CRITIQUES TOWARDS COSO'S ENTERPRISE RISK MANAGEMENT (ERM) FRAMEWORK IN ITS BASIC ASSUMPTIONS

Ika Atma Kurniawanti, SE., M.Si., Ak.
Department of Accountancy, the faculty of Economics, Airlangga University

ABSTRACT

Most professionals in internal control, risk management and other similar bailiwicks have agreed that Enterprise Risk Management discourses would've invariably referred to what the COSO had produced recently: the framework underlying ERM. But this paper takes a bit different stance that views several problematic issues stem from unclear conceptions of either the basic premise underlying ERM or the nature of some ERM's components outlined by COSO. This paper notes that, at least, there are three points of COSO framework that should be streamlined in order to smoothly establish an ERM policy in organizations as follows;

1. *Obscured definition of "risk" that remains unresolved in COSO,*
2. *COSO's view in determining the optimum balance between risk and outcome;*
3. *Practical difficulties in implementing ERM under the COSO framework*

As an alternative, this paper argues that rather than being confused with "risk" and "optimum balance" terms as mentioned by COSO, something that might be deemed as too academic, we better emphasize our concern towards what Anthony Marshal mentions as the "impact of negligence" (Marshall, Anthony; 2004). Furthermore, this paper also introduces a "reasonable care" treatment –a controllable threshold where some acceptable treatments should be in place to overcome certain predictable exposures, no matter that if they will strike you afterwards– as a preferable risk mitigation action for organizations. This is a more practical and reasonable approach in treating exposures that a company might be challenged by, rather than trying to cover too many types of risk.

Liability arises from fault. If there is no fault, there is no liability. If there is no negligence, there is no fault. And this premise should be upheld when organizations start developing their ERM.

Keywords: risk, optimum balance, impact of negligence and reasonable care

1. PREVIEW

The glamour stage of business struggle has long been glittered by cheerful behaviors of many preachers of management concepts and techniques that, each of them, campaigned as the most effective tool to fortify the business towards uncertainty. They come dazzling

down by touting themselves as a panacea towards any business illness or unfitness faced by business entities. Within the climate of ever-increasing corporate risks, indeed, this trend is gratefully welcomed by enterprises, which are thirsty with a definite answer responding to the business difficulties they face to. Such as numerous risk-related issues that have surfaced as a result of the business scandals like Enron and WorldCom, leaving many shareholders, executives, and boards wondering what exposures their own organizations may encounter to. And at this point, multifarious formulas are blended to offer a batter of medicine to answer the business problems, no matter that those are just a type of mode, or even meaningless. At least, following the trend means increasing the self-confidence that business is already on the right track, and in turn, will gradually reduce their anxiety.

One of the vastest threats the business facing is the risk. But more than just an embellishment of the one that traditionally comprehended; we'll find concept of risk has so expanded in nowadays literatures. Originally when we take a look at dictionary, we will find the term of "risk" is defined as the possibility of bad result, or cause of harm, or else; the level of security of business insurance or money lending (Longman Dictionary of Contemporary English, 2005). In the last phrase, we can see that risk even has a dual meaning; positive and negative, depending on the adjective accompanying the term; high or low. So the negative interpretation can't be simply connoted directly to the term of "risk". This is parallel with the concept of risk as quoted from Australian Risk Management Standard 4360 (Alijoyo, 2002), of which risk is defined as "the chance of something happening that will have an impact upon objectives"; a neutral position in viewing the risk. This is apparently the 1st acceptable common definition of risk beside other specific interpretations that frequently used by some professions such as in auditing, from whom we've learned about the technical terminology of risk such as inherent risk, audit risk, and so forth. But of course, it is considered not relevant to discuss such technical terms in detail on this paper.

