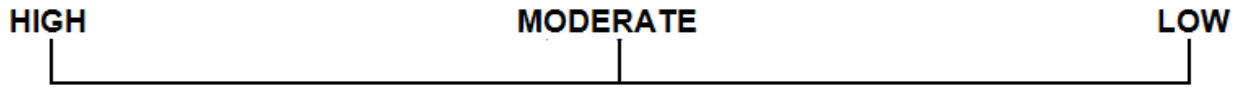
RISK ATTRIBUTION ISSUES

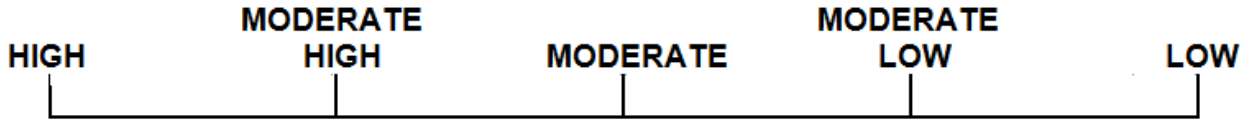
Sheldon C. Bachus

Previous articles in the *Business Forum Journal* have contributed to a general understanding of how risk assessment practices support the management of institutional and corporate risk. In this article we consider specifically the degree to which risk can be ranked and quantified.

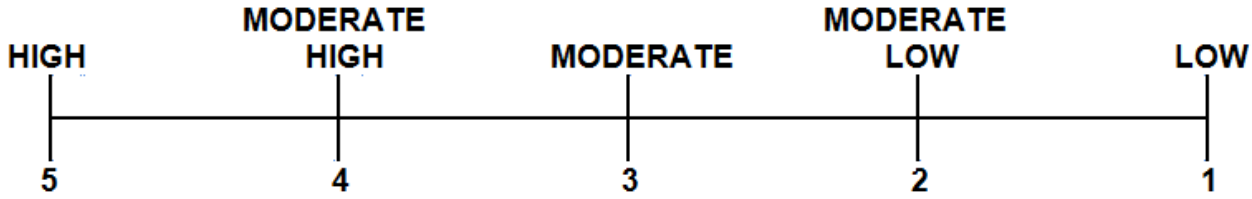
The assessment of institutional risk is not a simple task, nor are its results necessarily accurate. This is especially true when issues of risk attribution are involved. Risk attribution is the process by which we quantify or otherwise identify the threats associated with a given course of action, decision, or set of valued resources. Typically, the first step in the attribution process is to rank risk along a continuum ranging from high to moderate, and then low risk:



Viewed In this light, the risk attribution process is at its core *stochastic* – from the Greek *στόχος* meaning to *aim* or *guess*. From the outset, many of our decisions are intuitively based on where we see risk falling along the high-moderate-low risk scale. Our decisions are stochastic in the sense that we are aiming or guessing at the level of risk involved. To make our aim more accurate, we sometimes refine our estimate by increasing the accuracy of the scale:



Terms such as “moderately high” or “moderately low” are quickly recognizable as the shibboleths of investment brokers, and are part and parcel of the language of public stock offerings and their attendant prospectuses. Likewise, using the cudgel of the Gramm-Leach-Bliley Act (GLBA), government regulators and auditors tend to evaluate the strength of corporate risk assessments based on a quantified five point risk scale:



Unfortunately, using this quantified approach to risk attribution, not a few control reviews have ended with pronouncements such as “risk has risen to an unacceptable level of 3.95, and must be further controlled by immediate management action.” When pressed to demonstrate *why* risk is at precisely the 3.95 level, nobody can because, on a five point scale, values expressed with two decimal digits are relatively meaningless. The point here is*: we use quantified values only as a stochastic measure of estimating and identifying the approximate level of risk present, and its tendency to change within our institutional and corporate environments*. Remaining, however, is the question of *why* or *how* a given level of risk was determined in the first place.

The answer rests in the nature of risk itself, including the type of risk we are managing, its source, component threats, and expected institutional impact.

