

NotesOn: Risk Management - Risk Analysis Process Addendum

One of the items I failed to mention in the original post on Risk Management (NotesOn: Risk Management – Risk Analysis) is that Risk Analysis (RA) must be done from the top down *and* from the ground up.

“Top down” supplies the high level executive view of the risks inherent in a particular operation. This is the long term strategic and high level tactical plans stratum. This view does not, however, typically encompass the detail level and it would be remiss, it would leave a serious gap in the RM plan(s), if one did not take them into account, too.

“Bottom up” feeds the “nuts and bolts” risks into the process, risks that the executive level may not be, probably are not, aware of. Unless one is working “in the trenches” (or at least has worked in them extensively) there are, not may be, but are risks that just will not be seen; the large pot-holes, the stumbling blocks, the unseen trip wires that can quickly cause major delays and add unexpected costs. Risks at the project level, support level, infrastructure level, etc., risks at the departmental level can be every bit as much of a threat (and in some cases more so) as those observed and listed in senior management’s risk reviews.

So. While the IT execs develop their risks list, the “techies” – the Managers, PMs, Tech Leads and technical team members – must do theirs.

Once completed, both lists should be merged and prioritized; with nothing dropped off due to “insignificance” or “lack of budget”. It doesn’t matter from where a risk comes or who recognized it, each Vulnerability-Threat pair must be identified, analyzed, managed (including prioritization), monitored and, eventually (hopefully), retired.

By taking a top down and a bottom up approach you significantly limit the potential for missing the risk(s) that could “do you in” when least you expect it. What you don’t know *can* hurt you, what you fail to plan for can “get you”.

One more note on Risk Management, for now.

Do not let RM/RA intimidate you, do not permit a lack of understanding of RM/RA to limit your reach for success, to restrict your drive to expand and grow. That is not its purpose. RM, RA and the Risk Management Life Cycle are there to help you avoid the pitfalls that are out there, and they are out there. RM, RA and the Risk Management Life Cycle are there to help you attain your goals and objectives by eliminating (ideally) or reducing the number of unseen walls that you might otherwise run into and the quantity of camouflaged holes into which you might otherwise fall.

Late at night while laying in bed staring at the ceiling, the wish to ignore the subject altogether may creep up on you. After all, doing so would seem to make one’s life “easier”, less complicated. Perhaps at one time or another you may even have “gotten away with it”, i.e. you may have successfully managed an area or a product or a project without doing any RM/RA at any level at all. If so, you were lucky. But. Luck is not a thing to depend on as a risk ignored is an unexposed problem waiting to happen.



Nothing worth doing, building or possessing was ever obtained without successfully *dealing with* risks. Nothing. And keep in mind that there are risks before, during and after the doing and obtaining. Thus, RM/RA (which has to be applied sensibly and appropriately to the occasion) is a subject not to shy away from but, rather, to invest in. Increasing your familiarity with Risk Management's fundamentals, and then applying them, increases your chances for success.

Besides, if there were no risks at all in an endeavor ... it wouldn't be much fun.

Hope this helps,

DP Harshman

