LinkResQ
A LEADER IN ENTERPRISE RISK MANAGEMENT

# Enterprise Risk Management Looks Forward

## A Proactive Approach to Good Corporate Governance

A Risk Management White Paper by

Gerard Joyce

LinkResQ Limited

## Introduction

Corporate Governance is concerned with practices and procedures that ensure a company is run in such a way that it achieves its objectives.

Consider a typical enterprise and the accepted need for management controls, regular & precise reporting of essential metrics and the necessity to adhere to all statutory obligations, filings, tax returns and shareholder data. A large part of the compliance effort is spent annually in managing these controls and at year end (or more often), significant time is required to carry out a full audit.

The audit process looks back. Did you do what you say you do? Did you do what you said you would do last time an audit revealed a problem? Did you put those controls in place that you promised you were putting in place? Are the controls working as they should? It is accepted that auditing is an important function in the overall management of organisations but is there an over-reliance on auditing? Where the organisation is required to comply with certain rules and regulations then independent auditing gives external parties the confidence that the organisation is following (the letter of) the law. But the nature of auditing is that it comes **after the fact**. It looks at what has happened and what is in place. It is a "lagging indicator" of the performance of an organisation.

Where rules or regulations have been introduced to prevent risks, (like corporate fraud, corporate failure, unacceptable commercial practices, etc.) an audit is necessary to establish confidence in the organisation by shareholders and customers. But rules, regulations and auditing do not address all risks that an organisation faces and although an over reliance on this mechanism is not considered good management practice, many enterprises have come to **put off** necessary and maybe unpleasant actions pending the outcome of the annual audit. For some of these, alas, this can come too late to undo the damage caused. Likewise, the annual "clean bill of health" from the audit may offer some protection to your reputation, although failure to comply may be a cause of loss of reputation, and the damage may already be severe. For some risks – like damage to property - there is insurance, which at best is a cost smoothing mechanism. Your premium reflects the ultimate cost of these losses spread over many years.

## Best Practice

Organisations need to find a suitable balance between risks and returns, which is why in all Corporate Governance codes there is the recommendation that an appropriate risk management system be put in place.

For many risks there are neither regulations to make you do the right thing nor insurance to cover you if things go wrong. What remains to be prevented and mitigated must be addressed systematically and by implementing best practice. Risk management needs to be embedded in the organisation's procedures. You cannot always eliminate risk, but you can take steps to reduce either, or both, the likelihood and the consequences.

For this reason it has come to be recognised that a more effective and structured approach to implementing best practice is necessary. Based on the growing awareness that risk management is an aspect of business that has been somewhat overlooked or at best conducted in "silos" the International Standards Organisation has produced a set of principles and guidelines based on best practice and

published these as the ISO 31000:2009 standard.

Kevin W Knight AM, chairman of the ISO Working Group on Risk Management, when asked at a recent conference on risk management in Dublin how he viewed the need for more effective ERM policies, put it very succinctly: “Survival is not compulsory”.

**In Best Practice Organisations**

- **Compliance** imposes someone else’s risk appetite.
- It consumes energy
- It consumes resources
- It should be a consequence of good practice.
- In which case it **is FREE**

P O’Brien 2010

For those who want to survive and pursue their objectives with confidence the recently published risk management standard, ISO 31000:2009, gives clear guidance on how to go about integrating risk management into your management system and the steps you need to take to make risk management one of your business excellence processes.

## The Risk Management Standard

ISO 31000 is about principles and guidelines. It is not for certification, though many seek this. It’s about best practice. It’s about continuous improvement. It’s about doing things right, in order to increase your chances of success, minimise loss and provide an effective tool that works with your business cycles in real time rather than in hindsight.

The principles outlined in the standard are aligned with good corporate governance and support effective risk management.

The guidelines recommend that a framework for the management of risk be setup within the existing management system and that a consistent process to identify, analyse, evaluate and treat risk be implemented in the many areas and levels, functions and projects in the organisation.

The definition of risk as “the effect of uncertainty on [the achievement] of objectives” makes the alignment of the risk management programme with objectives a fundamental requirement. It is important to identify those risks that may have an impact on your objectives (positive or negative) so that resources can be appropriately deployed.

## Looking Forward

An organisation should be governed in a way that ensures the achievement of its objectives. If all things were certain then achieving objectives would be easy. It is in “the uncertainty” where the risks lie and that is why a systematic and comprehensive approach to identifying the risks and taking measures to prevent them or mitigate the consequences, is required. This is a proactive approach and serves to inform decision making.

The risk management standard suggests measuring the level of risk as a combination of the likelihood and consequences. This is a significant proposition as it shows that risks of low probability and high consequence can be as problematic as those of high probability and low consequence. The important point here is that one needs

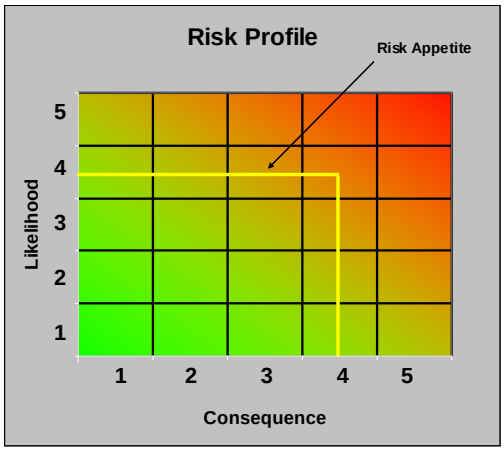
to understand the uncertainty of likelihood **and** the uncertainty of consequences in order to address the risk completely.

Probably one of the most difficult and much debated concepts in risk management is "risk appetite". It doesn't feel right to say "we will accept this much loss". But to say that any loss is "intolerable" would be to condemn the management to a life of surprises. It is important for the Board of directors to decide on "the nature and extent" of the risks the organisation is willing to take, so that others in the organisation are aware of where the limits are and can act accordingly. One method of representing risk appetite is as a line in the likelihood-consequence matrix (See right), or a number representing a limit in the level of risk.

E.g. If level of risk is Likelihood x Consequence you might set your appetite at 12 (25 being the highest)

This is a simple method of setting nominal appetite. In complex organisations additional statements will be required. For example you might set your appetite with policy statements that limit your exposure to a particular market sector or single customer. E.g. "No more than 25% of investments will be in the property sector."

Some "appetite" decisions will be very risk-specific, the important point is that limits are set and those responsible for managing the risk know the limits.




**Likelihood and Consequence Matrix from CalQrisk**

## Summary

Be clear on what you are defending and how much loss you can bear. Identify those risks that can cause you to fail to meet your objectives and put the appropriate level of control in place to prevent the risk occurring to the extent of your risk appetite. Where you cannot prevent a risk, consider preparing plans to lessen the severity should it occur. This will give you the confidence to pursue your objectives resolutely, while being prepared for mishaps along the way. Embedding the discipline of risk management in a structured way will in itself yield dividends as the heightened risk-awareness will mitigate many risks. Lookout! Identify and address the risks before they find you.

LinkResQ Ltd., 4200 Atlantic Avenue, Westpark, Shannon, Co Clare, Ireland
Tel: +353-61-477 888, email: @linkresq.ie, web: .linkresq.ie