Yet, referring to such modern business concept of risk, this term is now widely understood as something that adversely affects the organizations in achieving their objectives and goals effectively and efficiently. This term, of course, tends to be purely negative. Such as Vaughan who proposes his definition of risk as "a condition in which there is a possibility of an adverse deviation from a desired outcome that is expected or hoped for" (Alijoyo, 2002), some experts also view risk equal with uncertainty; meaning the larger it is, the risk will then be greater. The alternated definitions may take place in various ways indeed, but the point is firmed that the risk, in contemporary interpretation, is commonly associated with the obstacle preventing organization's objectives and goals accomplishment. That in turn, brings the business society to devote their attention seeking any possible ways to mitigate risks, or moreover, to remove their existence.

2. THEORITICAL FRAMEWORK

Enterprise Risk Management

A systematic approach to reduce risks is generally known as risk management. People undertake risk management activities to identify, assess, manage and control all kinds of event or situation (IIA(b), 2004). These can range from a single field or narrowly defined types of risk – e.g. market risk or environmental risk – to the overall threats and opportunities facing the organization as a whole. Back to the history, it can be trace back that the risk management concept has its origin from the insurance industry since the mid of 1950's, when insurance buyers attempted to increase their recognition and status, and began to expand their demands by including the loss prevention, industrial safety and employee benefits (Alijoyo, 2002). It was similar with the next developed strategy set forth to reduce the impacts of hazardous materials and pollutants in environmental terminology. But of course, it is totally different with the current circumstance, as the insurance or environmental treatment is only perceived as a part or possible treatment of which the overall risk management process encompasses various types of method to address and mitigate the risks. As described on the publication of the Australian and New Zealand Standard of Risk Management (AS/NZS 4360, 1995), the Risk Management process is defined as (Alijoyo, 2002):

> "…….An interactive process consisting of well-defined steps which; taken in sequence, support better decision-making by contributing a greater insight into risks and their impacts. The Risk Management concept can be applied to any situations where undesired or unexpected outcome could be significant, or where opportunities are identified".

Such a cutting-edge concept that views risks broader and more likely integrated may further and commonly be quoted from COSO (The Committee of Sponsoring Organizations of the Treadway Commission) (COSO, 2004). On September 29, 2004, COSO has released *the Enterprise Risk Management — Integrated Framework* in New York. This integrated framework was born from the apprehension towards a series of high-profile business scandals leading to mass debacles where investors, employees, and other stakeholders suffered a tremendous loss. The aftermath of such swell of business failures has led to the calls for the enhanced risk management concept that is expected to provide the key principles, a common language, and a clear direction towards a full set of risks mitigation strategy, regardless of organization's size. And therefore, the publication provides business organizations, for the first time, with a principles-based framework that will enable them identifying all aspects that should be presented in every company's enterprise risk program including how they can be successfully implemented. ERM has since been spreading over as a new paradigmn for managing risk that is even believed as the most effective strategy an organization can use to manage a plethora of risks, running the gamut of strategic, market, operational and

financial exposures to the daunting array of man-made and natural disasters (Banham, Russ, 2004).

Instead of relying on traditional, inter-departmental strategy, where each area of organization manages its own risks, ERM adopts a broader perspective that integrates and coordinates risk management across the entire organization. It does more than just integrating risk management, this enterprisewide approach is ultimately intended to enhance and protect stakeholders' values, as campaigned by its proponents (Walker, et all, 2003). Such overwhelming expectation can indeed be trace back to the definition of ERM as promoted by COSO (COSO, 2004):

> *"... a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives".*

This is parallel with another explanation issued by IIA that also defines ERM as below (IIA(b), 2004): "A structured, consistent and continuous process across the whole organization for identifying, assessing, deciding, on responses to and reporting on opportunities and threats that affect the achievement of its objectives".

All the above expanded definitions, however, have generated risk management to ambitiously go forward from its original form. The ERM is now accepted as a modern platform of which companies may combine and harmonize every single risk reduction effort into the company-wide level risk handling, called risks management portfolio. Along with other initiatives, this management tool will then be incorporated into a comprehensive business strategy.

