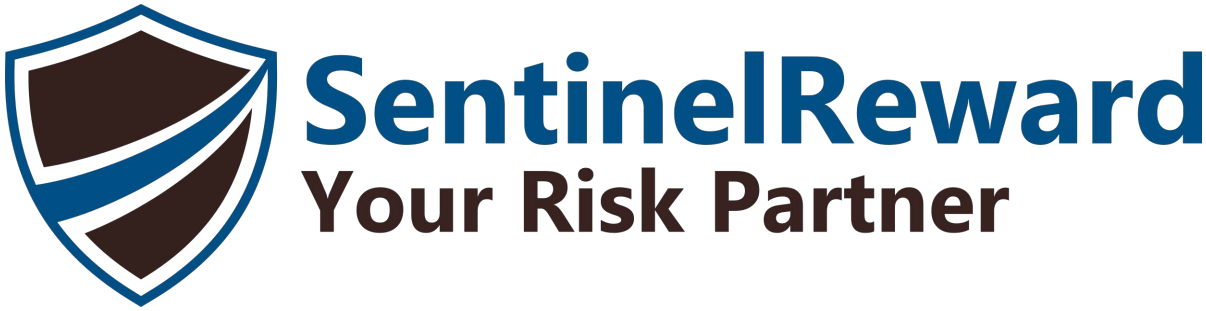


Effective Enterprise Risk Management: Mind the gap!

Effective Enterprise Risk Management: Mind the gap!

Introduction

Over the past twenty years Enterprise Risk Management (ERM) has become a fundamental part of the corporate vocabulary. When ERM is used to optimal effect it can make corporate strategy more robust by bringing both upside and downside risk into sharp focus on a pan corporate basis. It is however rare to see risk management applied in the most complete manner. Too often stakeholders witness a 'gap' between the envisaged framework and the actual ways of working post framework implementation. Companies and their stakeholders would be well advised to 'Mind the gap'. Minding the gap means working to reduce the gap to zero, and ensure the implementation matches the vision. In short, ERM must be a part of the 'Way of life' for the organisation if it is to be successful.

Arguably minding the implementation gap is the most important area of focus to achieve effective ERM. Multiple respected ERM frameworks exist which can be rendered bespoke to a company, but the most exceptional framework design all comes to nought if the people in the company do not understand why effective ERM matters for them.

The International Organisation for Standardisation in ISO 31000:2018 defines risk as being:

"the effect of uncertainties on objectives"

People working towards achieving organisational objectives can use ERM to help manage for such uncertainties. What person does not want to enable better business performance in their company? ERM is about both conformance and performance. This is a key element in landing the merits of effective risk management. To have the greatest impact ERM needs to flow through the veins of an organisations culture. Embedding ERM in the ways of working will improve management of opportunities and challenges facing that company. Embedding is all about implementation.

To paraphrase James Carville in the 1992 Clinton election, "It's the implementation stupid!". So how does a company get the implementation right. Start with people. Capture the hearts and minds of the company employees and you will have little to no gap between ERM vision and reality. Optimal implementation of ERM demands an embedded risk aware culture which manifests itself clearly in the ways of working for the company.

Can the enterprise risk approach influence the approach of the company if the pre-existing culture does not respect ERM principals? This is not intended to be a rhetorical question. A key determinant is the implementation methodology. Effective implementation will impact the very fabric of a company culture. ERM and the culture should become inextricably linked. Alternatively, ERM will suffocate if left in a vacuum, worse still it can lead to a false confidence for the stakeholders in the company. Consequently, implementation methodology matters. If there is a gap between framework design and how it manifests in the life of the organisation, stakeholders need to be aware of that gap and act on it as soon as possible.

How we define risk management

There are many different definitions of risk. ISO 31000:2018 describes risk management as:

> *"A co-ordinated set of activities and methods that is used to direct an organisation and to control the many risks that can affect its ability to achieve objectives."*

Arguably this is as good a definition as any, and even in reading this definition it should be clear that the 'How' and the 'Why' are just as important as the 'What'.

