# All.Net Analyst Report and Newsletter

***Welcome to our Analyst Report and Newsletter***

## Managing oops

Whenever I hear or see the word risk these days I stop and pause to see whether the word is being used in a meaningful way. I have previously identified risks and rewards as two faces of the same thing (i.e., future event sequences). We place our bets and we take our chances. Risk management (in conjunction with investment strategy) is the decision-making, influence, and observation process that seeks to anticipate and constrain (i.e., control) these futures to more desired sequences (the control envelope) over a defined future (the event horizon).

Residual risks and rewards are the event sequences that we decide not to explicitly control. We differentiate two types of residual risks, the ones we anticipate and the ones we don't.[1]

> The residual risks we do not anticipate should be few and far between, but unfortunately, the lack of adequately knowledgable risk and investment managers and the lack of strong supporting tools or their use often result in many anticipatable but not anticipated risks.
>
> The other residual risks are the ones we anticipate and choose not to constrain. Generally, we are asked to keep these below some threshold of acceptable risk. Note that there are indeed cases where rewards are limited (e.g., to keep a portion of a business below a regulatory threshold).

The risks we do not anticipate are managed by trying to be better at anticipating significant future event sequences. This is done by hard work and constant study.

The risks we anticipate and choose not to constrain are a far bigger challenge, because we hope to create and apply a decision-making process, and this decision-making process is one that, by its nature, is competitive. In essence, those who achieve better outcomes over time (which we define retrospectively as “better” decisions) do better in the competition. While we may have different objectives, each of us, in evaluating our own performance over time, look back and evaluate the outcomes. So the risk management process is, in some sense, seeking to predict the future better than our competitors.

## The one word you don't want to hear from your surgeon during your operation

There is an old joke about a surgeon operating on a patient who can hear the process as it is underway and hears the surgeon say “Oops”. I don't remember the rest of the joke, but I remember the “Oops”. Here's the thing. We compete over our ability to predict the future. We do it every time we walk across the street at a cross walk, imagining that we are safe from a driver who decides to hit the gas when we are in front of them. We predict that they will not and usually win. In risk management, we compete over our ability to make good decisions about the plan, and that means predicting the future better than the competition.

From an operational standpoint, we make our bets and we take our chances. But what happens when we aren't making the bets we thought we were making? Oops!

1 We will drop the need to always identify the duality of risk and reward from here forward and use risk to combine the notions except where they need to be explicitly differentiated.

 

### What to do about oops

"I've been thinking lately. Thinking about the good things to come."[2] This all ties back to the Plan, Do, Check, Act process of ISO 27001 and 27002. It is so basic and fundamental that we often seem to forget it. No plan survives contact with the enemy.[3] In risk management, there is all of this time and effort exploring ways of making better decisions, using statistics, assessing various things down to some number of digits of accuracy (I don't generally advocate that), and so forth. But perhaps the largest source of uncertainty in the risk management process, at least as far as operational risk is concerned, is in the execution of the plan, not in its conception. "We all work at our jobs. Collect our pay. We think we're gliding down the highway when in fact we're slip sliding away."[4]

In thinking about oops[5], I have come to conclude, that we're missing the boat, when we over-plan and under-execute. Somehow, the risk management function helps to specify what is to be done and should also use the audit function or a similar feedback mechanism to make sure it is being done. If and to the extent the things that should be done are not being done, it is the job of risk management to manage. And that doesn't always mean forcing compliance. It means changing the plan to adapt to the enemy. The enemy being the unanticipated and/or unconstrained future. We control by knowing what to anticipate and how to constrain it.

### Adaptation and response

Just calculating values of expected loss against acceptable thresholds and notioning about reductions associated with controls doesn't get it done. The effectiveness of controls involves synergistic elements that are not calculable by available methods today. Changes in training, social conditions, and ergonomics appear to effect password selection and usage. Changes in password policies appear to produce changes in group cohesion and compliance in other areas. What are the directions and magnitudes of these effects? We don't have the science to answer these questions definitively yet. And yet we live with the effects even if we are unaware of the causes or uncertain about the mechanisms. Human behavior is largely ignored in much of the analysis process, and yet human behavior may be the biggest factor of all in determining outcomes of many risk management decisions.

Risk management decision-making is also complicated by the differences between response and adaptation. Response is typically a tactical action taken as a result of a situation. This should rarely, if ever, be a "risk management decision". Tactical (common situation-based) responses should be largely programmed decisions, where risk management process defines classes of situations and desired responses, and tactical execution is up to operators.

Near the edges between different alternative tactical actions, there should be little difference in outcomes for differences in actions. In other words, sensitivity analysis surrounding tactical decision-making should show that if the decision to take action A over action B flips at a point "x", then the difference between ultimate outcomes from A and B near x should be small. The term "near" in this context implies that the ability to discern x is unclear in the time frame of

2 The last two sentences are quotes from a Cat Stevens song.

3 Per http://www.ralphkeyes.com/quote-verifier/, Helmuth Von Moltke said: "No operation extends with any certainty beyond the first encounter with the main body of the enemy." It has been paraphrased since.

4 Paul Simon – "Slip Sliding Away"

5 I wish I had a clever acronym here – Operational Oversight Planning Syndrome – the condition in which we make brilliant detailed operational plans but miss something critically important – their proper execution.

