Riskion Taxonomy (Riskion Elements and Risk Measures)

Industry/Standards Risk Terminology

We have included references and abstracts to industry and standard organizations' risk taxonomies for reference:

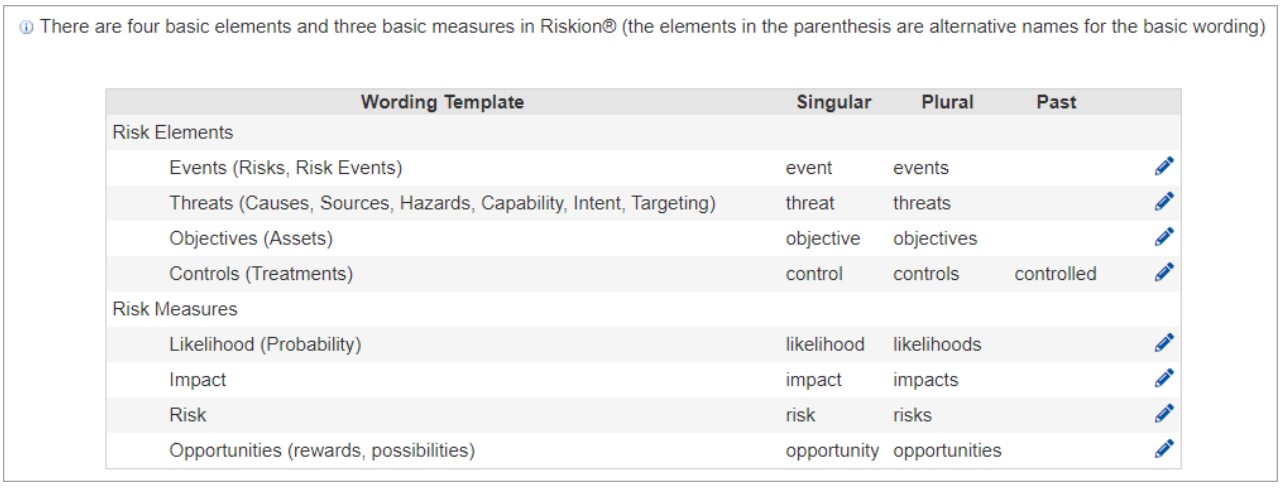
- DHS Risk Lexicon 2010 Edition
- Open Group
- ISO

The plethora of terms and definitions found in such references is a major obstacle for understanding and communicating risk. We have carefully distilled a large number of risk-related terms and definitions to just eight basic terms that we believe are necessary and sufficient to identify, measure, communicate and manage risk.

These eight terms include:

Four "**Risk elements**", and Four"**Risk measures**".

We have chosen 'default' terms for each of the eight as shown in the Wording Template in the figure below. This template is used in Riskion so that you can map the default terms to those that are familiar to those in your organization.


There are four basic elements and three basic measures in Riskion® (the elements in the parenthesis are alternative names for the basic wording)

Wording Template	Singular	Plural	Past
Risk Elements			
Events (Risks, Risk Events)	event	events	
Threats (Causes, Sources, Hazards, Capability, Intent, Targeting)	threat	threats	
Objectives (Assets)	objective	objectives	
Controls (Treatments)	control	controls	controlled
Risk Measures			
Likelihood (Probability)	likelihood	likelihoods	
Impact	impact	impacts	
Risk	risk	risks	
Opportunities (rewards, possibilities)	opportunity	opportunities	

As can be seen in the above template for customizing the terminology used in Riskion to that used in your organization, there are eight basic terms used in a Riskion model; four "**Risk Elements**", and four "**Risk Measures**".

Riskion Elements

Events

Events can be Risk Event or Opportunity Event.

Risk Events

The word '**risk**' is often used in two related but different ways: *What* can go wrong; and *How much* can go wrong.

What

When we ask, "*what* are the risks?" we are asking *what* can go wrong that will result in a **loss**, or perhaps multiple losses. We refer to these as **Risk Events** or just **Events** for short (for Risk Model).

When we ask "*how much* risk is there", we are asking for a measure or estimate of the risk of the Event or Events that might occur.

If, for example, you make an investment, you might ask what can go wrong that will result in a loss? The answer to this question might be formulated as:

One Event:

- "the investment declines in value", or

Several Events:

- "the investment declines 10% in value",
- "the investment declines 20% in value", ...
- ...
- "the investment loses all of its value".

Another example might be, "what can go wrong with our information processing operations?" This answer to this question might be formulated as:

One Event

- "a cyber attack is made to our information processing operations", or

Several Events:

- "a denial of service attack is made on our information processing operations";
- "sensitive information is accessed by an unauthorized individual or organization";
- "data is destroyed";
- "data is modified";
- .....