Co-ordinating activity and methods require people to embrace an approach. People have a greater propensity to excel if they believe in what they are doing and can appreciate its full importance. The implementation approach is the greatest opportunity to land a crystal-clear message as to why effective risk management is critical in the company and the definition above makes it clear that people have a central role to play in the process.

Where to begin in making ERM compelling for people?

You need to win people's hearts and minds on the merits of ERM, but where is the best place to start? Simon Sinek the motivational speaker, in his books 'Start with Why' and 'Find your Why', underlines how the powerful telling of real-life stories can be when trying to get buy in from your audience. Wells Fargo is an interesting case in point of an entity that lost focus on risk management, their story is striking. The 168-year-old bank received a $3 billion fine from the US Federal Reserve in February 2020. The Federal reserve stated:

> *"Wells Fargo pursued a business strategy that prioritized its overall growth without ensuring appropriate management of all key risks. The firm did not have an effective firm-wide risk management framework in place that covered all key risks."*

For most of its corporate life Wells Fargo was held up as an example of commercial virtue. Yet this all seemed to count for nothing as the fines from the Federal Reserve for false deposit accounts and cross selling emerged from 2011 onwards. In a Forbes article in September 2016, 'How the Wells Fargo Phony Account scandal sunk John Stumph' (Wells Fargo former CEO) reference is made to Stumph's mantra to his staff – "Eight is great", A reference to how many accounts he wanted each Wells Fargo customer to hold. Stumph introduced a new way of working at Wells Fargo which was at odds with sound risk management. Wells Fargo is just one example, there are many more stories to tell.

People want to work for companies they are proud of. If ERM is understood to be an effective means of protecting reputation and performance, it will be more possible to align the approach with company objectives and with the creation and execution of strategy. Employees will realise productive ERM is not static, it is dynamic just like the corporate organism it seeks to protect and enhance. Stories are a great place to begin to fully implement and embed ERM in the ways of working of the company. When it comes to ERM,

implementation methodology matters. ERM believers, particularly if influencers within the company, can become implementation champions.

Frameworks: The implementation matters most.

Modern day risk management is about positively managing both threats and opportunities. There are multiple enterprise risk management frameworks which have evolved to help companies get on top of this mission. Some are considered more relevant to a particular industry. A brief list of some of the most notable frameworks can be seen below:

> **COSO – Enterprise Risk Management: Integrated framework (COSO, 2004) –** In many ways the genesis for modern day ERM and was created post the WorldCom and Enron corporate catastrophes. Risk appetite is a key area of focus.
>
> **ISO 31000 – Risk Management Principles and Guidelines (ISO, 2018**) – An internationally recognised benchmark and is written in such a way as to be directly applicable for SMEs and manufacturing organisations.
>
> **CIIA – Three lines of defence model (2015)** – Most commonly found in financial services sectors and largely effective at demarcation of risk management responsibilities within large complex entities.

One common denominator of all these frameworks is their emphasis of the importance of aligning ERM to the core objectives of the organisation. Indeed, the COSO framework was revised in 2017 and called 'Enterprise Risk Management: Integrating with strategy and performance.' The title of this revised approach underlines the central message of this paper.

The ERM Framework must be fundamentally linked to the function and strategy of the company, if not, an extremely dangerous gap appears with potentially catastrophic consequences for the stakeholders. ERM must be inextricably linked to the company heartbeat and the corporate rhythm, per the 2015 PWC article 'How ERM Programmes Evolve', where they state:

> *"Effective ERM processes are typically aligned with the corporate calendar, which requires ongoing involvement throughout the year that moves beyond the initial enterprise risk assessment"*

Irrespective of which framework is selected and rendered bespoke, great attention must be given to its implementation if it is to 'come alive' within the company. David Tyler, Chairman of J Sainsbury put it well when he said:

> *"What counts is the actual behaviour of the organisation and its top people. This is far more significant than a hundred statements about a company's culture or its ethical policy"*

Arguably this 'coming alive' or embedding is more important than anything else to determine the creation of a genuine risk-aware culture. In short, as much if not more time and effort

need to go into the implementation plan, as the original framework design. Landing the power of the ERM framework has already been discussed as a key facet of the implementation, another area to consider in detail is where are the typical challenges that may be encountered in employee adoption.

