ERM-101: A PRIMER

SETTING THE CONTEXT: UNCERTAINTY

Imagine you had a magic wand and your wish of going back to the summer of 2019 came true.

If I had told you then that we are going to be faced with a global pandemic in just a few months – something that would bring the world to a brief stand-still and when we do recover, we would live in a completely new norm – what would have been your response? "There goes another conspiracy theory" would be my guess -- or something close to that! While it is debatable, whether or not the COVID-19 crisis was predictable based on intelligence available through several independent sources like the National Institute of Health (NIH). What is clear from our experience is this: as human beings in a free society, the general tendency is to underestimate the adverse impact of uncertainties from "what we don't know we don't know".

UNCERTAINTY IS A FACT OF LIFE.

There literally cannot be anything that we can be 100% sure about. From betting on the outcome of a game of cards to projecting your personal/business revenues to even day-to-day tasks like being just-in-time for a meeting – there is an inbuilt level of uncertainty in literally anything we can think of. It is one of those things from which you can try to run, but never hide. But, why try to hide from uncertainty when there is a proven way to manage it? The concept of risk management has been around from time immemorial and provides an effective framework for managing uncertainty and its impact.

DEFINITION OF RISK:

The term "risk" has been the center point of discussions on several platforms for a very long time. From Einstein's Theory of Relativity and Heisenberg's Uncertainty Principles to stochastic modelling that drives your Google Map algorithms, the concept of risk has attracted an almost infinite range of applications. The search of a consistent definition of the term "risk" will lead us to the conclusion that there are several definitions available based on the context. The one that I personally like is the definition of risk from the International Organization for Standardization's (ISO) Guide 73:2009. This internationally accepted Standard defines risk as the "effect of uncertainty on objectives." Among all definitions I have come across, this fits the KISS principle – it is simple, short and demystified! It is not the actual uncertainty that is the risk – risk is the impact of the uncertainty on what you are trying to achieve! What's interesting is that when ISO published it's *"ISO 9000:2015, Quality management systems–Fundamentals and vocabulary"*, the phrase "deviation from the expected, positive or negative" was added to describe the Guide 73 definition about "effect of uncertainty". Yes – as one can imagine, uncertainty does not always have to yield an adverse impact on our objectives; it can also contribute to the achievement of our objectives. The accelerated growth of online shopping portals like Amazon and digital business communication apps like Microsoft Teams and Zoom since the start of the COVID-19 pandemic illustrate the positive impact of uncertainty on objectives.

THE CASE FOR MANAGING RISK AT THE ENTERPRISE LEVEL:

If risk management is the business of managing the impact of an uncertainty on our objectives, the initial response we normally get goes something like this: "we do that already!" Yes – the crux of any manager or leader's job description is to predict and proactively prevent undesirable events. While this allows for a siloed approach to managing risks in one's individual function, it does not allow for consideration of risks outside the specific function. For instance, let's take two managers to illustrate this common pitfall: a Purchasing Manager and an Engineering Manager. The Purchasing Manager wants to install an Enterprise Resource Planning (ERP) system upgrade to reduce missed shipments from suppliers. The Engineering Manager, on the other hand, is keen on investing in a Digital Work Instruction module to reduce human error in manufacturing. Extrapolate this thinking to other functions of the organization – and you can only imagine the wish-list from each functional manager with the right intent to manage risks at their individual functional levels. While every manager's ask is valid, an enterprise with limited resources – financial and otherwise – has to deal with the challenge of prioritizing the most important investments in pursuit of the enterprise's objectives. During a recent presentation of this concept, a client of mine asked me in a satirical tone: "You mean, I can't go with the dude that yells the loudest?" We laughed about it, but deep within, I was just thinking that's not far from reality in a lot of organizations. Allocation of resources to prevent undesirable events without objectivity and independence can result in a range of problems – some minor, while others catastrophic. This is where the siloed approach to risk management fails and paves the road for an Enterprise Risk Management (ERM) model. The ERM model would allow for a single-view comparison of the risks presented by the Purchasing, Engineering and other individual functions. The result would be the prioritization of resource allocation required for the enterprise as a whole to pursue it's objectives.