How Much

In order to communicate and manage risk, we need to do more than just identify events, we need to measure or estimate their risks. This is the *"How much"* dimension of risk.

For example, there is a 15% risk to this investment, or 5% of our assets are at risk from a cyber attack.

For Risk Events, Riskion is designed to:

- Identify the "what" can go wrong (Events),
- Measure/estimate 'how much' risk each event poses (Expected Loss)
- Identify what can be done to reduce the risks (Treatments)
    - Decide what and how much to invest in reducing the risks (Allocate Resources)

Opportunity Events

An Opportunity Event is another type of Event that is an opposite of a "risk event" -- instead of asking *what* can go wrong that will result in a loss, we ask what can go right that will result in a "**gain,"** or multiple of gains.

For Opportunity Events, Riskion is designed to:

- Identify the "what" can go right (Events),
    - Measure/estimate 'how much' opportunity each event poses (Expected Gain)
    - Identify what can be done to increase the opportunities (Stimulants)
    - Decide what and how much to invest in increasing the opportunities (Allocate Resources)

Threats

- An EVENT may be unconditional or it may DEPEND on one or more THREATS.
    - The THREATS can be referred to as CAUSES, HAZARDS, or SOURCES.
    - A threat (cause or hazard or source) is a situation that contributes to or influences the likelihood of an event taking place.
    - For example, a hazard is a potential threat of harm. It can be an activity, condition, operation, or object which can cause one or more events that result in injuries, damage, loss of material, or inhibit the ability to perform a prescribed function.
    - In Riskion, we refer to threat, causes, hazards, and sources interchangeably. While they may have slightly different nuances depending on the context in which they are used, they serve the same purpose in Riskion -- they are all threats of risk.
    - An event can have but doesn't necessarily need to have a threat.
- Threats (causes, hazards, and sources) present a potential for loss, but the actual loss is represented by events as discussed above.
- A cause may depend on other causes which in turn may depend on other causes. These can be represented hierarchically in Riskion.
- Unlike Events that must be uncertain, a cause may be certain or uncertain. If uncertain, we need to measure or estimate its likelihood or probability.
- If an EVENT is dependent on just one uncertain threat, then:
    - the likelihood of the event is the likelihood of the cause times the likelihood of the event given the cause. The latter is referred to as VULNERABILITY.
    - Example:
        - What is the likelihood of having an automobile accident today?
        - We may or may not be in a car today so we could refer to the cause as driving in a car. (We could have more than one cause --- see below).
        - The likelihood of an accident would be the likelihood of driving in a car today times the likelihood of having an accident given that we drive in a car today.
    - If an event has two or more (mutually exclusive) causes that are uncertain then
        - the likelihood of the event is the sum product of the likelihoods of the causes times the likelihoods of the event given the causes (Vulnerabilities)
        - Example:
            - it might rain
            - it might snow
            - it might not rain or snow
            - The likelihood of an accident would be the sum product of the likelihoods of each of these causes (or situations) times the likelihoods of an accident given each of these causes.
    - Causes and events are often confused in practice and it is important to distinguish between them.
        - A cause may lead to an event entailing a loss, but a cause has no loss in and of itself.
        - In an article "Don't Confuse Risk with Risk Sources", (http://www.ababj.com/risk-management/item/4348-don-t-confuse-risks-with-risk-sources) EricHolmqist, of Accume Partners, states:
            - There is a common challenge we see in how people approach risk assessments, and that is distinguishing between risks and risk
            - Understanding the difference between these two is important to building better risk assessments,

and critical to creating effective and efficient treatments.
        - Holmqist suggests that:
            - a risk (or risk event)
                - is tied to a defined process, since virtually all risks represent a process failure of some sort;
                - should have an impact that can be quantified;
                - should generally reflect an unexpected outcome.
            - and that a risk source(cause/hazard):
                - Can be distinguished by asking the question "What might lead to an event taking place?"
                - is a circumstance or action that would set the stage for an unwanted event;
                - as a threat of the event, should not be confused with the event itself (what could go wrong).
            - Anything that is not a Risk (Event), may well be a risk threat (hazard/cause)