Everyone in the company must be considered, the board may be ultimately responsible for risk management and oversight but every single individual in a company are owners of risk. Every member of staff can potentially positively influence the outcome. Echo from the bottom is as important as tone from the top. To improve the effect of uncertainties on objectives the entire staff need to understand how they apply ERM to its full potential.

Mark Parker, the Executive Chairman of Nike put it very well when he once commented:

"We have a culture where we are incredibly self-critical, we don't get comfortable with our success"

A risk aware culture will serve the company well, ERM can assist in embedding that culture.

People related ERM Implementation Challenges

Advanced ERM frameworks will have many complex and technical components, the reality though is that typically technical challenges are solvable if you can access appropriate resources. The more challenging difficulties tend to be behavioural. Understanding these challenges clearly is critical to addressing them. Creating early warning indicators so the red flags become obvious early in the ERM implementation is a good idea. Some of the primary challenges are considered below:

- **Do what we say not what we do** – Management apathy to ERM.
  Arguably the most important element in effective implementation, the CEO and Executive have enormous influence on the acceptance/potential for ERM. Often termed 'Tone from the top', it is difficult to envisage any probability of success without the will of the top management.
  EWI: No attempt to combine risk evaluation with strategy creation.

- **We cannot clearly explain why ERM is important** – Unclear message on ERM
  The What, How and Why are not explained properly. No clearly understood risk taxonomy.
  EWI: Inconsistent understanding throughout the company.

- **Box ticking** – ERM Tools become an end in of themselves.
  Control and monitoring tools such as Risk Control Self-Assessment (RCSA) and Failure Modes Effect Analysis (FMEA) become the primary focus. Once tools are populated the view is risk management is complete. Risk is live, and therefore the management approach cannot be static, or worse still operate in a pure reporting mindset. Second order risk is also frequently missed as silo approaches can become common.

EWI: Pattern of risks materialising that were not envisaged in the ERM framework.

- **No one was listening** – Poor risk issue escalation process and a blinkered board. No crystal-clear manner for front line staff to call out concern and have that concern acted upon. It is also imperative for people to have courage of conviction if they have a genuine concern. If people with integrity who have the respect of others are ignored this is extremely damaging to the prospect of a risk aware culture.
  EWI: No evidence of action surrounding event data.

- **Group think** – No independent challenge/people prepared to take a contrarian view. Wilful blindness to data and information at odds with strategic direction.
  EWI: No evidence in committee minutes of challenge or contrarian debate.

- **Risk perceived as Business Prevention officers** – No senior executive support. The business views the risk department as an adversary as opposed to a partner and potentially best form of defence when setting sound strategy.
  EWI: High turnover in the risk function. Anecdotal interview evidence.

If you are witnessing any of these challenges presenting, they are red flags for ERM organ rejection. In 'The science of Successful Organisational Change: How Leaders Set Strategy, Change Behaviour, and Create an Agile Culture', Paul Gibbons commented:

> *"Business people need to understand the psychology of risk more than the mathematics of risk".*

In a scenario where executive management really want to realise the greatest potential of Enterprise Risk Management and embedding a risk aware culture, the best first step must be to help people realise why ERM matters both in terms of prudence and performance.

The implementation approach must be profound, that matters more than having a pristine bespoke ERM design because if you can embed the risk aware psyche, almost by definition the framework will evolve to better over time. A good place to start is to identify respected informal leaders in the organisation pre implementation of an ERM framework. Ideally you want to turn these influencers into champions of the ERM approach. If you can do that you are well on the right path to effective ERM.

