Risk vs. Uncertainty

Intuitively, risk and uncertainty are noticeably different. The former implies more specificity in terms of what might happen, while the latter is a reflection of a general state of ambiguity regarding the future. In more concrete terms, the key risk consideration is whether or not the (known) event will occur, while uncertainty connotes a non-specific insecurity or ambiguity regarding the future in general. Not surprisingly, risk theorists tend to conclude that it is extremely important to draw a clear line of demarcation between risk and uncertainty. Perhaps the best set of original ideas trying to differentiate between these two concepts can be traced back to the work of Frank Knight, dating back to the early 1900's. In his seminal book, *Risk, Uncertainty & Profit*, published in 1921, Knight comes to following conclusions: '...Uncertainty must be taken in a sense radically distinct from the familiar notion of Risk, from which it has never been properly separated. The term 'risk', as loosely used in everyday speech and in economic discussion, really covers two things which, functionally at least, in their causal relations to the phenomena of economic organization, are categorically different. ... The essential fact is that 'risk' means in some cases a quantity susceptible of measurement, while at other times it is something distinctly not of this character; and there are far-reaching and crucial differences in the bearings of the phenomenon depending on which of the two is really present and operating. ... It will appear that a measurable uncertainty, or 'risk' proper, as we shall use the term, is so far different from an unmeasurable one that it is not in effect an uncertainty at all. We ... accordingly restrict the term 'uncertainty' to cases of the non-quantitative type'.

Building upon Knight's work, Hubbard offered a more operationally clear differentiation between risk and uncertainty[1]. According to him, risk always implies uncertainty, but not the other way around—uncertainty does not necessarily imply risk, which is in keeping with the definition of risk offered in the opening paragraph of this chapter. More specifically, Hubbard offers the following risk vs. uncertainty tests: An event of a circumstance can be categorized as uncertainty if:

Definition:	The lack of complete certainty, that is, the existence of more than one possibility. The true outcome / state / result / value is not known.
Measurement:	A set of probabilities assigned to a set of possibilities. Example: There is a 60% chance this market will double in five years.

Otherwise, an event or a circumstance can be categorized as risk if:

Definition:	A state of uncertainty where some of the possibilities involve a loss, catastrophe, or other undesirable outcome.
Measurement:	A set of possibilities each with quantified probabilities and quantified losses. Example: There is a 40% chance the proposed oil well will be dry with a loss of $12 million in exploratory drilling costs.

Knight's and Hubbard's reasoning has a strong appeal, considering that the goal of managing threats confronting business organizations is to minimize the organization's exposure to potentially economically damaging events, or to support the attainment of stated strategic objectives. Uncertainty is undeniably ubiquitous and as such, very difficult—if not altogether impossible—to manage effectively. Risk, on the other hand, can be construed as a special case of uncertainty, further contextualized by the stated organizational strategic objectives.

It is also true, however, that much has changed since Knight published his insightful ideas. Most notably, the global economy is now leaning toward service, rather than manufacturing industries – in fact, according to the most recent figures available from the World Bank, of the twenty largest economies –

[1] Hubbard, D. (2007), *How to Measure Anything: Finding the Value of Intangibles in Business*, John Wiley & Sons, Hoboken, NJ, pg. 46.

i.e., the so-called G-20 – only three (China, Indonesia and Saudi Arabia) derive more than 50% of their gross domestic product from manufacturing. Hence it follows that a considerable number of business organizations are engaged in activities where the primary—meaning, of most concern—source of threat are events that both Knight and Hubbard would classify as uncertainty, rather than risk. For instance, a financial services organization, such as a bank or a mutual fund manager, can certainly be adversely impacted by natural catastrophes, but the potential peril would more than likely pale by comparison to the impact that mismanaged or miscalculated market or credit exposures would have on those organizations[2]. Secondly, in a methodological sense the notions of risk and uncertainty do not exhibit the necessary discriminant validity[3], as these two concepts are confounded and situation-dependent. For instance, two otherwise similar organizations could have considerably different analytical capabilities, so much so that what might appear to be un-measurable (and thus considered 'uncertainty') to one might be measurable (and thus considered 'risk') to the other.

In view of the above, what is the value of differentiating between risk and uncertainty, in the context of risk management? Are we getting too entangled in semantic considerations?