Objectives

- The consequence of an event is the loss in the form of failing to achieve one or more OBJECTIVES and or the loss to one or more ASSETS.
- ASSETS:
    - Assets may or may not be explicitly part of a risk analysis.
    - If included in risk analysis, assets are useful in helping to identify events that would cause a loss to the assets.
- Objectives may be broad (e.g., considering organization-wide strategic, operational, compliance, and reporting requirements) or more narrow (e.g., relating to a product, process, or function such as supply chain, new product sales, or regulatory compliance).
- Strategic risk analysis often includes a broad hierarchy of objectives/sub-objectives/... with the lowest level of the hierarchy consisting of the 'Consequences' to the organization's objectives.
    - External
        - Economic
            - Financial markets
            - Unemployment
            - Mergers & acquisitions
            - Competition
        - Natural Environment
            - Financial viability
            - Quality of execution
            - Service level agreements
        - Political
            - Government/policy
            - Laws & regulations
    - Internal
        - Infrastructure
            - Availability of assets
            - Capability of assets
            - Access to capital
            - Complexity
        - Personnel
            - Employee capability
            - Fraudulent activity
            - Health & safety
        - Process

            - Capacity
            - Design
            - Execution
            - Suppliers &dependencies
        - Technology
            - Data integrity
            - Data & systems availability
            - Development &deployment
            - Maintenance
    - The **Impact** would be the sum product of the consequences to each objective times the importance of the objectives.
- In simple cases, there may be just one or a few OBJECTIVES or CONSEQUENCES.
    - Example
        - What would be the impacts of a delay in delivery of parts by our one supplier
            - Financial losses
            - Brand damage
    - Scope:
        - The scope of risk analysis may be enterprise-wide or limited to a particular operational or geographical area

Controls

Three types of controls can be identified and evaluated with Riskion:

- Controls to reduce the likelihood of one or more sources of risk -- causes, hazards, and threats.
- Controls to reduce the likelihood of an event given a source (e.g. a cause).
    - The likelihood or probability of an event given a cause is known as a VULNERABILITY
    - A vulnerability or the likelihood or probability of an event given a cause is a conditional likelihood or probability.
- Controls to reduce (i.e. MITIGATE) the impact of an event on an objective.

For Opportunity Events, instead of "CONTROLS", we are identifying and evaluating STIMULANTS to increase the likelihood of one or more sources; the likelihood of events given a source, and the impact of an event on an objective.

Risk Measures

Likelihood

The Department of Homeland Security RiskLexicon distinguishes between qualitative/semi-quantitative and quantitative likelihood:

- Qualitative and semi-quantitative measures, e.g. high, medium, and low, may be represented numerically, but cannot be used mathematically.
- Quantitative measures, on the other hand, have derived likelihood measures that can be used mathematically
- While Riskion produces only 'Quantitative'measures that can be used mathematically (such as multiplying by impact to derive a measure of risk), most risk assessment tools use qualitative or semi-quantitative measures and thus do not produce a mathematically meaningful measure of risk.

PROBABILITY

The DHS Risk Lexicon defines Probabilityas a specific type of likelihood, meeting more stringent conditions:

1. the probability of the random event —”A” must be equal to, or lie between, zero and one;
    1. the probability that the outcome is within the sample space must equal one; and
    2. 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

- The 'Likelihood" measures in Riskion satisfy these conditions and could also be referred to as "Probabilities".
- Colloquially, as well as in Riskion, Probability is used as a synonym for Likelihood.
- In statistical usage, however, there is a clear distinction between probability and likelihood:
    - probability allows us to predict unknown outcomes based on known parameters
    - likelihood allows us to estimate unknown parameters based on known outcomes
    - Strictly speaking, Riskion's measures of uncertainty are 'probabilities' because the task at hand is to predicts outcomes rather than to estimate parameters of probability distributions. However, Riskion uses the term Likelihood because it is in more common usage for risk assessments.

Probability of Events

The probability of events may or may not be conditional. They are unconditional for events that do not depend on any cause (or any source).

- Event probabilities are conditional events that depend on one or more sources (causes/hazards/threats).
    - In this case, the event probability is the sum product of the probabilities of causes times the probability of the event given the causes
        - P(Events) dependent on Causes -- Venn Diagram
            - P(Events) dependent on Non-Mutually Exclusive Causes-- Venn Diagram
            - Each of the above probabilities estimated with one of several methods described below
    - For example, the DHS Risk Lexicon states that:
    - The likelihood of a successful attack occurring 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, the likelihood of occurrence is typically informed by the frequency of past incidents or occurrences.

Impact

- The IMPACT of an event is a CONSEQUENCE of the event in the form of a loss to one or more objectives of the organization.
- While some losses can be expressed in terms of dollars, other losses may be qualitative (e.g. damage to a brand).
- The IMPACT of an event is the sum product of the losses to the organization's objectives times the importance of those objectives, some of which are typically qualitative.
- The Analytic Hierarchy Process is ideal for structuring an organization's objectives in the form of a hierarchy and deriving ratio scale measures of the relative importance of objectives.

Risk

- The risk of an event (or just risk for short) is the product of the risk event's likelihood and its impact.

Opportunity

- The opportunity of an event (or just opportunity for short) is the product of the opportunity event's likelihood and its impact.