DEMYSTIFYING ERM – THE BASIC FRAMEWORK:

Enterprise Risk Management (ERM) is an extremely common-sense driven model. When you are faced with a task of preparing for an uncertainty, what would your natural instincts drive you to do? You would first want to know what are the possible uncertain events that can come your way. The term "possible" is interesting and is deliberately chosen for this context. Naturally, you cannot possibly list all possible uncertain events – but a good faith effort towards that end will challenge you to use cross-functional teams with diverse experience about the subject matter. Once you have identified foreseeable uncertain events, you would want to somehow prioritize the list, so you can focus on the vital few risks that would otherwise stop you from meeting your objectives. This would be the equivalent of choosing the battles you want to win/lose with an eye on winning the war – the battles being the risks and the war being the enterprise's objectives.

The above common-sense driven thinking can be summarized in the following three sequential steps:

1:RISK IDENTIFICATION
Ask "What could go wrong"?

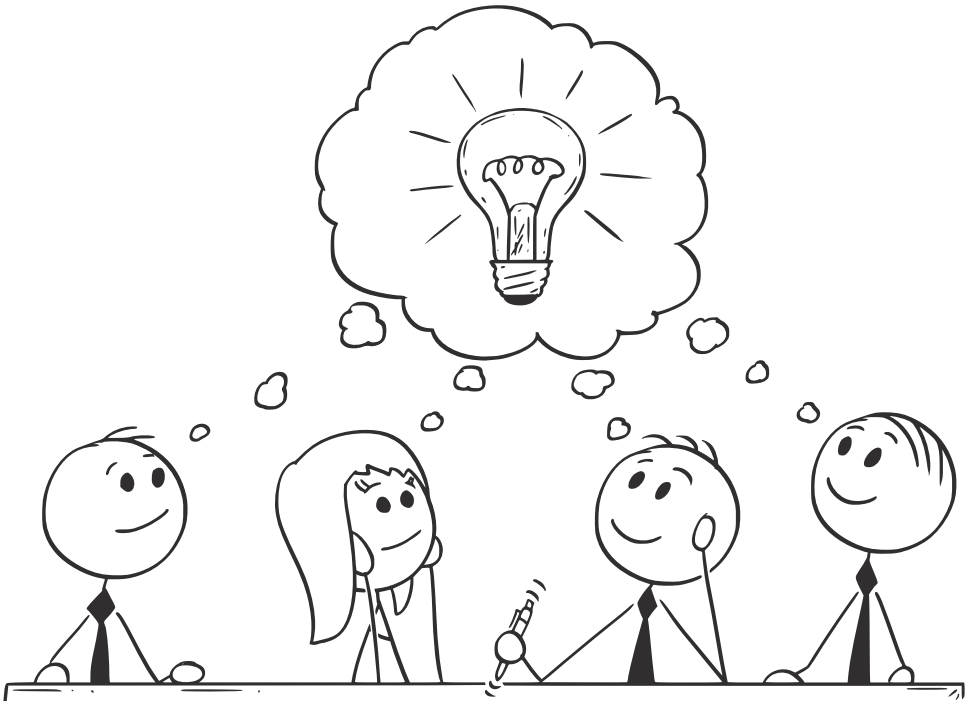
2: RISK VALIDATION
Ask "So what? If it went wrong, what's the worst-case impact? Can I accept it in pursuit of my objectives or not?

3: RISK RESPONSE
Ask "Now what? In other words, what do I do about it?"

While the scope of this article does not allow us to delve deep into the mechanics within each step, let us make an attempt to throw some light into some key aspects to be considered.

