



Skip the Numbers: Assessing Risk is not a Math Game!

By Larry Hubbard, CPA, CIA, CISA, CCSA

Executive Summary

Understanding organizational risk is an important consideration for the internal audit function. How one goes about gaining that understanding and how that understanding is communicated to others, especially senior management and the Board is an equally important consideration. Various means have evolved which run the gamut from detailed to general depictions. We know things may or may not change. Trying to predict when and to what extent something will happen is an exercise not worth undertaking. The best we can do is to make educated guesses preparing for the most likely happenings that will make the biggest impact on the organization. Developing a Risk Map is a function of discussions about future risk with those managers responsible for achieving organizational objectives. It permits consideration of the most likely scenarios and their impact and allows for timely preparation so the organization can readily deal with events as they arrive.

As internal auditors we use many approaches to address organizational risks. We select audits and audit areas using a risk-based approach; we evaluate and improve the organization's risk management process; we use risk matrices and risk registers in performing audit work; and we do risk mapping to help evaluate the importance of risk events. With all these 'risk' terms, it's no wonder there can be confusion, even amongst auditors, about their exact meanings. Most of the confusion is clarified within an organization by simply agreeing on consistent definitions. But other times the confusion can be more serious, because it impedes the overall effectiveness of the risk assessment processes, or at its worst can provide misleading results. This article examines the typical terms used in risk assessment processes, and helps auditors avoid one of the biggest risks of all, which is thinking that risk assessment is a mathematical exercise.

Some Simple Definitions

Let's start with some simple definitions (primarily from the Glossary to The IIA Standards) and a picture.

Risk event is the uncertainty of an event occurring that could have an impact on the achievement of objectives. Risk is measured in terms of impact and probability (also called consequences and likelihood).

Inherent risk (IR) is the risk to an entity in the absence of any actions management might take to alter either the risk's likelihood or impact.

Residual risk (RR) is the risk that remains after management's response to the risk. Risk assessment is applied first to inherent risks. Once risk responses (sometimes just called controls) have been developed management then considers residual risk.

Control risk (CR) is the risk that controls fail to reduce risks to an acceptable level.

Risk appetite is the level of risk that management is willing to accept in pursuit of achieving organizational objectives.

Audit risk is the risk of reaching a wrong audit conclusion. Within the context of sampling, audit risk comprises two types of risk: sampling risk and non-sampling risk.

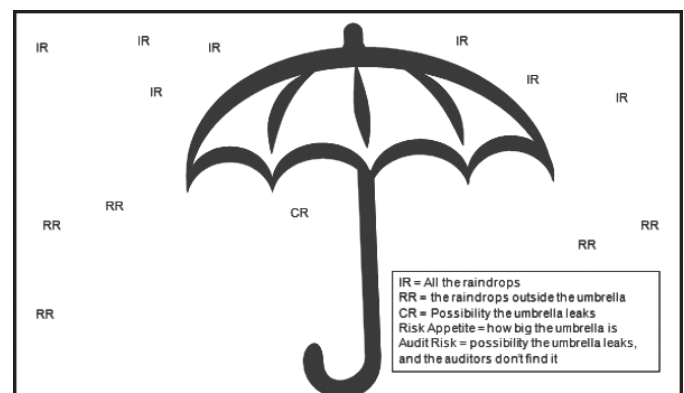
Sampling risk is the risk that an auditor's conclusion based on sample testing may be different from the conclusion reached if the audit procedure was applied to all items in the population.

Non-sampling risk occurs when an auditor fails to perform his or her work properly and fails to detect errors.

These terms are easily demonstrated by thinking of an umbrella (a control or risk response); raindrops (a risk event); and an objective to stay dry.

Risk-based Auditing—the First Math Game

For internal auditors, The Institute of Internal Auditors and other professional standards require auditors to base their auditing on an assessment of risks, and to focus on the most important objectives of the organization. We call this risk-based auditing, and it applies to the selection of audits to perform, as well as the areas to review within an audit. Often, auditors



use Risk Factors to help determine which audits to perform each year, and weight these factors based on their importance. One set of Risk Factors and weighting might be:

- Time since last audit—30%
- Results of last audit—10%
- Size or materiality of the area to be audited—40%
- Level or frequency of change—20%

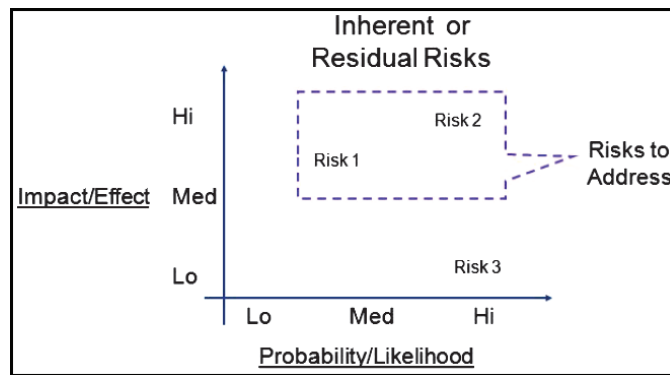
Regardless of the number of Risk Factors used or the weighting applied to each, it is impossible to predict, with certainty, which areas of an organization will need to be audited regardless of how we may define such a need. Similarly, while auditors do forecast the time an audit will require different auditors always forecast different (sometimes wildly different) time budgets for similar engagements. So, at best, deciding on the audits to perform each year, and the

At best, deciding on the audits to perform each year, and the number of auditors needed to perform those audits is an educated guess.

number of auditors needed to perform those audits is an educated guess. This is the first Math Game some departments engage in—by trying to select audits as a purely mathematical exercise rather than a decision based on discussions between the auditors, managers and the board. Those discussions are the valuable piece of the risk-based audit selection process, and being overly analytical can actually get in the way of good discussions.

