

NotesOn: Risk Management-Risk Analysis

Introduction (v1.2):

This post reviews and discusses the processes of Risk Management and in particular Risk Analysis in some detail. Both were discussed in recent posts but at a summary level. In *NotesOn: The Four Fundamentals Life Cycles of IT*, I presented and discussed the newly recognized Risk Management Life Cycle and tied it neatly into the other three primary Life Cycles of IT. In *NotesOn: An IT Executive's Survey And Checklist – Part IV*, I presented an overview of Risk Analysis and “starter” Risk Lists. What I did not have space for in either of these was a “nuts and bolts” review of the key RM processes.

Table Of Contents

Introduction (V1.2):	1
Risk Defined:	1
Risk Management (RM) – Purpose Of:	2
The Risk Management Life Cycle (RMLC) Review:	3
Risk Unknown:	3
Risk Identified & Risk Analyzed – The Process:	6
Risk Analysis – Exercise:	10
Risk Management Metrics:	10

Risk Defined:

It was Socrates I believe who insisted that one define one's terms before having a discussion, or debate, on a given subject. I did not do so in the earlier posts on this subject, and should have, so, allow me to provide a fundamental (mechanical) definition of “risk”:

Risk: A risk is composed of a “vulnerability” *and* a “threat”, i.e. a vulnerability-threat pair. If there is no vulnerability or no threat there is no risk, but “no risk” is not the same as “no known risk”.

To put it another way, if, after due diligence, after doing your homework, after thinking “outside the box”, you are honestly unable to match a potential vulnerability to at least one potential threat there may be no risk.

However.

At the moment, I cannot think of a single vulnerability that does not have at least one associated threat. The odds of the pair intersecting in the real world may be somewhere between “slim and none” but, “likelihood of occurrence” is *not* a factor in the fundamental definition of ‘risk’. That element belongs to risk analysis.

The above definition takes the subject of “risk” out of the realm of vague, hard to pin down concepts that include words such as “results” and “events” and “cause” and “effect”, etc. and gives it a concrete structure that one can do something with. Clearly and concisely defining it allowed me to recognize the existence of the Risk Management Life Cycle (RMLC) for the first time and how it fit into the other three primary Life Cycles.

Risk Management (RM) – Purpose Of:

Once I had the RMLC nailed down, the purpose of Risk Management came into very sharp focus:

The Purpose of Risk Management: is to identify, analyze, manage, and monitor unknown and known vulnerability-threat pairs and retire them as soon as legitimately possible.

If we all had the choice, we would do away with Risk Management completely. No one I know of likes to spend time digging through the “negative” side of Life. Dwelling on what “could” happen, what “might” occur. Nor does anyone I am aware of enjoy determining whether such threats are due to evil, malicious, intent or merely random happenstance; a factor in helping to gauge the relative degree of risk of a particular threat.

The fact is that, on the surface, Risk Management is neither particularly fun nor terribly rewarding.

After all, if the Risk Management team does its job well, little to nothing (negative) happens. And, it is nearly impossible to accurately measure what *didn't* happen. Since there is no “proof” there is often little political incentive to acknowledge, let alone reward, the Risk Management team. The reverse is not true, however. In the event a theoretical threat has a real impact the RM team is the first group to take the hit politically.

On the surface, Risk Management is a “darned if you do darned if you don't” proposition. On the surface. This is the apparent “Curse Of Risk Management”.

For those of you who have been around IT for a while, you might recall the Y2K (Year 2000) hullabaloo in which corporations around the world spent billions upon billions of dollars to prevent something which, as far as the public was concerned, didn't happen and was “no big deal”.

Of course nothing could be further from the truth. If the work had not been done, if application after applications had not been reprogrammed and hardware device after hardware device had not had its chipsets modified, followed by system wide testing and certification as Y2K ready, a great deal *would have* happened. Society as we know it wouldn't have been brought to its knees, as some folks cataclysmically predicted, but the true cost of failure to the world economy had we not done Y2K would have been staggering.

