

Risk & Uncertainty Management – Processes & Oversight

Dave Tate (San Francisco)

Attorney / CPA (inactive)

<http://tatetalk.com>; davetateesq@gmail.com

(See also board and audit committee self-evaluation materials for additional detailed discussions.)

I. Introduction and Overview

Management is responsible for risk and uncertainty management. The board and directors serve an oversight function. As a general proposition it is not possible to identify, assess, eliminate, control or manage all risk and uncertainty. To varying extent risk and uncertainty management requires the exercise of judgment relating to the future.

Although risk and uncertainty management topics tend to emphasize steps or processes, let's keep in mind that the steps or processes should be taken by people who should be qualified for their tasks, have access to the necessary pertinent and timely information, and have the appropriate demeanor or mindset, approach, knowledge and commonsense. Steps and processes are what they are, but people choose and exercise their own actions.

As risk, uncertainty and the future are always ongoing and changing, risk and uncertainty management isn't a one-time event but can be 24/7 in some circumstances. Keep in mind as you monitor, follow-up, and schedule subsequent meetings and actions it is possible that some of the risk and uncertainty management that you do on day one might or might not be as helpful or relevant on day two, or in a week, a month or six months.

I have not discussed in this form board, board committee or director oversight or risk oversight responsibilities in detail as those topics and discussions are for other materials. You can discussions in my separate Board of Directors Annual Self-Evaluation materials; Audit Committee Annual Self-Evaluation materials; and 2-Page Board & Director Guidelines. However, it should now be clear that risk management oversight is a board function.

Technical materials, discussions and opinions about risk and uncertainty management already are voluminous and increasing. As eyes gloss over it's easy to lose sight of the forest for the trees. Instead, the intent of this form, as an ongoing work in progress, is to provide one useful version of a concise and uncomplicated but accurate easy-to-use and get started format to assist you in the oversight of risk and uncertainty management processes.

For some people the format provided in these materials will be too uncomplicated or detail lacking – some of my risk professional friends might well consider this approach too simplistic – but any person using these materials can add and continue to add as much detail as desired. These materials encourage a get started and keep going approach.

I do note that as this is a developing area different people might in part use different or additional risk management terminology or processes, some of which might or might not be appropriate or understood with universal meaning. Ask appropriate questions if necessary.

The discussions in these materials are applicable for all entities – public companies, private companies and organizations, nonprofits and governmental entities – although depending on the entity type or situation, sometimes the terminology or context might be or need to be different. And of course some members of management and directors are extremely knowledgeable about these topics whereas others are somewhere in the middle or just beginning. All of that is okay.

These materials are a work in progress. Why is that? Because in this circumstance the current state of risk and uncertainty management, and board and director oversight of risk and uncertainty management are in various degrees of continual development and they will continue as such for some time to come.

I have intentionally not provided a checklist approach. More specific or targeted risk and uncertainty discussions can sometimes be found in other materials. But doing so in this material could cause more limited application of this form, which is contrary to my intent.

One additional comment – about terminology issues – I can generally say that in certain circumstances I have issues with some of the risk and uncertainty terms that appear in some of the resources, depending on how those terms are used or described including in some circumstances, for example, risk appetite, risk tolerance, assessment, and similar terms. My difficulty with terminology relates to situations where the terminology or its use might imply that a specific level or quantity of risk is acceptable particularly when the possible resulting impact or harm could be significant. Even if developed through legal counsel, I would certainly assume and act as if risk management identification, evaluation and processes are discoverable in litigation.

These materials do not provide legal or other professional advice, evaluation or opinion, and do not discuss legal or other professional standards, requirements or responsibilities – you should consult with a professional about your specific situation. These materials are updated from time to time, and as stated above, new developments are regularly occurring. This paper was prepared on June 20, 2014.

II. Risk and Uncertainty Management Defined

Several established and broadly recognized organizations have developed and provided their definitions of risk and uncertainty management. But there is no universally accepted definition. You will note that throughout these materials in addition to “risk” I have included “uncertainty.” I prefer “uncertainty” to “risk” but the more often heard reference is “risk” management. “Risk” suggests the occurrence of a negative or loss deviation from expected results; but as deviations can also be positive or beneficial, I believe that “uncertainty” management is the more accurate description. In part ISO 31000 *Risk Management* uses the “uncertainty” terminology (ISO stands for International Organization for Standardization). Accordingly, for these materials I have used both “risk” and “uncertainty” while recognizing that the use of the term “risk” is more universal.