Reflecting its auditing roots, risk is conceptually organized into two broad categories – inherent and controlled. *Inherent risk*, sometimes referred to as *native risk*, represents the level of risk present before any precautions are taken to mitigate it. For example, doing business over the Internet produces a plethora of inherent risks ranging from hacker attacks on corporate data to identity fraud. The risk associated with these threats is mitigated by protective measures or *controls* such as data encryption, firewalls, etc. With these measures in place the risk remaining is referred to as *controlled*. Interestingly, in response to GLBA regulatory requirements, many risk assessments found in the financial services sector tend to distinguish only between these two basic categories of risk, e.g.:

RESOURCE	INHERENT RISK	CONTROLLED RISK
Customer Data – Core	4.60	2.50

The weakness of this approach is that it does not distinguish between two important aspects of controlled risk. Conventional risk assessments implicitly define controlled or residual risk as *the risk remaining after controls have been implemented*. The distinction is that, when viewed in the context of conventional risk assessments, controlled risk is simply a desired *target*, and in no way is it intended to reflect the level of *actual controlled risk* that may be present.

In this light, if a risk assessment is to be a valuable management tool, it should distinguish between *targeted* and *actual controlled risk*. Typically, the actual controlled risk level should be based on the test results of the institution's most recent control review – an example being:

RESOURCE	INHERENT RISK	CONTROLLED RISK	
		TARGET	ACTUAL
Customer Data – Core	4.50	2.50	2.50
Customer Data – Mobile Apps	4.60	2.75	**3.00**

As illustrated, red-flagging of actual controlled values with a risk higher than their associated target level further enhances the utility of risk assessments based on this expanded concept of controlled risk. In any case, *we should always view specific risk assessment values only as approximate indicators of the level of risk present, and not as exact or "scientific" statements*.

So, to the final question: even if they are only relative indicators of risk, where do the quantified risk assessment values come from?

Successful risk quantification begins and ends with inherent risk. As indicated above, for any given resource or risk-weighted decision, inherent risk quantification rests on the accurate identification of component threats, their probability of occurrence, and potential impact. Each component is assigned an estimated risk scale weight, and then an aggregate risk level can be calculated from the component set, e.g.:

RESOURCE	THREAT / IMPACT ANALYSIS					INHERENT RISK
	Source	Probability	Exposure	Magnitude	Criticality	
Cust. Data Mobile Apps	4	4	5	5	5	**4.60**

Implicit in this approach is the assumption that the assignment of scaling values to each component follows a reasonably rigorous protocol. For example, reflecting the five point scale illustrated here, component threat occurrence probabilities (e.g., 0.995, 0.722, 0.568, 0.387, 0.009) are organized into a set of tiers such that the highest probability level (0.995) is weighted at 5, the second or "moderate high" probability (0.722) at 4, etc. Establishment of the tiered probabilities should, of course, rest on a generally accepted and empirically substantiated standard.

Once inherent risk levels are established, their associated target control risk values are defined as a function of two parameters: (1) the specification and presence of the requisite set of controls necessary to mitigate the inherent risk; and (2) the institution's accepted target control risk value. Although both parameters are subject to regulatory negotiation, the first generally determines how control testing proceeds, as well as the institution's overall cost of control. The second, the specification of a global standard target controlled risk value, has technical as well as regulatory implications, and is discussed in summary below.

Many risk assessments, use a single global target controlled risk value for all risk assessment items. Usually, selection of this value is slotted by negotiation between managers and regulators at a mid-point between moderate and low risk. However, the slotting process may reflect any number of institutional variables ranging from operating history to regulatory performance. For example, *de novo* banks are frequently required by examining agencies to meet a lower target control risk level than are more mature institutions.

Rather than use a single global target controlled risk value for all risk items, increasingly many risk assessments employ a tiered risk table to adjust target controlled risk based on each risk item's associated inherent risk level. The assumption here is that *the magnitude of the inherent risk will necessarily elevate the value assigned to the target controlled risk level*. The use of this approach permits elevated target values when, in fact, the cost of control is excessive. Generally, the regulatory community has accepted this risk assessment strategy because it demonstrates that management has performed appropriate due diligence by acknowledging the increased target controlled risk level, and opted for a concomitant increase in cost of risk rather than cost of control.

In summary, it remains important to apply quantitative techniques to the assessment and ranking of institutional risk. However, we should likewise remember that quantified risk values serve only as a stochastic indication of the actual risk that may be present.