ERM – What does great look like?

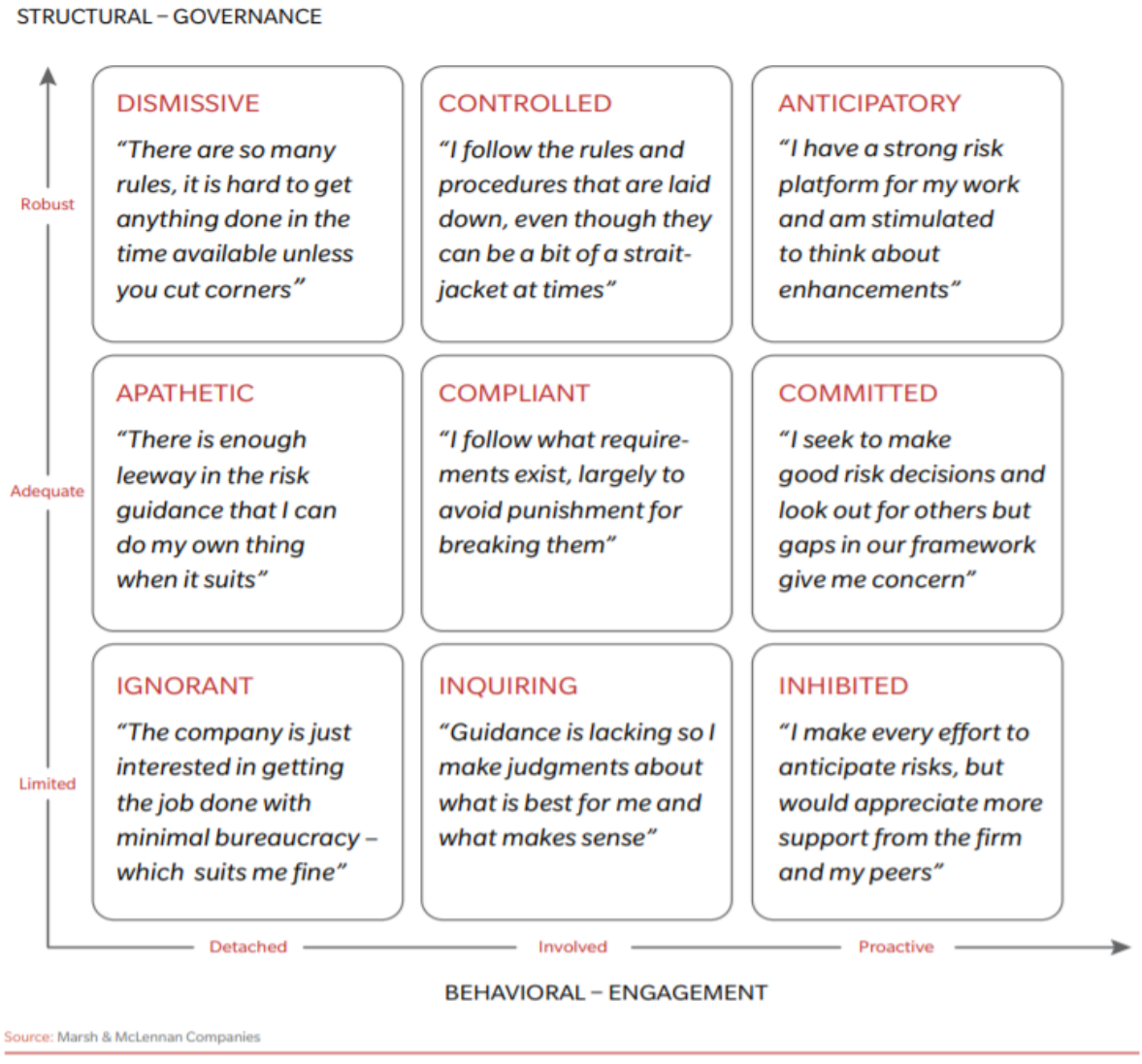
In their paper 'A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000'– The Institute of Risk management tells us:

> *"Risk Management must be integrated into the culture of the organisation…. It must translate risk strategy into tactical and operational objectives, and assign risk management responsibilities through out the organisation"*

Moreover, In the PWC report – 'The COSO ERM Framework one year later: What we have learned', Helen Katz and Frank Martens comment:

> *"We found organizations that were shifting their view of risk appetite, seeing it not merely as a compliance-driven evaluation exercise but instead as a way to expand their thinking when deliberating important decisions. Those organizations have learned—quite possibly the hard way—that by making more risk-informed decisions up front, they can more easily address evaluation concerns later."*

This looks like further evidence of some companies getting closer to a 'great' approach. The truly enlightened companies have deduced ERM is genuinely about both prudence and performance. If you can close the gap between your vision and actual implementation of ERM you can then start to evolve towards 'great' more meaningfully. Marsh McClennan devised a useful way to consider where your company stands as regards having an embedded ERM approach, see below:



Source: Marsh & McLennan Companies

ERM is about both Conformance and Performance

Taking ERM to the next level is about looking at both upside and downside risk. The regulatory or stakeholder imperative tends to drive many companies to employ an ERM approach, but companies need to be aware of the dangers of a pure compliance motivation. It can lead to the wrong behaviours and regulators are now very much alive to that, so much so in fact that they are beginning to look much more deeply at 'ways of working' in organisations.

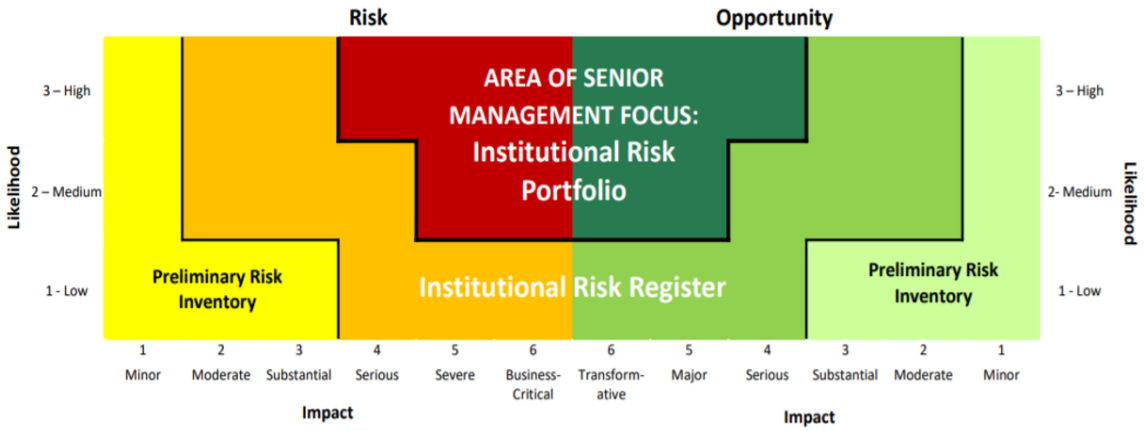
By way of example in the banking world the Financial Conduct Authority in the UK actively consider Governance, Leadership, Purpose and Reward through an organisational culture lens. The Central Bank of Ireland is also giving far more emphasis to good practice and how they expect to see it embedded in ways of working in the organisation. Indeed, identification of a 'gap' between an ERM design and its actual implementation would be a red flag to a supervisor/regulator as well as to an observant management.