Applying some twenty factors, each weighted differently and scored from

Table B



1 to 10, and then multiplied by a factor representing the anticipated length of the audit (retaining the decimal points) is a math game not worth playing! Using five equally weighted Risk Factors, which all measure different aspects of risk, and using simple High, Medium, Low scores can provide all the analytical input needed to support the discussions of what to audit.

objective. Then, based on the importance of each risk, management determines the action to take (e.g. change the objective to avoid or reject the risk; minimize the risk with a response; or accept the residual or remaining risk). Making an avoid, minimize, accept decision is the purpose of a Risk Map, also shown below.

Inherent Risk Assessment

Risk Map

Often the results of Risk Assessment and Risk Mapping are recorded in a Risk Matrix or Risk Register (Table B). These tools are used by many people—by auditors in performing an audit, by risk management personnel in conducting Enterprise Risk Management (ERM) workshops, and by managers in the Risk Assessment component of the COSO internal control framework.

Scoring the risk events on the Risk Map is the Second Math Game we sometimes play. The above example uses three levels: Low, Medium, and High to score risks. That method offers plenty of distinction to determine how to respond to a risk, because the real value of the scoring is to generate discussion about the risk events, not to decisively conclude about their impact or probability.

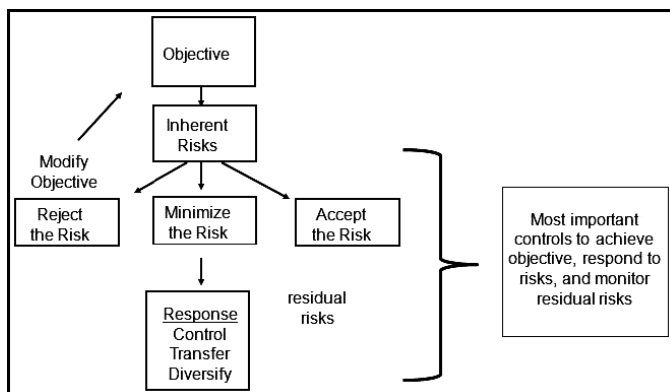
Risk events are about the future, which cannot be predicted. If an event does occur, then maybe it is a problem to be solved and avoided in the future, but it is no longer a potential risk event. Not solving existing problems, or letting them re-occur is not risk assessment—it’s called bad management.

So, while we cannot predict the future, we know there will be a future, so we had

Risk Mapping—the Second Math Game

Risk events are measured in terms of impact and probability, and often Risk Maps are used to determine the importance of a potential risk event based on those two terms. Mapping is used to determine whether to accept or respond to the risk event. Again, this is better depicted in pictures. Table A is an Inherent Risk Assessment. This identifies all the inherent risks that might impact achieving a particular organizational

Table A



better be ready for whatever happens. The economy will get better or worse or stay the same, but we don't know which. An event may happen or may not happen, at some unknown interval. At best we need to make educated guesses about those things, and prepare first for the most likely risks with the biggest potential impact. Shame on us if we do not prepare for the most common and most important things that could go wrong. But, just as no one can be sure they know all the inherent risks, because risk is about the future, neither can anyone really know how likely the risks are to occur. Regardless of the time spent, we simply cannot identify all risks in advance. So, risk assessment is about being ready for the future, not trying to predict it.

We get ready to deal with future risks by discussing, (with those responsible for achieving the objectives), the most likely and most important risks first, then move on to those which are less likely and less important. No one can finish the task of discussing all potential risks, but the more risks discussed, the more likely a group is to effectively deal with those risks no

one can predict. Risk appetite is actually a measure of that level of discussion. Managers with a low risk appetite spend lots of time discussing potential risks, and those with a higher risk appetite spend less time on it.

Risk assessment is about being ready for the future, not trying to predict it.

Conclusion

The point of a Risk Map is to generate discussion about the likelihood and impact of risk events, and to allow potential events to be dealt with in the order of their perceived importance. Any Risk Map with more than three gradients (low, medium, high) is likely trying to put more accuracy into predicting the future than is possible. If that mathematical accuracy gets in the way of effective risk discussions, then the risk assessment process suffers.

Finally, the COSO Risk Assessment components (in both the Internal Control and ERM frameworks) are about a group's ability to manage the risks to encounter while achieving their objectives. So any group of internal auditors completing Risk Maps, or identifying and scoring risks related to business objectives, without involving those responsible for achieving the objectives, really needs to think—are you evaluating an internal control (management's risk assessment processes), or are you attempting to perform an internal control yourself? Either way, you are not helping the business workers or managers get better at achieving their own business objectives, and that's that is even worse than a math game! **NP**

Larry Hubbard is a professional internal auditing trainer and consultant with a broad background in accounting, auditing, and finance. Prior to founding Larry Hubbard & Associates, Larry's work experience included careers at Mobil Corporation and Ernst & Young. More information is at www.LHubbard.com, and you can contact him at Larry@LHubbard.com.