Let us go back to the basic definition of risk compiled by Merriam-Webster: Risk is a possibility of loss or injury. A loss can be a result of property damage caused by a natural disaster, it can be a result of a lawsuit brought by customers (product liability), shareholders (executive liability) or regulators (non-compliance), or it can stem from a decline in value of market securities. It can take on a number of other forms as well, but in all cases it will manifest itself as adverse impact on the organization's earnings. Furthermore, just because the outcome itself appears more tangible does not mean that the potential threat is more measurable. Each year, several hurricanes move along the Gulf Coast of the United States, and even though many follow very similar paths, their impact varies considerably. With that in mind, let us consider Hubbard's definitions of risk and uncertainty, presented earlier. The author defines uncertainty as '…the lack of complete certainty, that is, the existence of more than one possibility; the "true" outcome / state / result / value is not known'. At the same time, he defines risk as '…a state of uncertainty where some of the possibilities involve a loss, catastrophe, or other undesirable outcome'. Are these definitions meaningful, or sufficiently distinct, in the context of the aforementioned Gulf Coast hurricanes? Not at all and here is why.

Whether our focus is on hurricanes or any other type of a natural or a man-made threat, it is hard to envision a situation other than 'the lack of complete certainty', to use Hubbard's words. Short of being able to gaze into the proverbial crystal ball, the lack of complete certainty is a ubiquitous property of future events, as prior to materializing the future state of any outcome is probabilistic in nature. Even if we know that the onslaught of a bad storm is unavoidable or the shareholder suit imminent – we do not have complete certainty regarding the ultimate consequence of either of these two, and countless other threats. The reason that Knight's and Hubbard's uncertainty vs. risk differentiation lacks operational clarity and definitional distinctiveness is because they do not expressly consider the *degree of knowability* of individual threats.

The key to being knowable, for a particular threat, is to be estimable using objectively sourced information. Furthermore, to be estimable a threat has to be assessed in the context of two key dimensions that jointly determine its expected consequences: 1. how likely is it to occur, and 2. how severe will be its impact. Recalling an earlier-made assertion that all future events are speculative (probabilistic), the distinction between the likelihood (#1) and the severity (#2) helps to illustrate why that is the case: From the standpoint of managing the organization's risk exposure, it is imperative to not only know the expected chances (likelihood) of a particular threat occurring, but it is also critical to know the force of its impact (severity). For example, if threats A and B have 90% and 10%, respectively, probability of

[2] Two relatively recent events illustrate that point: The Financial Crisis of 2007-08 (also known as the Great Recession) and the Superstorm Sandy both directly impacted Lower Manhattan, home to some of the world's largest financial service organizations, yet only the former threatened the very survival of the said companies.

[3] A notion describing the degree to which a particular operationalization diverges from other, conceptually distinct, operationalizations – in other words, does it just sound differently, or is it indeed different?

occurrence, threat A appears to be clearly more worrisome – however, if A's severity is estimated at $10,000, while B's at $1,000,000 a different conclusion emerges[4].

Keeping the above in mind and turning our attention to the uncertainty vs. risk distinction and the notion of the degree of knowability, I define *uncertainty* to include all threats that have non-estimable likelihood and severity, and I define *risk* to include all threats that have estimable likelihood and severity. Furthermore, both likelihood and severity will be deemed non-estimable when the requisite data either do not exist or are insufficient, in view of an estimation methodology under consideration. Lastly, given the multiplicative nature of the two threat-defining dimensions of likelihood and severity, to be estimable a particular threat has to have the requisite data available for both dimensions.

Broadening the Scope of Risk

As discussed in the preceding section, the term "risk" denotes a *threat*, which is a reflection of certain amount of linguistic conditioning causing us to think of risk as a possibility of an undesirable event taking place. And certainly, every business organization faces a considerable amount of *downside*—defined here as asset damaging or loss-generating events—risk. The same organizations, however, also face a wide array of *upside risks*, defined here as an unrealized growth opportunity. For example, an electric utility with power generating plants located in the Gulf of Mexico region faces the downside risk of hurricane related wind damage, while at the same time it faces the upside risk associated with the decision to invest or not in renewable power generation assets. To truly appreciate the risk exposure of the said utility, it is necessary to assess both its downside as well as upside risks, hence our conception of risk needs to be framed in the context that includes both the avoidance of undesirable events, i.e., downside risks, as well purposeful pursuit of desired states, i.e., upside risks.

Downside risk is the possibility of asset-damaging or loss-generating events taking place, while *upside risk* reflects the chances of anticipated growth not materializing. Both can adversely impact the organization's earnings.