To be intentionally redundant: as you invest in Risk Management keep in mind that it is difficult to measure and monitor what *didn't* happen. There is a reasonable solution though, one we will get more into a bit later on in this article.

So, what is the purpose of Risk Management?



The Risk Management Life Cycle (RMLC) Review:

As a brief refresher, or if you have not yet seen and read *NotesOn: The Four Fundamental Life Cycles of IT* (and if not I invite you to do so), one of the key Life Cycles for IT is the RMLC (as a side note: it applies to other business entities and trades not just IT). The RMLC is composed of the following six major phases:

- Risk Unknown
- Risk Identified
- Risk Analyzed
- Risk Managed
- Risk Monitored
- Risk Retired

My focus for this post is specifically on: “Risk Unknown”, “Risk Identified” and “Risk Analyzed” as these are the “building blocks” for the other three phases.

Risk Unknown:

The first action of the Risk Management team is to recognize that its group, company or other social entity has vulnerabilities. And that there are both known *and* unknown threats that can attack every one of those vulnerabilities. The RM team must never assume anything, they must never operate “inside a box”, they must never become complacent and assume that their “lists are complete”, i.e. all vulnerabilities and threats are known and identified. This is WHY Phase 1 of the RMLC is “Risk Unknown”. For, without Risk Management the “Law Of Unintended Consequences” (http://en.wikipedia.org/wiki/Unintended_consequence) comes into play and is its own proof that RM isn’t being done. ... Macro examples to help clarify why may be in order:

Note: though the purpose of www.fromtheranks.com is not the discussion of politics, the site’s Rules Of The Road permit it where the political arena presents a relevant example of, in this case, how not to exercise the RMLC.

During the nearly worldwide Great Depression of the 1930’s, U.S. President Franklin Roosevelt created the “New Deal”, a plan to put people to work on infrastructure projects paid for with government spending (and debt). It is arguable that were it not for WWII the program might have failed in the long run (governments of any form are incapable of supporting, let alone building, a long term stable economy), but the good news was it helped keep people alive during a severe crisis and those people did construct dams, power grids, highways, water ways, harbors, buildings and so forth; the foundations of a common, nationwide infrastructure.



However. That the New Deal worked at all was almost a fluke; one could call it a brilliant accident of right place, right time, questionable idea; a not likely ever to be repeated collision of events and decisions the success of which was, on the whole, based solely on two crucial fundamentals – ones that may not have been recognized as such:

1. the New Deal programs built critical infrastructure very much needed by the *entire* country; facilities that allowed for future national growth and industrial and technological expansion (just in time for WWII),
2. and, no less important: “The People” as a *whole* ... *worked* ... to achieve it. At a personal level, if they didn’t work they didn’t get paid. If they didn’t get paid they didn’t eat, except in soup lines. But. It was a program embraced by The Country as a whole body. Rather than a few selected individuals.

However, again. For all the good the New Deal did, there was at least one unintended consequence: the discovery by the federal government that a government could apparently *buy* its way out of an economic situation with debt.

Unfortunately, the two key factors of FDR’s nominally successful formula, which should have been included in and seriously tempered the above discovery, either went unrecognized or were ignored. Either way they have been omitted from virtually every single subsequent government “hand out” program since.

Particularly from the 1960’s on (President Lyndon Johnson’s “War On Poverty”), an endless number of “Welfare” schemes (some might say ‘cons’) have been tried, minus those two success factors. Sadly, year after year the (presumably) unintended consequence of such “solutions” has been a rising dependency, by ever larger segments of the population, on government “aid”. FDR’s “helping hand *up*” has become a virtually guaranteed “Right” that few politicians wish to touch, for fear of losing elections, despite the fact that any first year Economics student can easily predict that handing out something for nothing is unsustainable.

(Note: Off-shoring, save for true expansion purposes, also violates those two key factors, for shipping jobs overseas to “cut costs” ultimately denies the entire country the opportunity to strive towards and eventually reach the level of innovation and excellence necessary for the internal resolution of internal problems.)

