A psychological consequence of the disease outbreak could include the reluctance of the public to visit hospitals, 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

Sample Usage: 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

Sample Usage: Engineers at the plant used a quantitative risk assessment methodology to assess the risk of system 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

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

RELATIVE RISK*:

Definition: measure of risk that represents the ratio of risks when compared to each other or a control

Sample Usage: Although the site is prone to frequent low level flooding, the relative risk posed by a hurricane is greater than that posed by a flood.

Annotation:

1) The relative risk value of a scenario is meaningful only in comparison to other similarly constructed risk values.

2) Due to inherent uncertainties in risk analysis, relative risk may be more useful to decision makers than risk measured in expected annualized dollars lost or lives lost.

3) Using relative risk might convey the necessary meaning to decision makers while avoiding the disclosure of sensitive or classified information.

See Also: absolute risk

RESIDUAL RISK:

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

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

Synonym: unmitigated risk (residual risk)

RESILIENCE Ω:

Definition: ability to adapt to changing conditions and prepare for, withstand, and rapidly recover from disruption

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

Extended Definition: ability of systems, infrastructures, government, business, communities, and individuals to resist, tolerate, absorb, recover from, prepare for, or adapt to an adverse occurrence that causes harm, destruction, or loss

Annotation:

1) According to the QHSR, "Resilient individuals, families, and communities—and the systems that sustain them—are informed, trained, and materially and psychologically prepared to withstand disruption, absorb or tolerate disturbance, know their role in a crisis, adapt to changing conditions, and grow stronger over time."

2) Resilience can reduce the consequences associated with an incident, event, or occurrence; resilience can also impact the likelihood of a significant incident, event, or occurrence happening at all.

See Also: deterrent

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

Sample Usage: 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.

See Also: break-even analysis

RISK Ω:

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

Sample Usage: 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.

3) For terrorist attacks or criminal activities, the likelihood of an incident, event, or occurrence can be estimated by considering threats and vulnerabilities.

RISK ACCEPTANCE:

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

Sample Usage: 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 commonly used risk management strategies, along with risk avoidance, risk control, and risk transfer.

RISK ANALYSIS:

Definition: systematic examination of the components and characteristics of risk

Sample Usage: 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

Sample Usage: 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

Sample Usage: 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

Sample Usage: 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, 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

Sample Usage: He exercised a strategy of risk avoidance by choosing not to live in an area prone to tornadoes.

Annotation: Risk 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

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

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.

RISK CONTROL:

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

Sample Usage: As a risk control measure, security guards screen items to reduce the likelihood of dangerous articles getting inside of office buildings.

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

RISK DATA*:

Definition: information on key components of risk that are outputs of or inputs to risk assessments and risk analyses

Sample Usage: Risk data can be securely stored from earlier assessments and analyses to allow for comparisons or identification of trends.

RISK EXPOSURE*:

Definition: contact of an entity, asset, system, network, or geographic area with a potential hazard

Sample Usage: The scenario described the estimated costs that would be incurred in the event of risk exposure.

RISK GOVERNANCE*:

Definition: actors, rules, practices, processes, and mechanisms concerned with how risk is analyzed, managed, and communicated

Sample Usage: Risk governance applies the principles of good governance that include transparency, effectiveness, efficiency, accountability, strategic focus, and the need for the chosen solution to be politically and legally feasible.

RISK IDENTIFICATION:

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

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

RISK INDICATOR*:

Definition: measure that signals the potential for an unwanted outcome as determined by qualitative or quantitative analysis

Sample Usage: The facility operators were trained to recognize certain risk indicators during inspections.

RISK MANAGEMENT Ω:

Definition: process of identifying, analyzing, assessing, and communicating risk and accepting, avoiding, transferring or controlling it to an acceptable level considering associated costs and benefits of any actions taken

Sample Usage: The organization employed risk management to understand and reduce the risk it faced.

Annotation: Effective risk management improves the quality of decision making. Risk management principles acknowledge that, while risk often cannot be eliminated, actions can usually be taken to control risk.

RISK MANAGEMENT ALTERNATIVES DEVELOPMENT:

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

Sample Usage: After completing the risk management alternatives development step, the analysis team presented 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

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

RISK MANAGEMENT METHODOLOGY Ω:

Definition: set of methods, principles, or rules used to identify, analyze, assess, and communicate risk, and accept, avoid, transfer, or control it to an acceptable level considering associated costs and benefits of any actions taken

Sample Usage: 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

Sample Usage: 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

Sample Usage: Mutual aid agreements are a risk management strategy used by some emergency response authorities 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

Sample Usage: 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 Ω:

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

Sample Usage: Through risk mitigation, the potential impact of the natural disaster on the local population was greatly reduced.