It follows that risk is not necessarily something to be avoided—in fact, good risk taking can have a very positive impact on the organization. Microsoft took a risk by tying its success, in terms of its core operating system, to the proliferation of personal computers, just as Google took a risk by deviating from an established practice of charging advertisers based on the actual visits to their websites, rather than total traffic (which was an established practice at that time). These are examples of companies that successfully increased their exposure to upside risks—of course, there are numerous examples of ineffective upside risk taking, such as the much-anticipated entrance of IBM into the personal computer industry in the 1980's (which turned out to be unprofitable for the company, ultimately causing it to exit out of that business) or the ill-advised decision by Gateway in the 1990's to vertically integrate by expanding into retail. Although the anecdotal evidence is mixed, the aggregate results overwhelmingly point to the desirability of increasing the exposure to the upside risk, as evidenced by the higher overall returns realized by investors (both individuals and organizations) who put their money in equities, rather than government and corporate bonds.

There is an important nuance, however, that needs to be addressed—risk taking recklessness. First reported by Bowman[5], and subsequently coined the Bowman Paradox, the positive risk-return relationship does not hold for organizations engaging in poor risk taking. Specifically, firms earning below average returns tend to exhibit negative risk-return relationship, while those earning above average returns tend to exhibit the (expected) positive risk-return relationship. In other words, good risk taking will advantageously increase the upside risk, while limiting the downside risk.

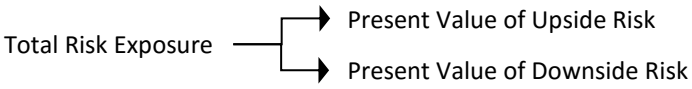
---

[4] 0.9 * $10,000 vs. .1 * $1,000,000.

[5] Bowman, E.H, (1980), 'A Risk/Return Paradox for Strategic Management,' *Sloan Management Review*, vol. 21, 17-31.

Bowman, E.H, (1982), 'Risk Seeking by Troubled Firms,' *Sloan Management Review*, vol. 23, 33-42.

Overall, at any given time the organization-specific total risk exposure will be a sum of net present value of both the downside and upside risk, or

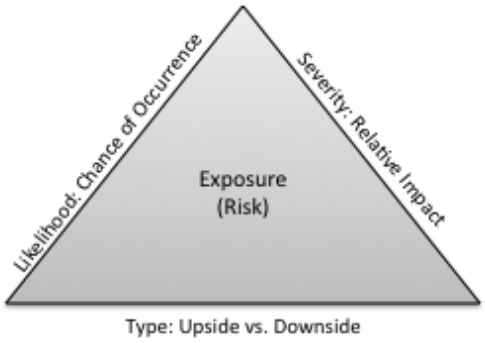


It is competitively advantageous to an organization to thoughtfully increase its exposure to upside risk, while systematically lowering the potential impact of downside risk. Increasing the spread between the two types of risks will systematically enhance the organization's competitive advantage. It follows that management of upside risk entails systematic evaluation of risks to be taken, while management of downside risk calls for systematic reduction of risk exposure.

Aside from considering what types of events should fall within our conception of risk, it is also important to explicitly estimate the possibility of both the upside and downside risks affecting the organization. It is intuitively obvious that risk potential is a function of two, usually independent dimensions of *likelihood/probability* and cost, usually referred to as *severity*. Risk is inherently probabilistic because it reflects uncertainty associated with the future. Events that have not yet occurred but whose future occurrence is known with certainty are not risks—they are more accurately described as either assets or liabilities. For instance, a lease payment that is to be made on a periodic basis is a liability, because its occurrence (or rather, its recurrence) and amount are known exactly ahead of time. On the other hand, future wind or flood related property damage is a risk because neither its occurrence nor the amount of damage are known ahead of time. Both good and bad outcomes, and upside and downside risks, respectively, can be expressed in terms of the likelihood of occurrence and the magnitude or severity of the resultant gains or losses.

The third and final component of the definition of risk, in the organizational context, should the standardized impact estimation. This is most important when dissimilar risks are evaluated in a holistic, or enterprise-wide setting, and when resource allocation decisions are based on those evaluations. The most reasonable benchmark for cross-risk-types impact comparisons is the net earnings impact assessment. Stated differently, to adequately communicate the magnitude of an upside or downside risk, and to make rational (i.e., reflecting risk type-specific impact) resource allocations, the assessment of risk needs to be expressed in terms of the impact on the organization's revenues or earnings. Figure 1 summarizes the three key definitional components of risk.

