ERM - Let the Truth be Told

You have an ERM programme in place?

Great! The organisation has an ***enterprise risk management*** ("ERM") programme in place. After all, it is a corporate governance requirement for public-listed companies, and everyone knows that it also provides benefits to the organisation. These are the expectations of ERM.

Now, for the reality check, we need to ask:

.....is the ERM programme working as it should be?

.....does it truly meet with corporate governance requirement?

.....has it delivered? Add to achieving KPIs and to the bottom-line?

Or .....is it only a facade - an image of the real thing that consumes precious corporate resources but not yielding the expected benefits?

All over the world, business managements ponder over whether there are economic returns from their ERM programmes. Many are doubtful but still allow the programme to continue nonetheless. But doubting is not an available option. CEOs, CFOs and independent directors hold fiduciary obligations to see to it that the organisation's system of internal controls and ERM are adequate. They are duty-bound, by corporate governance rules, to ascertain and to declare unequivocally their positions on the efficacy of such processes for the protection of minority shareholders, failing which they could face admonitions or even criminal charges.

Let the truth be told.

The greatest risk about ERM is the risk in its implementation outcome. Incredible, but true!

The common outcome for many organisations is that ERM implementation frequently leads to fruitless reviewing of the Risk Register at biannual/annual intervals for the sake of compliance reporting. Such are invariably cursory reviews on risk registers, changing dates on documents and submitting a report saying that everything is fine, and life continues until the same is repeated at next reporting date. There is, sadly, often no co-relation with the real business conditions nor with actual risks that the organisation faces.

The reality in the practical world, is that a high proportion of ERM programmes haven't really delivered their expected benefits. **This is the truth that must be told.**

Now, **Risk** is the impact of a probability of change to status quo. Based on definition, risk can bear bad impact so it is a 'bad' risk, and it can also bear good impact, a 'good' risk. Risk has size - determined by the frequency of occurrence and the impact magnitude of the risk.

There are things to know about business risks.

(1) Managing a business is all about managing its array of risks. A successful business succeeds only because it is able to manage *bad* risks and exploit *good* risks. An industry leader leads because it manages its business risks more effectively than its peers within the industry. Those that have little ability to manage their business risks will fall by the wayside, and are prone to meritocracy or business failure.

(2) Every risk has its potential impact, good or bad. Fire-fighting, a common phenomenon nowadays, has bad impact. A fire-fighting episode means a risk has been triggered and it now requires immediate attention, stealing scarce time and resources from productive work. It follows that an effective ERM programme that eliminates or reduces fire-fighting episodes must translate into improvements on: productivity, customer service, resource usage, which altogether must show up at bottom-line profit and in happier employees.

Meeting Expectations

The Board is accountable to its shareholders. Minority shareholders based their investment decisions on risks they perceived through disclosures, which should be accurate statements of risk exposures facing the business. Hence, corporate governance rules make it incumbent for the Board, CEO and CFO to ensure that business risks, particularly major ones that affect current/future earnings be properly managed; and to make official declarations that internal control and risk management processes had been put to bear in managing risks, and where applicable, to provide disclosures of unmitigatable risks that may affect investment decisions.

Unfortunately, most top managements find it difficult to fulfil their fiduciary obligations. Why?

(a) Most ERM programmes focus on strategic and financial risks, which is good. But they do not entreat lower operational risks because they believe them to be non consequential, which is not reality. It is often the small innocuous but unmitigated risks that cause business failures! It is the incessant trickling from fractured small pipes that result in wastages and inefficiencies - all these lead to loss of earning potential affecting the investments of minority shareholders.

(b) When managed at high level, the risk's characteristics become blurry rendering it difficult to diagnose its dynamics that is required to prescribe doable treatment actions. In the absence of doable treatments, there is no link to day-to-day operations. Eventually, the ERM programme becomes only a paper-exercise, a wasteful ritual conducted without apparent benefits in return. With this rather indeterminate outcome, top management is non-wiser yet they are obliged to put their signatures attesting to the effectiveness of internal controls and risk management.

So, what constitute an effective ERM programme ...that delivers results?

The ERM system should be built and be customised to the organisation based on ISO 31000 Standard or the COSO framework, with the following ten (10) key operative features:

		rate yourself Score (Max 10)
1.	ERM organisation, accountabilities, roles and responsibilities established for: (a) ERM oversight [by Risk Management Committee, or AC], (b) ERM programme management [by Risk Manager], and (c) risk ownership [by functional managements].	
2.	Risk management of (a) strategic risks, (b) operational risks, at all impact levels and including occupational safety and health.	
3.	Risk appetites established on four impact bases: (a) financial, (b) human capital, (c) reputation and (d) governance.	
4.	Prescription of doable risk treatment actions for all risks, to be acted upon by designated risk owners/officers.	
5.	Quantify/qualify the effect of the prescribed risk treatment actions, which may be verified by independent persons (e.g. Finance).	
6.	Annual/biannual review, or when there is significant change in business scope or operations, undertaken by risk owners, including attesting that prescribed risk treatments were indeed carried out. These require proper documentation.	
7.	Annual ERM Report issued by Risk Manager, reporting on new risks, risk incidents, status of major risks, critical follow-up actions, points of consultations with or for decision-making by top management. Report should enable audit trail on actions taken or scrutiny by senior management, if such is required.	
8.	Annual ERM Validation by Risk Management Committee or Audit Committee, when the CEO presents the status of the organisation's risk situation.	
9.	Submission for disclosure be prepared, for AGM or for insertion into the annual report, based on the Annual Report that had been earlier validated by RMC.	
10.	Effective risk communication system to notify the proper management persons in event a risk has been triggered off.	

ERM is indeed the very foundation of business management. The smart will put it into good use, while those seeking only expediency will continue to lose its benefits unknowingly even when the price to implement the programme has been paid.

Total (max 100)