Annotation: Risk mitigation 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

Sample Usage: Some medical professionals advise the risk mitigation option of vaccinations to reduce the risk of infection.

RISK PERCEPTION:

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

Sample Usage: Fear of terrorist attacks may create a skewed risk perception.

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

RISK PROFILE Ω:

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

Sample Usage: A risk profile for a plant may address risks such as structural failure, mechanical malfunction, and insider threat.

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 Ω:

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

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

Annotation:

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

2) Risk reduction can be accomplished by reducing vulnerability and/or consequences (damages).

RISK SCORE:

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

Sample Usage: By installing a surveillance system, the plant was able to change 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 Ω:

Definition: degree to which an entity, asset, system, network, or geographic area is willing to accept risk

Sample Usage: After a disaster, a community's risk tolerance may decrease.

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

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

Annotation:

1) 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).

2) Risk transfer is one of a set of four commonly used risk management strategies, along with risk control, risk acceptance, and risk avoidance.

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

Sample Usage: After reading about threats and vulnerabilities associated with vehicle explosives, she practiced risk-based decision making by authorizing the installation of additional security measures.

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, but incorrectly, 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

Sample Usage: He 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

Sample Usage: The team designed a scenario involving a terrorist attack at a plant to help assess the risk of certain types of terrorist attacks.

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.

SECONDARY CONSEQUENCE*:

Definition: see indirect consequence (synonym)

Sample Usage: The secondary consequence of a terrorist threat on a subway could be the decreased use of public transportation over time.

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

Sample Usage: 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

Sample Usage: 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 Ω:

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

Sample Usage: The scientists designed a simulation to see how weather affected the plume of smoke.

See Also: model

SOCIAL AMPLIFICATION OF RISK*:

Definition: distortion of the seriousness of a risk caused by public concern about the risk and/or about an activity contributing to the risk

Sample Usage: Social amplification of risk can result in public concern with an otherwise insignificant risk.

Annotation:

1) Describes the phenomenon by which hazards interact with psychological, social, institutional, and cultural processes in ways that may amplify or attenuate the public's perceived level of risk.

2) The social amplification of risk phenomenon is the subject of a field of study that seeks to systematically link the technical assessment of risk with sociological perspectives of risk perception and risk-related behavior.

STRATEGIC FORESIGHT*:

Definition: range of activities associated with longer range planning and alternative futures analysis

Sample Usage: The organization's strategic foresight initiative called for horizon scanning and analysis of the long-term implications of security policies.

Annotation: Strategic foresight can be applied to activities such as scenario development, critical thinking and brainstorming about long-term trends, Delphi sessions, workshops, trend analysis and gaming (or "war-gaming").

STRATEGIC RISK*:

Definition: risk that affects an entity's vital interests or execution of chosen strategy, whether imposed by external threats or arising from flawed or poorly implemented strategy

Sample Usage: An analysis of the organization's strategic risk considered threats to carrying out its essential mission functions.

Annotation:

1) Managing strategic risk is associated with the ability to recognize future trends, challenges, and threats and match these with appropriate operational concepts, capabilities, competencies, and capacity.

2) Strategic risk can arise from three basic sources. First, strategic risk can arise from the actions of adversaries, from natural hazards or from non-adversarial human actions, such as accidents. These can be thought of as imposed risks. Second, strategic risk can be created by the unintended consequences of the strategies we adopt in response to imposed risks. These can be thought of as self-imposed risks. Finally, strategic risk can arise from obstacles to successful implementation of an adopted strategy. These obstacles can be either imposed (*e.g.*, the actions of an adaptive adversary to counter a security measure or to exploit an unintended vulnerability created by a security measure) or self-imposed (*e.g.*, failure to adequately resource, or to prematurely abandon, a strategy or course of action that would otherwise be beneficial).

See Also: operational risk

SUBJECT MATTER EXPERT Ω:

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

Sample Usage: 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. Frequently abbreviated as SME.

