

## **Risk: How much is too much?**

### **A Risk Management White Paper by**

Paul O'Brien

LinkResQ Limited

Sept 2013

## Q. Risk: How much is too much?

## A. Ask your Granny.

Like the question how long is a piece of string, it depends. The degree of risk depends on a number of factors and this article looks at one of the dependencies: the enterprise **Attitude** to risk. Or how much do we care?

When we think of risk the tendency is to look to the dark side. Negative risk has a connotation of cost and cost is always bad. Mitigating negative risk is never sexy and the justification process is often made difficult by an enterprise attitude that at best agrees “we have to do this”, e.g. insurance, basic compliance etc. In an enterprise with this “compliance only” attitude management engagement in a mitigation decision is grudging and typically the level of justification required from the mitigation champion is higher than that required of a manager seeking support for investment in the development of a widget with wings.

My Granny was an enterprise risk manager, she knew things. “Don’t put all your eggs in one basket” she advised without knowing she had, established a risk context, identified the magnitude of risk consequence, confirmed the magnitude of likelihood, conducted a risk assessment, and devised a mitigation strategy, all without a college education.

The decisions she confronted us with were to, bring a second basket,(capital intensive), make more trips to the hen house, (labour intensive) or accept the risk she had identified and advised against (risk intensive). Her advice was based on common sense observation of risk and the wisdom of experience. The process through which she came to her advice is as valid in the board rooms of today as it was in the farmyards of the past.

The **attitude** to enterprise risk management could be described in five levels:

|  |                                |              |
|--|--------------------------------|--------------|
| We should have done this years ago.      | Realising the benefits         | Optimised    |
| There might be something in this for us. | Recognising the opportunities  | Standardised |
| We ought to do this.                     | Understanding the process      | Informal     |
| We have to do this.                      | Basic compliance and insurance | Ad hoc       |
| We shouldn’t have to do this.            | Denial                         | Absent       |

There are other dependencies that determine the maturity of an organisation with respect to how it treats risk. These are summarised in the table below.

How much is too much is determined by the enterprise risk attitude. The attitude is often established by factors such as the industry sector, industry standards, organisation complexity, size, maturity and position. Some organisations seek only to do what they are obliged to do; others seek best practice and have enterprise risk management embedded in their processes as a fundamental part of their way of doing business. The Enterprise Risk Management processes act to minimise the negative or downside risks and enhance the upside risks, with the same level of management attention and the same decision making criteria applied to both.

My Granny had a china statue of three monkeys, see no evil, hear no evil and do no evil, they looked like they were in denial about something and I wonder if a modern court would find they were in fact conspiring to take, condone or ignore risk while trying not to be associated with the decision.

The Sarbanes Oxley act has driven compliance in that it has ensured that the business leaders are responsible and are held accountable for the decisions and actions of the enterprise in law. Whether

it be the “hear, see, do and know of no evil” management team at Enron or the “conspiring board” at Tyco, the prospect of going to jail has taken most enterprise managers out of denial. The attitude to risk has changed as a result in many companies. Enterprises that use ERM processes did not have to be driven by SOX they already knew the level of any potential exposure and have a proactive attitude to risk. They take some, avoid some, and mitigate some but they engage in assessment processes that identify all the known risks to their enterprise, including the risks of corrupt or illegal governance.

To test the attitude of an enterprise take any one of the enterprise objectives you are responsible for and ask, what would happen if you failed to meet it by 10%? Would you, as the responsible manager be fired or forgiven?

If you survived a 10% miss keep escalating the percentage by which you failed to meet the objective until you get to a number where you would get your P45. You just found, for your objective, how much is too much.

The attitude of the enterprise will modify if the probability of failure was known in advance; if it had a warning. Good enterprise risk management processes provide knowledge of the factors and circumstances that could possibly cause primary objectives to be missed by amounts that the enterprise finds intolerable to the point where it becomes unforgiving. The knowledge of the risks makes for better informed decisions in the establishment of the objectives in the first place. Knowledge is the essence of enterprise management.

Extend the forgiveness test across all of the primary objectives and into the secondary objectives of any enterprise and you will begin to determine the enterprise risk appetite. In simple terms effective organisations measure what matters and the measures matter. Risk matters, whether you take it or avoid it, it matters. In risk lies your opportunity to surprise or be surprised. If the objective you are responsible for has an inherent risk that you have identified and the advent of that risk could bring your metric beyond the threshold of your P45 percentage, mitigate or emigrate!

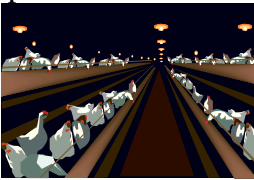



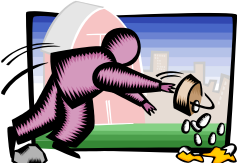
My Granny was not old enough to remember the maps of the world from when it was flat. But she told me her granny told her the maps used to have little signs that said “here be dragons” or “there be monsters”. These were Mitigation strategies identified by enterprise risk managers with knowledge of the limitations of the technology available at the time.



Know the risks and know how far you can go without causing significant loss.

As Isabella said to Columbus, after she and Ferdinand had seen the enterprise risk manager’s power point presentation on his proposed venture, “If you’re mad enough to go, we are mad enough to fund it.”

Paul O’Brien is Director of Business Development at LinkResQ [pobrien@linkresq.ie](mailto:pobrien@linkresq.ie)

| Level   | Attitude   | Practices  | Information Systems   | People   |
|---|--|--|---|--|
| <b>4. Optimised</b><br>    | Enterprise Risk Management is embedded in strategic planning. Benefits are recognised. Policy documented and communicated. | Risk Management embedded in all of the organisation's practices and processes. RM performance measured and reported. RM and Objectives are aligned. Plans regularly exercised. | Risk Identification and assessment captured electronically. Risk register maintained and updated regularly. Priorities identified. Treatments recorded. Progress tracked. | All senior managers support RM policy and actively promote it in their areas. Good performance rewarded. Poor practice shunned. Individuals aware of their roles and responsibilities. |
| <b>3. Standardised</b><br> | Senior management recognise the opportunities that can flow from formal Enterprise Risk Management.                        | RM customised for the organisation taking policies and culture into account. Standard practices in most areas.   | Central register of risks maintained with a consistent method of measurement of likelihood and consequence. Visible to all managers.                                      | Senior manager with overall responsibility for RM appointed. Resources identified in annual budget.  |
| <b>2. Informal</b><br>     | Compliance and best practice driving RM in some key areas. Recognition of the value of compliance.                         | Some categories of risk are managed well. No coordination between individuals handling different categories. No single standard.   | Lists maintained by individual managers in personal drives.   | Some individual managers taking responsibility for risks in their area of responsibility. Varying degrees of risk perception among managers.   |
| <b>1. Ad-hoc</b><br>      | Expenditure on Risk Mitigation seen as a pure cost and grudgingly spent.   | The company does what it has to do to be compliant and no more.  | Sporadic recording of initiatives and associated costs. No consistency.   | Managers in reactive mode and mitigating risk as it happens.   |
| <b>0. Absent</b><br>     | The management of the company does not recognise the need for basic risk management and control.                           | Employees regularly exposed to dangers. Financial and operational controls weak or non-existent. Compliance requirements ignored.  | Little or no information on incidents, or costs associated with incidents and accidents, available.   | Management unaware of extent of risks. Nobody taking responsibility for employee safety, property loss control or financial control.   |

Enterprise Risk Management Maturity Model © LinkResQ Ltd [www.linkresq.ie](http://www.linkresq.ie) Tel + 353-61-477 888