Another example of unintended consequences comes to us from the U.S. Forest Service. Historically forests, hills and flatlands alike were “maintained naturally” by the occasional occurrence of fires. Yes, they threw some smoke in the air but they also reduced or eliminated over-grown brush, destroyed diseased plants and trees, helped fertilize new growth and so forth – in some cases fire is the only way certain species can propagate. But. Beginning in the 1970’s, environmentalists stopped nearly everyone from burning nearly anything in nearly every forest, parkland and open range they could manage.

While “saving the environment” in such a manner seemed logical, to some, the unintended consequences of such policies have resulted in decade after decade of massive atmosphere and water polluting Super Fires that destroyed, and continue to destroy, untold billions of dollars of property, millions of acres of once natural landscape with their fragile ecosystems while also taking heavy toll in both human and animal life. Not too

long ago the Forest Service in Yosemite National Park, as one example, finally told the environmentalists to go pound sand (presumably politely) and went back to controlled burns that mimic the earlier *natural* processes.

In another arena, that Federal and State governments seem to have close to zero control over their budgets is an absolute giveaway that, in addition to no political will, our politicians are not doing RM.

When a friend and I were chatting about this subject he suggested that governments need to put in audit controls on spending. While that is true, audits are typically *re-active*, they analyze what has happened. Risk Management is *pro-active*. It helps identify and prevent problems *before* they occur.

Here's another for instance. Setting aside the question of whether or not such a Bill is actually needed, the various versions of the 2009 "Health Care" legislation in the U.S. House and Senate are going to be (unless killed or completely re-written) prime future text book cases of an absence of Risk Management. As written, it *will* result in a laundry list of unintended consequences. How do I know RM has not been done? Because, from everything I have read, heard and learned few if any of our hundreds of representatives in either House have studied the Bill cover to cover. I asked Congressmen and Senators in *two* states if they had read (let alone understood) *all* 2000 +/- pages of their respective bills and not one of them answered the question. Not one. What I received back were "form e-letters" that said nothing and committed them to nothing.

You cannot do RM if you don't know what questions need to be asked or what areas to look into. And, again, if you don't do RM, unless very lucky, the "Law Of Unintended Consequences" will, not may but will kick in.

One more example and then we'll move on. Not too long ago a fairly large company decided to out-source their infrastructure and data center operations; all of their infrastructure and data center operations, including system administrators, database administrators, security administrators, network administrators, ... the works. In theory this was going to cut costs. The reality was, it did anything but:

Costs rose, significantly, because the third party vendor "low balled" their bids to get the contract -- which the executives were warned about by their IT group but chose to ignore -- and the vendor felt compelled to charge and overcharge for everything not absolutely perfectly nailed down in the contract. But that was just the beginning.

User dissatisfaction skyrocketed as the vendor ran into countless implementation delays, due to issues they claimed they "hadn't known about" despite the fact that the IT group fed them every piece of information the vendor asked for and then some. Nor were the users the least bit happy as and after the vendor cut support personnel to save money.

Then, in an effort to stop their continuous financial bleeding, the vendor replaced virtually all of the promised "first string" (most adept and skilled) technical personnel with "wet behind the ears" junior grade people. The service level plummeted, further, the SLA's were violated, further, and, as a direct consequence, the IT group's customers began hiring their own IT people and buying their own hardware, etc., to satisfy their customers.

Despite huge financial losses (tens upon tens of millions) and a tremendous amount of negative feedback from everyone, when last I checked with my contacts both the company's and the vendor's executives were

charging ahead with a “new” master plan. They decided the answer to all their problems was to off-shore as many of their combined IT functions as they possibly could, without *completely* destroying the company’s IT functionality. All in the name of chasing “cost savings” that they have not and never will see.

That it hasn’t and won’t work continues to escape them –in the first place it was done for the wrong reasons and in the second the vendor lied to one and all to get the contract. That the executives are piling on even more risk has apparently also escaped their notice. If they *are* doing RM, that data is being ignored as well.