SUBJECTIVE PROBABILITY*:

Definition: interpretation or estimate of probability as a personal judgment or "degree of belief" about how likely a particular event is to occur, based on the state of knowledge and available evidence

Sample Usage: Analysts use their knowledge of terrorist strategies, objectives, and capabilities in combination with evidence from operations to estimate a subjective probability of 10 percent for an attack to occur within the next five years.

Annotation:

1) Like all probabilities, subjective probability is conventionally expressed on a scale from zero to one where zero indicates the event is impossible and one indicates the event has or certainly will occur.

2) Within the subjective probability interpretation, it is possible to estimate probabilities of events (using experts or models) that have not previously occurred or that have only rarely occurred, such as acts of terrorism. However, because subjective probabilities incorporate historical or trial data when available, the subjective probability will approximate the frequentist probability as data becomes more plentiful.

3) Subjective probability is currently one of the most common uses of probability among statisticians and the risk analysis community.

4) Bayesian probability is colloquially used as a synonym for subjective probability. In statistical usage, Bayesian probabilistic inference is an approach to statistical inference that employs Bayes' theorem to revise prior information using evidence.

See Also: frequentist probability, probability, and Bayesian probability

SYSTEM:

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

Sample Usage: 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

Sample Usage: 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

Sample Usage: Analysts suggested that the greatest threat to the building was from specific terrorist attacks.

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 Ω:

Definition: product or 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

Sample Usage: Analysts produced a threat assessment detailing the capabilities of terrorist organizations to threaten particular infrastructure sectors.

See: Appendix A for 2008 definition

THREAT SHIFTING*:

Definition: response of adversaries to perceived countermeasures or obstructions, in which the adversaries change some characteristic of their intent to do harm in order to avoid or overcome the countermeasure or obstacle

Sample Usage: Installing barriers around only one of several neighboring government buildings may result in threat shifting, where the adversaries will target one of the remaining unprotected buildings.

Annotation:

1) Threat shifting can occur in one or more of several domains: the time domain (*e.g.*, a delay in attack or illegal entry to conduct additional surveillance, etc.), the target domain (selecting a different, less-protected target), the resource domain (adding resources to the attack in order to reduce uncertainty or overcome countermeasures), or the planning/attack method domain (changing the weapon or path, for example, of the intended attack or illegal entry).

2) Threat shifting is commonly cited as a reason for countermeasure failure or ineffectiveness – particularly in the case of target shifting. For example, when police occupy one street corner, the drug dealers simply go a few blocks away. This assumes that threat-shifting is frictionless for the adversary, which frequently is the case.

3) However, threat shifting is not always frictionless for the adversary – and therefore can be of some value to the defenders. The adversaries may delay their attack, consume additional resources, undertake complexity, expose themselves to additional counter-surveillance and counter-terrorism scrutiny, and/or shift to a less consequential target.

4) Threat shifting can, in some cases, increase risk by steering an adversary to an attack that is more likely to succeed or of greater consequence.

See Also: deterrent

UNACCEPTABLE RISK*:

Definition: level of risk at which, given costs and benefits associated with further risk reduction measures, action is deemed to be warranted at a given point in time

Sample Usage: The presence of contaminants in excess of a certain level represents an unacceptable risk to public health.

UNCERTAINTY:

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

Sample Usage: The uncertainty in the estimate was due to a lack of information for the particular environment and situation.

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.

UNMITIGATED RISK (RESIDUAL RISK)*:

Definition: see residual risk (synonym) (Definition for residual risk is "risk that remains after risk management measures have been implemented")

Sample Usage: A risk to the facility that was not considered in the risk assessment was a potential unmitigated risk.

VALUE OF STATISTICAL LIFE (VSL)*:

Definition: amount people are willing to pay to reduce risk so that on average one less person is expected to die from the risk

Sample Usage: The analyst estimates the monetary value of the mortality risk reduction from the initiative by using the VSL estimate.

Annotation:

1) The VSL is not intended to value very large reductions in mortality risk or place a value on the lives of identified individuals. VSL measures the monetized value of small reductions in mortality risk for a large number of people. For example, a countermeasure that reduces the annual risk of death by one in a million for 20 million people will, on average, save 20 lives a year. If the VSL is estimated at $5 million, the value of this mortality risk reduction is $100 million (20 expected lives saved times $5 million per life).

2) Most VSL estimates are based on studies of the wage compensation for occupational hazards or studies that elicit people's willingness to pay for mortality risk reduction directly.