A number practitioners said that, as in contrast with the traditional risk management that works best on financial risks – the risks that are transferable – ERM stresses management in operational and strategic risks (Banham, 2003). While the traditional risk management requires more accounting-type skills, ERM requires skill in strategic planning, process reengineering, and marketing. For example, a financing company's operational risk would be its back office, in terms of how prudent they evaluate the credit applications coming in, how good they monitor their outstanding debts and ensure the repayment of loans, and eventually, how they settle down their non-performing loans. This is just similar with a vehicle dealership company whose their operational risks involve the supply chain of vehicles stock, delivery to customer, and aftersales service availability. As a brief, the difference between conventional type of risk management and ERM can be described as follows (Banham, Russ, 2003);

Figure 1
Traditional RM vs. ERM: Essential Differences

Traditional risk management	ERM
Risk as individual hazards	Risk in the context of business strategy
Risk identification and assessment	Risk portfolio development
Focus on discrete risks	Focus on critical risks
Risk mitigation	Risk optimization
Risk limits	Risk strategy
Risks with no owners	Defined risk responsibilities
Haphazard risk quantification	Monitoring and measuring of risks
"Risk is not my responsibility"	"Risk is everyone's responsibility"

Source: Russ Banham, 2003

COSO has provided eight components of the ERM framework that are interrelated each other. Five of them are taken from Internal Control-Integrated Framework – PricewaterhouseCoopers estimates that 60 percent of the new document is leveraged from COSO's earlier work (Chapman, 2003) – but the ERM Framework is nonetheless quite different. It is because risk is a more all-encompassing topic than internal control so that the resulting discussion found in the new framework is much more comprehensive than its predecessor. Not only does the ERM Framework include three additional components that different from Internal Control-Integrated Framework; those are objective setting, event identification, and risk response, but five items taken from the control model are broader in their descriptions and in term of the practical guidance. In sum, the ERM components consist of : 1. Internal Environment, 2. Objective Setting, 3. Event Identification, 4. Risk Assessment, 5. Risk Response, 6. Control Activities, 7. Information and Communication, 8. Monitoring

The broader coverage of the framework is indeed deemd as a key strength, at least within the eyes of the COSO Board and Project Advisory Council. The next development of modern concept they brought should not impair the previous one. As quoted from Prawitt statement (Chapman, 2003);

> "Many organizations have adopted the COSO control framework, various audit standards rely on that framework, and it looks like the internal control reporting required under Sarbanes-Oxley will be heavily based on the COSO internal control model. So it was absolutely critical that the new risk framework not undermine COSO's earlier work."

And thereof, ERM framework is considered incorporating, rather than replacing; COSO's groundbreaking 1992 study, Internal Control-Integrated Framework.

But all the above concepts, however, haven't necessarily proven that the COSO's framework of ERM is the most recommended practical solution in managing organizations'

risks. Many external factors such as regulation and legislation have influenced the glaring of the COSO's concept; and all those factors are now intersecting in one confluence. And the factors, hence, have apparently compelled many enterprises to swallow right the way the new concept of ERM, adapt to it and then implement it without ability to question critically whether such new concept is suitable or not. How the certain condition is cited as "ready", or otherwise "not ready" for ERM implementation? What is supposed to do if the entity is not well prepared to apply the ERM? Answering such questions is critical as if the organization hadn't been ready to it, they wouldn't have gained too much from ERM. Instead of optimizing the opportunity by managing risks, they might become a milk cow for consulting firms that are now hustling out to offer the ERM consultation as their new expensive service portfolio. So, don't hire your consultant before finishing this paper.

3. PROBLEM

The Problematic Issues of ERM

It is not the aim of this paper to discuss each component above in detail, as the study such a way will take a multi-dimensional approach to complete. Of course there is no wrong with the concept outlined by COSO, as it is ideal and such ideal is always attractive, and even provocative. However, to gauge the success of management concept cannot merely focus on how broad the concept is accepted and implemented, especially in the case of ERM. Such concept should be challenged, at the theoretical concept espousing and at the practical stage as well. All formulas and theories alive are underpinned by certain assumptions that could be right or wrong, and therefore, would be subject to examination. Regarding to the idea, this paper is intended to show and criticize the issues; 1. Obscured definition of "risk" that remains unresolved in COSO, 2. COSO's view in determining the optimum balance between risk and outcome; 3. Practical difficulties in implementing ERM under the COSO framework. In coming up elaboration, we would present those problems in more detail.