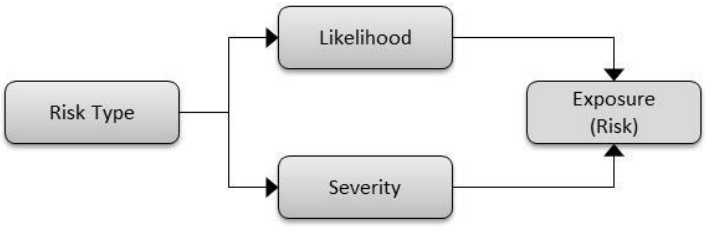
Figure 1
Key Components of the Definition of Risk



Although nominally the type of risk, the possibility of occurrence and the relative impact all play a role in framing individual risk types, their roles are not the same. More specifically, the type of risk and the possibility of the risk event materializing are both antecedents (i.e., they precede) the risk event, while

its impact follows the risk event. Hence from a causal standpoint, it is more appropriate to express risk in the following manner:

Figure 2
Causal View of Risk



The causal view of risk is essential to the development of a holistic risk management approach, or active management of the organization's risk profile, because it draws attention to the distinctiveness of managing the underlying root causes of risk and the capitalization of the possible risk outcomes. To actively manage the organization's exposure to risk, explicit steps need to be taken to mitigate the possibility of unfavorable outcomes and to put in place economically optimal capital provisions.

Assessment of Risk

Accepting the dual face—upside vs. downside—of risk stretches the conceptual boundary of our conception of risk and so by extension, it also expands the requisite operationalization of it. Intuitively, there are considerable measurement differences separating risks as diverse as hurricanes, fraud, and cost of capital fluctuations or strategic missteps. The risk estimation process, however, will tend to follow a similar set of steps, as depicted in Figure 3.

Figure 3
Risk Estimation Process

First and foremost, individual risks need to be clearly identified. As detailed later, there is a long list of upside and especially downside risks that could potentially have a material impact on the organization's financial well-being. Once clearly delineated, the potential impact of each of the risks needs to be estimated, in terms of the probability of the event taking place as well as its severity. The *Estimation* stage is usually most readily associated with the notion of risk analytics, as it tends to be the most "analytical" part of the overall process, however, just presenting the likelihood and severity estimates outside of the earnings impact can be of limited utility to the decision makers because it does not expressly contemplate the net impact of risk on earnings.

Mapping of the individually identified and estimated risks is the next step in the risk analytics process. It is, in effect, putting together of a "risk puzzle", or a matrix of individual risks categorized in the context of estimated likelihood and severity. Figure 4 offers a generic example of a risk map.

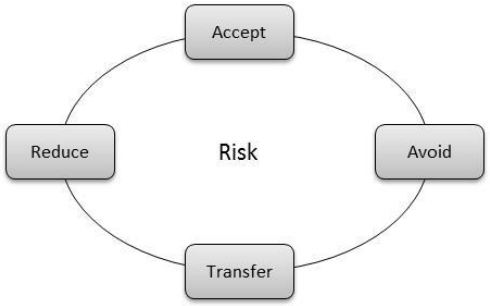
Figure 4
Hypothetical Risk Map

In the illustration shown above, each individual risk is plotted on the likelihood—severity grid, with each risk dimension being broken out into four magnitude-based quartiles. In effect, the probability and the estimated cost of each event are used as basis for placing individual risks into an appropriate cell. In the resultant 16-cell matrix used here, the four cells falling at the intersection of the top two likelihood and the top two severity quartiles are highlighted (in red) as the high risk region, while the four cells falling at the intersection of the bottom two likelihood and bottom two severity quartiles are highlighted

(in red) as the low risk region. Using quartile-based likelihood and severity is somewhat of an arbitrary choice, as circumstances might warrant a more granular (such as decile-based) or coarser view—the important point here is that an single categorization schema should be applied to all risk to enable robust and objective side-by-side risk impact comparisons.

The next step in the risk analytics process is that of determining the most appropriate response. Consider Figure 5.

Figure 5
Response Selection



There are four distinct risk responses: *acceptance, reduction, transfer* and *avoidance* (more on each later in this chapter). The goal of this stage of the risk analytics process is to overlay the impact on earnings-adjusted efficacy of each of the four options onto the risk map develop in the previous stage, which leads to the final stage of the process: *Capitalization*. Virtually all non-zero likelihood risks, both upside and downside have capital implications ranging from setting aside funds for insurance coverage acquisition to contingent capital planning to product infrastructure investments.