VULNERABILITY Ω :

Definition: physical feature or operational attribute that renders an entity, asset, system, network, or geographic area open to exploitation or susceptible to a given hazard

Sample Usage: 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 entity, asset, system, network, or geographic area susceptible to disruption, destruction, or exploitation

VULNERABILITY (DEGREE)*:

Definition: qualitative or quantitative expression of the level to which an entity, asset, system, network, or geographic area is susceptible to harm when it experiences a hazard

Sample Usage: In developing the scenario, analysts sought to express the asset's vulnerability in the event of a particular type of attack.

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 Ω:

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

Sample Usage: 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.

See: Appendix A for 2008 definition

WILLINGNESS-TO-ACCEPT*:

Definition: amount a person is willing to accept to forgo a benefit

Sample Usage: Researchers designed a survey to estimate the willingness-to-accept dollar value travelers would require to compensate for time, convenience, and privacy potentially lost under a proposed security measure.

WILLINGNESS-TO-PAY*:

Definition: amount a person would be willing to pay, sacrifice, or exchange for a benefit

Sample Usage: A survey estimated the public's willingness-to-pay in dollars for new security measures.

III. DHS Lexicon Governance Structure

The DHS Lexicon Program of the DHS Executive Secretariat (ESEC) is responsible for the management of controlled vocabulary for DHS. The DHS Lexicon Program 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 an official Lexicon for the Department and topical glossaries. These include specific glossaries supporting Advanced Distributed Learning system lesson modules as well as broader glossaries 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 ESEC and the RSC work together to manage the DHS Risk Lexicon.

A. The DHS Executive Secretariat

The 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

The RSC leads the development, implementation, and sharing of IRM 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 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 Staff.

IV. MAINTENANCE OF THE DHS RISK LEXICON

The DHS Risk Lexicon is expected continue to grow and mature beyond this second publication of terms and definitions. Institutionalizing the use of a common risk language requires processes to ensure that the DHS Risk Lexicon remains relevant to the practice of homeland security risk management as the Department's approach to IRM matures. The DHS Risk Lexicon must be constantly maintained and updated to adequately support the risk COI 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 COI 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 Program. In its role representing the risk management COI, the RLWG oversees the introduction of additional terms as well as revisions to published terms.
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 publication and submitted via the RSC/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 RMAexecsec@hq.dhs.gov.
The DHS Lexicon Program welcomes all comments and proposed revisions to the DHS Risk Lexicon, and has delegated responsibility for adjudicating those comments to the RLWG, as the risk COI for the Department. As comments are received on existing terms, RMA, in support of the RSC, will compile and record all requests for revision and will coordinate 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 its 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 / RLWG representative.
If the RLWG accepts a proposed revision, RMA shall recommend the change to the ESEC's DHS Lexicon Program. The revision will then be entered into the official revision process that governs the DHS Lexicon. If the DHS Lexicon Program 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/RLWG representative or through the DHS Lexicon Program. Proposed additional terms submitted to ESEC will be forwarded to the RLWG. The RLWG coordinates the addition of terms into the DHS Risk Lexicon on the submitting individual's behalf, although the submitter is welcome to participate as appropriate in the process. Submitting individuals can send single terms or lists of terms to Lexicon@dhs.gov with a copy (Cc) to RMAexecsec@hq.dhs.gov, or through their Component's RSC representative.

The DHS Lexicon Program 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, Lexicon Process Phases, of this publication.

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 ESEC's DHS Lexicon Program 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 periodically survey the RSC and RLWG membership 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. C, Validation, Review, and Normalization, of this publication. 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 ESEC homepage on DHS Connect. DHS Connect can be accessed through http://dhsconnect.dhs.gov/org/comp/esec/Pages/default.aspx.

RMA works with the ESEC's DHS Lexicon Program 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 / 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. 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.

V. USE OF THE DHS RISK LEXICON

The DHS Risk Lexicon facilitates the clear exchange of structured and unstructured data essential to the interoperability of terms amongst the DHS risk COI. Since 2008, the DHS Risk Lexicon has been used by DHS risk practitioners, decision makers, stakeholders, and State, local, tribal and territorial government partners, as well as academia. The DHS Risk Lexicon has assisted in the development of institutional policy and technical guidelines, training and educational materials, and communication throughout the Homeland Security Enterprise.