4. ANALYSIS AND DISCUSSION

Actually, there are several problematic issues stem from unclear standpoint of either the basic premise underlying ERM or the nature of some ERM's components as elaborated by COSO. Such presumption set forth to underpin the concept of ERM can be referred to below statement (COSO, 2004);

> "……that every entity exists to deliver value to its stakeholders. Since all entities face uncertainty, the challenge for management is to determine how much uncertainty to accept as it strives to grow stakeholders' value. Uncertainty brings up the events of both risk and opportunity, with the potentiality to erode or enhance value. Value is maximized when

> management sets strategies and objectives to strike an optimum balance between growth and return goals and related risks, efficiently and effectively deploys resources in pursuit of the entity's ojectives".

From sentences above, at least, we can capture two words containing vagueness; the 1st one is the term of "risk" itself, while the other one is the "optimum balance". Both complicated terms will be unraveled in coming up discussion.

We have seen the distinctive idea of "uncertainty" from the above simple narration of which it contains both risk and opportunity. And consequently, risk has to represent the negative thing that should be avoided in contrary with opportunity. The framework, indeed, doesn't intend to claim that risk is both positive and negative in nature. Instead, risk is clearly defined as "the possibility that an event will occur and adversely affect the achievement of objectives" (Chapman, 2003). The framework covers the upside of risk by calling for management to identify all potential events that could affect the organization's ability to successfully implement its strategy and achieve its objectives. Those events with potential negative consequences represent risks to be addressed through the risk management process (COSO, 2004). This is a significant change compared to the previous definition of risk that views risk as something that may have positive or negative impacts depending on certain circumstances behind. Now, risk is perceived as a purely negative thing, such as written by IIA; "Events that may have a negative impact represent risks" (IIA(a), 2004).

In the meanwhile, another events that may have positive outcomes, are defined as opportunities, which the framework indicates that it should get back into the organization's strategy and objective-setting processes (IIA(a), 2004). This is a kind of tepid demeanor, in which COSO's framework tries to overlook other different perspectives in viewing risk. By doing so, they have utterly simplified the process of framework development trough pressing down the adverse arguments to stay beyond the surface, such as Prawitt statement;

> "By talking about potential events that may have either positive or negative outcomes, the framework supports both the individuals who see risk as opportunity and those who are dedicated to managing the downside aspects. Yet, it maintains its focus on risk management as a process for managing possible negative outcomes and their impacts. That's important, because if you try to put together a framework that incorporates both the positive and the negative in the definition of risk, the discussion of risk management gets unwieldy. Plus, it doesn't really fit with a lot of people's conception of what constitutes risk".

Of course, disguising the problematic definition of risk would not solve the problem anyway. We cannot compel such mindset by certain ideological term without compromising it with other opposite arguments that may exist. Such as Jackson who

perceives that discussing about "risk" should also consider the context and any circumstances surrounding; the term of risk may therefore be accepted in various senses depend on the context underpinning (Chapman, 2003);
"If you talk to a business unit leader who has to generate profits for a company, he or she may view risk as opportunity. However, if you talk to auditors or treasurers, they will likely view risk as downside exposure that needs to be managed. As a result, there has been a tendency to insist that any definitions of risk include both the idea of opportunity and adversity."

We must still remember the lesson from one ancient economic principle we'd ever learned that the amount of risk is equivalent with the return; higher risk you tolerate, higher return you may expect, and vice versa. So within this principle, how're you supposed to measure the "negative" side of risk while it always contains the positive inherently as well? It will, in turn, rise up unstoppable debates about the nature of negative or positive impact brought by risk. But one thing is firmed; the organization has to devote their attention and effort to prevent anything that may be harmful for its going-concern or sustainability, whatsoever its name, while on the other hand, keep moving to maximize its return or income.