'Great' requires ERM to be deeply embedded in the way of life of a company. The Chairman of the UK National Grid underlined this in his observation on 'Corporate Culture and the Role of Boards' for the Financial Reporting Council in the UK:

> *"Like risk, culture doesn't benefit from being given its own separate status and processes. It is part of doing good business and needs to be intrinsic in everything"*

The message here is powerful, it may be referring to the area of culture but there is an explicit recognition that risk like culture must be intrinsic to everything the organisation does.

Perhaps one of the most replete ways to evidence this is if the company has fully evolved to reviewing both risk downside and upside in a consistent manner. This would suggest that the company sees optimal risk management as a commercial imperative. It would mean that the business and ERM were inextricably linked. Emily J.Stebbins-Wheelock and Al Turgeon of the University of Vermont show us a snapshot of what that might look like practically in a tool they include in their 'Guide to risk assessment and response'.



Intuitively one might expect a company employing 'great' ERM to have evolved to this point.

Conclusion

Enterprise risk management is continuing to evolve. Many frameworks and associated tools exist and are easily understood as constructs. What matters most though, is execution. If there is a ‘gap’ between your design and its practical application on the ground, that is a fundamental gap that is potentially ultimately terminal for your company. The board and senior management would be wise to mind that gap, that is they need to manage it to zero.

If management are genuine in their appetite to work towards great ERM they will be highly motivated to manage and reduce the gap. If management are not genuine in their approach the gap will expand and ultimately expose their ‘false’ approach to stakeholders including regulators and supervisors. Ultimately the gap may result in a terminal event for the company or in the case of Wells Fargo and so many other former great entities a fall from grace in the most astonishing manner.

The good news is, as this paper has illustrated, there are ways to position your ERM in a truly intuitive manner to the people in your company. The CEO and senior management must be true believers and standard bearers. Furthermore, Internal influencers can become your champions if they fully appreciate the prudence and performance capability of ERM, and that it will serve to protect their company long into the future. Implementation and adoption won’t happen overnight but if you ‘mind the gap’ by being prepared and establish clear EWIs, and employ them in thorough ongoing audit, your company has a much better chance of getting to truly great ERM than most.

Bibliography

- CIIA – Three lines of defence model (2015)
- COSO – Enterprise Risk Management: Integrated framework (COSO, 2004)
- COSO, 2017: Enterprise Risk Management: Integrating with strategy and performance
- Financial Conduct Authority: DP20/1: Transforming culture in financial services – driving purposeful cultures
- 'Find Your Why', 2017 Penguin Books, Simon Sinek, David Mead & Peter Docker
- Financial Reporting Council, July 2016, Corporate Culture and the Role of Boards
- Forbes, September 2016, 'How the Wells Fargo Phony Account scandal sunk John Stumph'
- International Organisation for Standardisation in ISO 31000:2018 defines risk
- ISO 31000 – Risk Management Principles and Guidelines (ISO, 2018)
- ISO 31000:2018, definition of 'risk management'
- James Carville in the 1992 Clinton election
- Mark Parker, the Executive Chairman of Nike
- Marsh & Mclennan Companies (2015) Risk Culture Think of the consequences
- Protiviti, The Bulletin, Volume 3, Issue 6: Ten Common Risk Management Failures and How to Avoid Them
- PWC report, October '18, 'The COSO ERM Framework one year later: What we have learned' Helen Katz and Frank Martens
- PWC, June '15, 'How ERM Programmes Evolve'
- PWC, October '15, The COSO ERM Framework one year later: What have we learned?
- The Institute of Risk Management - 'A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000'
- The Institute of Risk Management, ;A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000'
- The science of Successful Organisational Change: How Leaders Set Strategy, Change Behaviour, and Create an Agile Culture', Paul Gibbons
- University of Vermont, October 2018, 'Guide to risk assessment and response'- Emily J.Stebbins-Wheelock and Al Turgeon
- US Federal Reserve in February 2020, Wells Fargo Financial Sanction https://www.federalreserve.gov/newsevents/pressreleases/enforcement20180202a.htm
- 'Start with Why', Penguin Books, Simon Sinek