In order to encourage the use of the DHS Risk Lexicon, RMA has worked with RSC and the RLWG to enhance awareness at the DHS Component level and will continue to promote its use within the Homeland Security Enterprise. The RSC continues to incorporate DHS Risk Lexicon definitions and terminology into materials it produces, including the IRM policy and doctrine, the Risk Management Guidelines, and other implementing documents that include Standard Operating Procedures (SOPs) and technical guidance.

DHS is currently identifying and developing training opportunities related to the practice of homeland security risk management and analysis. RMA has worked with the RSC to identify and enhance training opportunities within DHS Components and advocate the implementation of risk terms and definitions in training and educational materials, as appropriate.

As part of the RSC's mission to support IRM within DHS, the DHS Risk Lexicon acts as a benchmark document for homeland security risk management. The DHS Risk Lexicon breaks down linguistic and conceptual barriers across the enterprise so that partners can achieve common understanding and unity of effort. RSC members include DHS Risk Lexicon definitions in Departmental documents that support the Homeland Security Enterprise.

VI. Appendices

Appendix A: Revised Definitions from 2008 Publication

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, process, 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.

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.

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.

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.

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)

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

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.

PROBABILITY (MATHEMATICAL):

Definition: likelihood that is expressed as a number between zero and one, where zero indicates that the occurrence is impossible and one 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.

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.

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 MANAGEMENT:

Definition: process of identifying, analyzing, 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 mesures (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 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 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.

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.

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.

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 of 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.

Appendix B: 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**	**Justification for Proposed Change**	**Recommended Solution Language**

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.

ACAMS:

Long Form: Constellation/Automated Critical Asset Management System

Description: A Web-enabled information services portal that helps state and local law enforcement, public safety, and emergency response personnel to collect and use critical infrastructure and key resource (CIKR) data, assess vulnerabilities, and develop plans. It is available at no cost to state and local jurisdictions from the DHS Office of Infrastructure Protection (IP).

AMRA:

Long Form: Air Modal 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.

BTRA:

Long Form: Bioterrorism Risk Assessment

Description: A Science and Technology Directorate (S&T) program aimed at providing a comprehensive, quantitative assessment of bioterrorism risk to the homeland to inform investments; to aid in identifying threats, vulnerabilities and knowledge gaps; and to support strategic risk management planning.

BZP:

Long Form: Buffer Zone Plan

Description: A strategic document developed by local jurisdictions, with the support of DHS, to identify significant assets in the buffer zone - the area outside a facility that can be used by an adversary to conduct surveillance or launch an attack - of designated CIKR that may be targeted by terrorists for attack. This document also addresses specific threats and vulnerabilities associated with the sites and their significant assets.

BZPP:

Long Form: Buffer Zone Protection Program

Description: A DHS-administered grant program focused on providing funding to local law enforcement for equipment acquisition and planning activities to address gaps identified in Buffer Zone Plans and enhance security capabilities for the highest risk critical infrastructure sites.

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.

CBAT:

Long Form: Computer Based Assessment Tool

Description: A tactical tool that creates an interactive visual guide of a location by integrating data to generate a 360-degree geospherical video and geospatial panoramic imagery of facilities, surrounding areas, routes, and other areas of interest. The visual guide incorporates a wide variety of data including vulnerability assessments, evacuation plans, standard operating procedures, and schematic/floor plans.

CFIUS:

Long Form: Committee on Foreign Investment in the United States

Description: An inter-agency committee of the U.S. 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 U.S. 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: A quantitative scenario risk assessment methodology designed by IP to enable defensible cross-sector comparisons and comparisons of risk to combinations of infrastructure within a jurisdiction, sector, or attack type in support of return-on-investment evaluations of alternatives and to test methodology enhancements.

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 IP 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.

CTRA:

Long Form: Chemical Terrorism Risk Assessment

Description: An S&T program aimed at providing a comprehensive, quantitative assessment of chemical terrorism risk to the homeland to inform investments; to aid in identifying threats, vulnerabilities and knowledge gaps; and to support strategic risk management planning.

DSAT:

Long Form: Dams Sector Analysis Tool

Description: An integrated data management system and dams-specific analysis tool that incorporates a wide range of data input from multiple sources. It provides a focal point for all Dams Sector related information and analysis tools.

ECIP ASSESSMENT:

Long Form: Enhanced Critical Infrastructure Protection Assessment

Description: A security survey conducted in collaboration with Federal, State, local, and private sector stakeholders to assess the overall security posture for CIKR.