 

the decision. Thus once we determine the bounds on accuracy and precision of our ability to determine the relevant factors in the tactical decision, anything within the bounds of uncertainty should produce roughly equivalent outcomes regardless of whether we do A or B. As information leads us further from x, clarity around A or B should be more readily apparent and the differences in outcomes may reasonably start to vary more significantly.

It is the job of risk management, at the architectural level, to make decisions, characterize tactics, and define information needs such that tactical decisions can be programmed with the desired properties. Risk management should also verify that these regimens are in effect and adapt the architecture, hopefully slowly, over time to assure that things that work are properly applied and things that don't are changed.

Risk management should really focus on the architecture of tactical decision-making, and as such, should be strategic in nature.

**How does this work in practice?**

The practical area I am most familiar with is information-related risk management. Information and related technology require investment and such investment has tremendous rewards. If we don't take risks in this area we will certainly not make progress and will fall behind our competition. And yet there are many unknowns. A simple example is in the area of social media and its use in influencing business progress. In what ways should we participate in social media and how should we reasonably control that participation? At the simple decision-making level, there is the question of whether or not to participate in any given social media marketplace. Should we invest in Twitter? That tactical decision varies for different businesses, but suppose we have decided to participate at a minimal level by having an ability to respond in that media, but not actively using it to move our business forward. It is a defensive approach to Twitter. The reason for defense is potential damage to reputation, but the reason for offense, in the sense of more active participation, may be enhancement of reputation, market presence, and a channel to inform clients and potential clients about business opportunities. So suppose we decide that LinkedIn is a place to be for our business.

As we work our way through the decisions about Twitter, LinkedIn, Facebook, Yammer, and so forth, we will, hopefully, develop a strategy for participation. The strategy might have several factors, like presence of client base, total number of participants, ease of use, ability to stop abuse, operation on platforms we use, and so forth. And to the extent that there is a small difference between Yammer and Facebook for our factors, the decision to chose how to participate in one or the other likely has a small effect on outcomes, especially given that, if properly managed, changing decisions can be done at relatively low cost early on. As this strategy unfolds and adapts over time, the rewards and risks start to become more obvious, and likely far larger.

Now let's look at some of the bases for decision-making. Suppose we have and continue to study these media, and determine that, operationally, other companies have had insiders leak sensitive information on Twitter, disgruntled insiders make claims that damage their reputation on Facebook, and outsiders challenge attempts to drive opinion on LinkedIn. We have lost our Yammer feed for days, had accounts taken over on Google, etc. These feed our risk understanding, and we should be tracking this and learning from it. The lessons should be generalized, so we should assume that insiders on Yammer might leak sensitive information, and more generally, that any class of incident might happen in any forum.

 

We should also seek to understand the limits of prevention and tactical response to these sorts of incidents in these various fora. For example, we might use a review process to make more certain that our authorized presence in these for a does not leak sensitive information, but this then also means that we cannot respond as quickly as we might with less control. We might use a training process as well, for those authorized to speak for us. If flash mobs are a concern, then we may need a detection methodology to allow us to find out about such mobs before they fully form, regardless of the social media they use, and create a response regimen that rapidly acts to diffuse such flash mobs before they form by some sort of social influence strategy. Or we might go for a different strategy based on broader-scale reputation so that people are unlikely to believe that we are worth flash mobbing. Or we might have a strategy that prepositions party supplies and outsources a festival company so that as flash mobs form, we create local parties that promote our products and services, turning the flash mob into a positive. We might even start our own flash mobs for preplanned sales events.

Operationally, each of these strategies involves specific actions, and as our programs develop and mature, we get finer and finer grained decision-making about them as their risk and reward values increase. From an enterprise level, the tactics of how to counter the negative potential effects of flash mobs using twitter going against our offices in some location are not individually important from a strategic perspective, and don't justify significant risk management effort. The paralysis of analysis and excessive planning approach are not likely to be effective. Rather, the job of risk management is to define the architecture and use feedback and feedforward (what has happened and can be anticipated from external events and sources) to adapt that architecture over time. Our social media strategy example includes the risks and rewards and the means to turn negatives into positives, and supports good decision-making at a local level. It adapts over time and adopts good and new ideas to the extent that the foreseen outcomes can be reasonably anticipated and constrained.

**Summary and conclusions**

The desire to constrain the future by crushing change and forcing compliance is problematic for risk management in that it stifles innovation, the very stuff that produces reward. The tendency to overanalyze and under-adapt is also problematic in that it increases costs while failing to track risks. Some combination of strategy and tactics must change rapidly in a rapidly changing environment, and to do this, the process by which risk is managed must also change. But change does not imply a lurching from emergency to emergency.

Managing risk in these conditions is largely about gaining understanding of the nature of the changing environment, anticipating the futures that may emerge, choosing what to constrain, how to constrain it, and how closely to constrain it, and learning how to do better over time. It is not and is not likely to be an art that becomes perfected. Rather, it is a life of constant adaptation to the new and different futures that emerge in the world. It means constantly learning and thinking about the future from the past.

Managing oops is about understanding the range of futures and recognizing that just because you know that something can happen doesn't mean you can or should do anything about it. By eliminating residual risks we do not anticipate, we create a potential problem in terms of the law of liability, in that we become responsible for our decisions about it. But willful ignorance is not bliss. Rather, it guarantees a lack of diligence and prudence. Managing oops means making better decisions without over-thinking them.

 