Exposure

It is intuitively obvious that the degree of risk exposure will vary, at time significantly, across companies. Upon a bit more reflection, it also becomes intuitively obvious that cross-company risk exposure will depend primarily on the degree of business spread (the number of distinct product or service types offered) and geographic spread (the number of physical locations). A business entity that is comprised of multiple, dissimilar business units—i.e., a diversified conglomerate—will tend to be exposed to a wider array of risks than an entity operating a single business unit. For example, a vertically integrated electronics manufacturer (i.e., a company engaged in manufacturing and retail) will bear the risks associated with manufacturing as well as retailing, while a company engaged only in manufacturing will only bear the risks associated with manufacturing.

In a similar manner, an organization that operates in multiple geographic locations and/or jurisdictions will face more risks than a single location organization. For instance, a multinational firm is exposed to proportionally more regulatory, environmental, contractual and physical risks than an organization operating in a single location/jurisdiction.

Of course, that is not to say that it is more advantageous to only compete in a single product line or a single location as this type of concentration carries its own perils—the assumption of risk needs to be evaluated in the context of return it generates. In other words, the risk posture of an organization needs to be commensurate with the organization's economic returns. Furthermore, any incremental risk associated with the contemplated course of action needs to be contrasted with the expected incremental economic gain. For example, building an oil refinery in the coastal region of the Gulf of Mexico heightens the risk of hurricane-related wind damage, while at the same time it is advantageous from the standpoint of crude oil access and transportation costs. To make a rational build vs. not build decision, one has to be able to objectively estimate the incremental economic values of both sides of the risk—return relationship. Doing

so, however, will amount to just a single step in the multi-step enterprise risk management process. In addition to wind damage related risk, what other risks need to be taken into account to make a more holistic risk assessment of this particular project. And what is the nature of any cross-risk type interdependencies?

Management of Risk

In 1956, Harvard Business Review published 'Risk Management: A New Phase of Cost Control', which posited that a professional insurance management should be the domain of a risk manager. Roughly two decades later, The American Society of Insurance Management changed its name to Risk and Insurance Management Society, and about a year later, in 1976, Fortune magazine published a seminal article titled 'The Risk Management Revolution', which discussed '…the coordination of formerly unconnected risk management functions with an organization with oversight by the board of directors'. In many regards, these events marked the rise of formal (i.e., department-based) corporate risk management functions. The creation of the first-ever Chief Risk Officer position by GE Capital in 1993 brought even a greater level of recognition of the importance of organization-wide, senior management level risk exposure oversight.

Risk management as an attempt at diminishing the exposure to risk, rather than a structured organizational function, has a far longer history. Interest rates, which started to emerge roughly 5,000 years ago in Babylon, are the earliest known form of a specific, definable way of treating risk. The Code of Hammurabi, circa 1755 BC, contains the first formal form of risk shielding, or insurance. By creating the concepts of 'bottomry' (i.e., ship bottoms) and 'respondentia' (or cargo), it laid the foundation for marine insurance which was built around the three key components: 1. a loan on a vessel or cargo, 2. an interest rate, and 3. a surcharge to cover the possibility of loss. In effect, ship owners were the insured and lenders were the underwriters. By about 750 BC, the concepts first introduced in the Code of Hammurabi were refined into the notion of 'general average', which became a fundamental notion underlying marine and other forms of insurance coverage.

Modern day insurance based risk management dates back to 12th century Italian ports, most notably, Venice (in fact, the term 'policy' is derived from Italian 'polizza', meaning a 'promise' or an 'undertaking'). Roughly five centuries later, insurance began to take hold in the Great Britain, with the Great Fire of London of 1666 giving rise to the first insurance company, The Insurance Office, formed a year later.

As noted earlier, however, risk management goes far beyond insurance coverage acquisition—more specifically, it encompasses the following set of activities:

Risk type identification.
Specific and distinct threats to the organization need to be singled out in an operationally clear manner.

Risk type impact estimation.
The two distinct and independent dimensions of risk—likelihood and severity—need to be estimated in terms of their potential impact.

Aggregate risk mapping.
Individual risks need to be pulled together into a single, coherent picture of the overall threat to the organization.

Response optimization.
Taking action is a logic consequence of the previous three steps.

These four sets of activities are causally related, as shown in Figure 6 below.

Figure 6
Interdependence of Risk Activities