ESSAT:

Long Form: Emergency Services Self Assessment Tool

Description: A secure web-based tool that allows owners and operators of fixed emergency services assets to assess physical vulnerabilities.

FAIT:

Long Form: Fast Analysis Infrastructure Tool

Description: A tool created by the National Infrastructure Simulation and Analysis Center (NISAC) under DHS direction that produces regional economic analyses, asset descriptions, and other important information on assets for NISAC's internal analysts.

HAZUS:

Long Form: Hazards United States

Description: A nationally applicable standardized methodology and software program developed by FEMA that estimates potential losses from earthquakes, hurricane winds, and floods.

HIRA:

Long Form: Hazard Identification and Risk Assessment

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

IEISS:

Long Form: Interdependent Energy Infrastructure Simulation System

Description: A tool created by Los Alamos National Laboratories to study the interdependency relationships within and among energy subsectors, as well as 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.

IST:

Long Form: Infrastructure Survey Tool

Description: A multi-use web-based platform used in conjunction with ECIP security surveys to provide sector and cross-sector comparisons, dependency and interdependency identification, and cascading impacts and effects.

ITRA:

Long Form: Integrated Chemical, Biological, Radiological, Nuclear Terrorism Risk Assessment

Description: An S&T program aimed at providing an integrated quantitative assessment of the relative risks associated with chemical, biological, radiological and nuclear (CRBN) terrorism to the homeland. Applications of the ITRA include informing strategic resource allocation investments and risk management planning and identifying the relative threats, vulnerabilities and knowledge gaps associated with CBRN terrorism.

MD SHARPP:

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

Description: A mnemonic composed of the above terms 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 Analysis Model

Description: A United States Coast Guard (USCG) 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 IP organization, including elements of Los Alamos and Sandia National Laboratories, 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 USCG all-mission risk assessment that informs budget and planning guidance.

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 USCG risk assessment process 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 RMA 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 TSA agent based computer simulation model for analyzing and informing decisions about risk reduction options based on threat, vulnerability, and consequence data.

RRAP:

Long Form: Regional Resiliency Assessment Program

Description: A cooperative, IP-led interagency assessment of specific CIKR and regional analysis of the surrounding infrastructure. The RRAP evaluates CIKR on a regional level to examine vulnerabilities, threats, and potential consequences from an all-hazards perspective to identify dependencies, interdependencies, cascading effects, resiliency characteristics, and gaps.

RSAT:

Long Form: Risk Self Assessment Tool

Description: A secure, Web-based application designed to assist managers of stadiums and arenas with the identification and management of security vulnerabilities to reduce risk to their facilities. The RSAT application uses facility input in combination with threat and consequence estimates to conduct a comprehensive risk assessment and provides users with options for consideration to improve the security posture of their facility.

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, to identify security gaps and provide options for consideration to enhance protective measures.

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 and Evaluation for Leadership Decisions

Description: Collaboration between FEMA's Office of National Capital Region Coordination and RMA to create a regional risk analysis model, encompassing both a risk assessment and strategic approach to risk management.

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 CIKR 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 FEMA) 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: Threat Risk Assessment and Management

Description: A FEMA service which compares relative risk of threats against assets within a given jurisdiction and identifies and prioritizes enhancements in security, protection, response, and recovery that can be implemented to reduce those risks.

TRAVEL:

Long Form: Transportation Risk Assessment and Vulnerability Evaluation Tool

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

TSSRA:

Long Form: Transportation Sector Security Risk Assessment

Description: A TSA strategic-level risk assessment of terrorism-based risks facing the U.S. transportation sector. Comprised of attack scenarios and attack families, and based on the inputs of government and private sector transportation stakeholders, the TSSRA evaluates and compares threats, vulnerabilities, and consequences of selected terrorist attack scenarios across all modes of transportation (except maritime). It is intended to identify needs for more detailed analysis, inform planning and resource decisions, and establish a baseline for other periodic analyses and analytical activities related to transportation security.

VCAT:

Long Form: Voluntary Chemical Assessment Tool

Description: A tool developed to provide the means for owner /operators of non-tiered facilities to identify their current risk level. The web-based tool facilitates a cost-benefit analysis allowing users to select the best combination of physical security countermeasures and mitigation strategies to reduce overall risk.

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.

Appendix D: DHS Lexicon Contact Information

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

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

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

RMAexecsec@hq.dhs.gov

This page is intentionally left blank.