In Summary:

The above examples were given not to point fingers but as real life examples of how RM applies not only to the world outside IT, but to IT, at all levels, very much including “day-to-day” IT plans and projects:

1. You need to do RM to avoid, as much as humanly possible, creating and executing plans and projects with costly holes in them, and to avoid as many unintended consequences as possible.
2. RM is not perfect: a missed risk can be something no one ever thought of (maybe it was too far outside any box to be “reasonable” or perhaps the odds of it happening were considered to be “astronomical”); just don’t let it be missed simply because no one thought.
3. Before you can successfully do RM you have to acknowledge that both vulnerabilities and threats can and do exist, internally as well as externally, and then you have to go look for them.
4. Once you start looking you *will* find them and once found you have to think, and analyze, and anticipate possible consequences.

The above list is *why* “Risk Unknown” is the first phase of the RMLC. Failure to acknowledge the fact that vulnerabilities and threats are out there, including ones that may be initially unknown, will leave you with an incomplete Risk Analysis, and leave you vulnerable. Ignorance of or ignoring risks leads to project failure.

So, assuming you and your team acknowledge that there may *be* something, at least slightly unpleasant, to discover, your next question is probably: “What does one *do* in the *Risk Identified* and *Risk Analyzed* phases?”

Risk Identified & Risk Analyzed – The Process:

After all of that buildup, what follows may seem overly simplistic. If you were looking for something terribly erudite (terribly scholarly thus often complex and confusing) you may suffer a bit of an emotional letdown. However. Don’t let the simplicity of the following process fool you , when done and done thoroughly it is a powerful tool in your Risk Management arsenal ... *if* ... you don’t overcomplicate it. With that in mind, here is the combined Risk Identification and Risk Analysis process in outline form:

#1 -- Identify Vulnerabilities and Potential Vulnerabilities

- Identify actual and potential internal and external vulnerabilities (**definition:** areas inadequately protected and susceptible to harm; leverage points that leave one open to attack); list them
 - If desired, and it makes sense, group related vulnerabilities and potential vulnerabilities under a common heading but do not “summarize” the grouped vulnerabilities
- Assign a “best guess” **Vulnerability Value** to each one (ex: 5 of 1-10)
 - Not all vulnerabilities are identical, some are “riskier” than others
 - Be willing to adjust these values as you learn more
- Review the complete Vulnerability List and associated values, obtain agreement

#2 -- Identify Threats and Potential Threats

- Identify actual and potential internal and external threat sources, do not limit them to what you think might match up to an existing vulnerability, better too many than too few; list them
 - If desired, and it makes sense, group related threats and potential threats under a common heading but do not “summarize” the threats
- Assign a “best guess” **Threat Value** to each one (ex: 6 of 1-10)
 - Not all threats are identical, some are “riskier” than others
 - Be willing to adjust these values as you learn more
- Review the complete Threat List and associated values, obtain agreement

#3 -- Identify Vulnerability-Threat Pairs

- Do a “best guess” determination of which threats can potentially impact each individual vulnerability
- Create Vulnerability-Threat pairs (a vulnerability can have more than one threat and vice versa) (ex: firewall-hacker)
- List them as you go (typically on a spreadsheet), do not delete them even if they seem inconsequential

#4 -- Identify Vulnerability-*Unknown* Threat Pairs

- If you have a known vulnerability but no matching threat you have a *potential risk*
- These should be few and far between and typically are only temporary, i.e. the analysis is a “work in progress”; all vulnerabilities have threats but sometimes it takes time to identify the exact threat(s)
- Create a Vulnerability-Unknown Threat Pair, do not leave them off the list

#5 -- Determine Likelihood of Occurrence of each Vulnerability-Threat pair

- Do the math (**Likelihood of Occurrence Value** = Vulnerability Value x Threat Value) (ex: 5 x 6 = 30)
 - This step is not addressing impact, it is a best guess “odds of happening” calculation
- Vulnerability-*Unknown* Threat Pairs have a low Likelihood of Occurrence Value of course but they *must* stay on the list for future re-evaluation