Risk and Uncertainty Management: activities and processes used to help identify, evaluate or assess, prevent, manage, control, and monitor risks and uncertainties or deviations that may or may not occur in the future. Risk, according to ISO 31000, is the effect of uncertainty on objectives. Uncertainty or lack of certainty exists when the knowledge or understanding of an event, consequences, or likelihood is inadequate, incomplete or not absolute. In other words, as to the future we don’t have a crystal ball, and there is a chance that things will not go according to plan or as anticipated or assumed. The chance of deviation from plan or anticipation or assumption can be negative or a loss, or positive or a benefit.

III. Risk and Uncertainty Management Processes

Currently there are different approaches to risk management. There is no agreed upon or universally accepted overall approach; however, within certain specific topic areas of risk management by statute, regulation, rule or community standard or recommended approach there are requirements or approaches that have been enacted, adopted or recognized – it is beyond the scope of these materials to cover specific topic areas that you will need to know for your specific areas of interest and responsibility.

The following steps and processes are intended to help you with your framework and approach. You might find for your situation that some of the below steps and processes are not needed, or you might decide that additional steps, processes or detail are needed. As previously stated – your judgment definitely is important in this process.

1. Identify the people who will be involved in the risk and uncertainty management process, or if necessary reevaluate the people who were previously selected to be involved in the process, and make changes, if any.
2. Identify the focus of the risk and uncertainty management – i.e., the organization, a division, a location, a project, a product, a category or type of risk, etc.
3. Identify the goals, strategies, objectives, initiatives or missions, etc. for #2.
4. Identify and know the relevant risk and uncertainty management laws, statutes, regulation, rules and guidelines that apply to your industry, organization, people, activities/actions and focus of the risk and uncertainty management.
5. Identify the potential risks and uncertainties for ## 2 and 3.
6. Identify the events, actions and root causes, etc. that could cause the #5 potential risks and uncertainties to occur, including possible multiple or interrelated events, actions and root causes, etc.

7. Identify key indicators, leading indicators, and post indicators, if any, for ##5 and 6 occurring or having already occurred.

8. Evaluate the likelihood of the #5 potential risks and uncertainties occurring. Likelihood could, for example, be evaluated as low, medium, or high – unlikely, reasonably possible, or probable or likely – or by percentages – or evaluated by pre-leading indicators or events, or post-leading indicators or events – or by other means, criteria or measures.

9. Evaluate the speed or velocity that the risks or uncertainties might occur or begin to occur or accelerate after initial occurrence.

10. Identify, describe and evaluate the potential impact and harms, etc., and potential ranges of impact or harms if the #5 potential risks or uncertainties occur. Impacts or harms might be safety/physical, financial/economic, reputation, product or service related, or otherwise.

11. Identify and evaluate the possible steps or processes available to prevent, control or manage the possible occurrence of the #5 potential risks or uncertainties.

12. Identify and evaluate possible steps and processes available to help control, manage, mitigate, and respond to the occurrence of the #5 potential risks or uncertainties.

13. Identify and describe the steps and processes adopted and their applications to address the specific #5 potential risks or uncertainties taking into consideration the additional information that you obtained in ##6-12 above.

14. Identify the people and departments, etc., who are responsible for the implementation of the steps and processes adopted.

15. Determine the timing for the implementation.

16. Develop and establish processes to detect and determine whether a risk or uncertainty has already occurred or is occurring and conduct an evaluation to identify already existing or occurring risks and uncertainties.

17. Develop and establish respond, mitigate and recover processes for risk and uncertainty occurrences.

18. Develop and establish reporting and evaluation processes relating to implementation status, timing, successes, issues, and problems as prudent based on the facts and circumstances, make decisions, and take appropriate additional actions.

19. Schedule and implement monitoring, potential monitoring trigger points and timing, and the people and departments responsible.

20. Exercise overall oversight, review, evaluation, and possible reconsideration and modification of the above, make decisions, and take appropriate additional actions.

* * * * *