RISK IDENTIFICATION:

It is not uncommon to see organizations recognize the impact of uncertainties after an undesired event hits us (ex. a customer recall, losing a key employee to competition or a regulatory lapse). As an alternate to this reactive model, a deliberate proactive effort to scan internal and external factors that could impact a business is the key to effective risk identification. Although a wide range of tools to aid the risk identification exercise is available, an organization must carefully choose methods that align well with their business model and culture. For all that you know, your organization may already be using a few effective tools that can be repurposed for your enterprise level risk identification exercise. For instance, with some effort, several traditionally used continual improvement tools like Value Stream Mapping (VSM) and Failure Modes & Effects Analysis (FMEA) can be adapted to help identify internal risks.



Organizations that are not too complex can probably get away with even simpler tools for risk identification like brainstorming and the use of simple questionnaires & surveys. While these tools can work effectively to identify internal risks, risks that can occur due to factors outside an organization cannot be ignored. An easy way to remember some key external risks is the PESTEL acronym – Political, Economic, Social, Technological, Environmental and Legal risks. Depending on the complexity of an organization's business model, its products and technology impact, identification of external risks can be challenging. The use of SWOT analyses, competitive intelligence, benchmarking and environmental studies are some tools to consider for external risk identification.

RISK VALIDATION:

Once identified risks are consolidated in a single dashboard view, the task at hand is to assess the impact of each risk event on an organization's ability to meet objectives. The idea of risk appetite is a useful thought process in this exercise. Let us face it – unless you have infinite resources, it is not practical to try and respond to everything that can go wrong. You have got to pick your battles. In this context, ask yourself what is the maximum risk you are willing to accept in pursuit of your objectives? Once articulated, this becomes your risk appetite. The mechanics of how to articulate an organization's risk appetite is the subject for another article, however, at this point, it is safe to assume that risk-averse organizations have lower appetites for risk acceptance than their risk-hungry counterparts. Comparison of each identified risk against an organization's risk appetite allows for classification of the risks into two broad buckets: risks that are lower than your risk appetite; and those that are higher.

RISK RESPONSE:

The heavy lift is done by now – you know which risks are below and above your appetite. "Now What?" In the simplistic model, you accept the risks below your appetite in pursuit of your objectives. What do you do with the one's that are above your appetite? You cannot accept it, of course! Ready for another acronym? You can TAM your unacceptable risk – Transfer, Avoid or Mitigate it. While increasing your insurance coverage is an example of transferring your risk to another entity that is willing to accept it, the concept of risk avoidance would require you to stop engaging in any activities that can result in the particular risk. Mitigating a risk is where you engage in continual improvement initiatives to bring the risk below your appetite. Lean, Six Sigma and other problem-solving tools come in handy for this option. Post implementation reviews to ensure long term effectiveness of the risk response actions must be completed diligently.

CONCLUSION:

Seamlessly embedding the ERM process within an organization's strategic planning and operational monitoring activities will enable an organization to manage uncertainties in pursuit of enterprise objectives. Such organizations are generally better prepared to deal with uncertainties compared to organizations that do not have an enterprise-level framework for managing risks.

The intent of this article is to serve as a demystified primer for the vast domain of Enterprise Risk Management (ERM). There are several other aspects of this critical subject matter that must be discussed and understood before one can start effectively leveraging benefits. Impact of organization structures, governance model, role of internal audits, development of the enterprise risk-registry, articulating consistent risk appetite, exploiting opportunities from uncertainties, information technology & related security concerns, business continuity and disaster recovery programs are some areas that need further coverage. The author hopes to continue this discussion on this topic in successive upcoming interactions to support the interested reader's efforts in building a robust ERM framework in pursuit of enterprise objectives.

Sri Vilayanoor is the President/CEO of Ignition Life Solutions, Inc. Management systems consulting firm. He has an MS in Industrial Engineering and BS in Mechanical Engineering.