#6 -- Estimate Potential Impact of Vulnerability-Threat Pairs

- Create a Risk Profile of each Vulnerability-Threat value
 - Document the potential negative impacts of each Vulnerability-Threat pair; this should be a concise narrative but don't “pretty it up” to be politically “sensitive”, tell it like it is
 - Include: time, cost, legal, public relations, etc. impact factors in the profile
- Assign “best guess” **Impact Value** to each Vulnerability-Threat pair (ex: 9 of 1-10)
 - Some pairs have the potential of creating a cascading event, i.e. one event triggers another that triggers another that ... consider and describe these in the narrative and reflect this potential in the Impact Value
- Do the math (**Risk Value** = Likelihood Value x Impact Value) (ex: 30 x 9 = 270)
- Based on Risk Value assign each Vulnerability-Threat pair to a Risk Tier (1, 2, 3, etc.)
 - Order your list by Risk Value
 - Determine an arbitrary Risk Value ‘cut-off’ point for each Tier

#7 -- Present the Risk Analysis and supporting data to management and executive levels, obtain buy-in

- For a graphical representation, generate a “Heat Map” of at least the “Tier 1” Vulnerability-Threat pairs (Y axis = Likelihood Value, X axis = Impact Value), but do not “ignore” Tier 2 and Tier 3's
 - A common way to generate a heat map is to use Excel and some code that colors the cells based on the X-Y value in the cell. Here are a few examples:
 - <http://sparklines-excel.blogspot.com/> & <http://sourceforge.net/projects/sparklinesforxl/files/>
 - <http://www.vni.com/products/imsl/cSharp/v501/chartpg/heatmap.html>
 - <http://www.mbeckler.org/heatMap/>
 - Some dashboard software packages have utilities that will generate one or more heat map report styles for you

- You can find applets and plugins on the web but they require a knowledge of Java, .NET, etc.
- In lieu of (or in addition to) a heat map, your original master spreadsheet of prioritized vulnerability-threat pairs can work equally well
 - include the pair name, a brief description, all of the above assigned and calculated values and the assigned Tier value.
 - Risk Value would be your primary sort order, but in this format you can re-sort as desired during your presentations.
- Add a proposed resolution approach for each Vulnerability-Threat pair to the master list
 - The resolution options are (see “NotesOn: The Four Fundamental Life Cycles Of IT” for details on these four):
 - Mitigate it, or
 - Avoid it, or
 - Transfer it, or
 - Accept it
 - Draft a matching action plan for the assigned resolution option
 - The first steps of each Vulnerability-Threat pair plan should include what can be done now, what can be accomplished now. Don’t wait for the perfect solution, or for ideal funding. Any action is better than no action. You can’t improve on what you haven’t started.
- Prepare a RACI chart (Responsible, Accountable, Consulted, Informed) of all stakeholders
- Present the Risk Analysis at a “summit conference” of all stakeholders, the goal of which is to obtain buy-in, executive sponsorship of, and funding for your Risk Management action plans
 - The summit conference will be an “iterative” discussion in which some of the above value calculations may change as new data comes to light. That is okay. The end goal is a master Risk Management plan that is workable and that the company/group can support and afford.
 - Tier 1 Vulnerability-Threat pairs are the first target but don’t forget/ignore the other Tiers.
- Review the subsequent Risk Analysis and Risk Management plan with all stakeholders regularly.

Note: Any SOX, PII, PCI, HIPAA, Safe Harbor and COBIT controls in effect, and the “NotesOn: An IT Executive’s Survey And Checklist – Part IV “ provide a starting point for your Risk Analysis, but only a starting point.

Risk Analysis – Exercise:

As an exercise, do a Risk Analysis using the above process on “buying a used car”. I’ll give you a couple of hints as to areas to look in for vulnerabilities and threats, in case you’ve never bought one before, but don’t limit yourself to these:

- Your available cash and/or credit
- The reputation of the seller/dealer
- The ownership of the car
- The history of the vehicle (actual versus anecdotal)
- The mechanical condition of the car
- The electrical condition of the car
- The safety features of the car
- The aesthetic qualities (i.e. appearance) of the car

List out the potential vulnerabilities, everyone you can think of, then the potential threats, match them up, assign values, do the math and, finally, prepare your Risk Analysis report.

Risk Management Metrics:

Last, but not least, is the subject of metrics. It may seem off point, but it is not. In order to do Risk Management, you not only need “buy in” from the entire organization you need a way of demonstrating the ongoing value of your work. One way, a key way, to do so is to develop a set of metrics. Unfortunately, due to the nature of the job, the only realistic way to apply metrics to the RM team is indirectly.

Rarely can you as a manager or executive say: “Hey everyone, look what my RM team did. We stopped _____ from coming through the fire-wall and attacking the XYZ application’s failover database cluster in our disaster recovery server farm in _____.” You can, and probably should, subscribe to statistics from your virus and spyware protection software but, even if you do, that is only a small fraction of what RM is about; besides those numbers can be somewhat subjective.

So, the question is, what to measure. Here’s a hint, a starting point:

The cardinal rule of metrics is: “You get what you measure”.

I don’t recall where I first read that quote (it is now all over the Web), but I instantly burned it into my memory for the simple reason that it made perfect sense. For instance, if you implement a help desk metric of

“number of trouble tickets closed”, the number of tickets closed per hour / day / week / month will soar ... most likely without reference to quality or satisfied customers (not a joke, I have seen this first hand).

So, what can you measure in RM that is truly meaningful? That will get you what you want? How about creating a metrics pair, measurements that help forward the purpose of Risk Management, such as:

1. The RM team gets credit for the success of any area of the business it touches
2. The RM team gets credit or dinged for the Percentage of Items on the Risk Analysis (master risk list) that both did and did NOT cause a significant problem for the company.

As to #1, if the statistics of that area of the business rise, then it is assumed that the RM team, in doing their job, had a hand in the risk reduction and thus the improvement. The reverse would also be true. A down-tick or down trend would / should trigger the RM team to take a closer look at the area to see if one or more vulnerability-threat pairs were missed or improperly managed.

As an example of #2: if we assume your master risk list has (to pick a number out of the air) 500 items on it and, further, that the sum of the Risk Value of all vulnerability-threat pairs on the list is 22,500, and if there are only two vulnerability-threat pairs that had a negative impact for the metric period (week, month, quarter, year) and their combined Risk Value was 476, then the weighted success percentage would be 97.88%. Weighting it so gives you a more accurate picture of the negative impact [versus: $(500-2)/500 = 99.6\%$].

Now, you might be thinking to yourself that your RM team will “pad” the heck out of the list, i.e. make it as long as possible to increase their odds of having a high success percentage.

My response is: “Fine. Let them make their master list of vulnerability-threat pairs as long as they want ... providing each pair is at least within the realm of possibility. ... Because, the metric is actually the *trend* of the success percentage over periods of time (weekly, monthly, quarterly, yearly).”

You do not want them limiting the size of that master list. No. No. No. No. Just make sure they’ve assigned rational values and have a proper strategic response: Mitigate, Avoid, Transfer, Accept.

But what if a vulnerability-threat pair that was *not* on the list has a significant impact on the company?

My response is: “If something significant was missed the entire Risk List and Risk Analysis process needs to be reviewed and a significant penalty would need to be assigned to adjust the metric for the missing threat pair. What that penalty would be is up to you.”

In the end (after training, coaching, mentoring and managing), you should have a top-flight RM team that is geared exclusively towards, focused solely on: (1) the success of the company, and (2) the demonstrable management of all reasonable and possible to predict known and potential risks.

Hope this helps.

DP Harshman

PDF Link