Setting the Tone of Optimum Balance

The unresolved debate of risks will then bring us to the 2nd problematic issue in which the term of "optimum balance" is closely related with any efforts exerted to minimize risks and to maximize returns as well. It is envisaged that company may only endeavor to maximize its value by setting an optimum balance among the business growth, its return, as well as related risks. But exactly at this point, the dilemmatic position arises. COSO leaves the most complex term – optimum balance – behind to each ERM implementer, under its own interpretation. In fact, every single business with the purpose of maximizing profit has its own risks as the cohesive part; if there is no pain, no gain. So how suppose to determine the level of balance they mentioned anyway? It is mostly a kind of abstract term rather than the definite one. How if, let say, an organization that aimed to reduce risks would have concurrently also reduced its potentiality to gain the return regarding to the fact that higher return you expected, so higher risk you would encounter to? Defining the optimum balance amongst risk, business growth and expected return is not so simple as there are no discrete criteria to do so. In fact, you may even have to enlarge your risk in order to get your income higher occasionally. Or another worse possibility; by reducing one of your organization's risks, you probably trigger up another risk – something that maybe more perilous. So it is obvious that setting up the "optimum balance" is one responsibilty that almost impossible to discharge.

In the area of financial management, there is a common practice that before investing a certain number of fund, we would compute firstly the value of our expected returns as well as risks involved. But defining the optimum balance between both terms is a different

matter. There is no, so far, the most acceptable parameter of what level we should set up values for return and risk. Moreover, COSO's framework doesn't intend to discuss solely about financial risks, it encompasses a wide range of risks. All those terms can't necessarily be refered to certain amount of dollar value just like in financial risk indicators, such as Loher and Stohl's statement (Loher, Diedre D. and Richard M. Stohl, 2005); "We auditors definitely need to break out of the "risk silo mentality" and become more experienced in identifying "real-world business risks." It's difficult at times when the emphasis is to attach a dollar value to associated risks; not everything can be quantified in such a way. And, just because you can't attach a dollar value, doesn't mean it isn't a significant risk to the organization".

The ERM covers all types of negative possibilites; from natural disaster risks till financial risks. Scoring or quantifying risks in order to simplify the identification process, or determine which one is favorable rather than others, may be acceptable. But adversely, determining precisely an "optimum balance" is imposible. So, how exactly we could balance both terms if we couldn't measure them up? In fact, the term of "optimum balance" is the one critical reason why COSO proposed its framework.

Some experts argue that in order to determine the acceptable level of the optimum balance, it's better to use the potential losses value for paramater. For example; the risk of polluting seawater with hazardous and toxic waste may be measured with the magnitude of potential disaster it may cause. But again, in our opinion, this is not a wise solution. The reason is two points; (a) The negative impacts of certain risks are frequently difficult to predict, and in turn, it will be difficult to measure the potential losses, (b). In fact, some industries have inherent risks which are related with nature, that seems almost impossible to compromize or balance to. For example; a certain maritime business such as fisheries may inherently be facing to risks of hurricane or typhoon from time to time. If you were a businessman, and you had been aware with such potential risks of disasters you might face to, it would have meant nothing to you. The business must go on, and the natural disaster is just a matter of destiny, as simple as that. We cannot remove or reduce the impacts anyway.

Regarding to the above fact, so some questions may arise. How we're expected to balance risk and return, if on certain occasions, risks – especially those ones related with natural events – may have a fatal impact? For you who get involved in fisheries business might realize that you could get a tsunami in your workplace anytime you go offshore fishing. But you still go there.

Practical Viewpoint in Risk Management Treatment

Beside those major issues discussed above, there is still another problem in practical viewpoint when one company decides to use COSO's ERM framework. Although those components of ERM may be perceived as a series of step by step of actions that should

be taken by companies when they develop ERM, COSO prefers to perceive the ERM as not a serial process where the one component causes the next (COSO, 2004). It is more likely a multidirectional, reciprocal process in which almost any component can and does influence another. However, variation amongst the companies in the term of how the entire components are supposed to be implemented is recognized. The eight components will not be functioning identically for all entities, as this should be in line with the size of entity, their business scale as well as many other unique factors. And therefore, the practical model of ERM may be various in different organizations and cannot be judged as right or wrong.

Confronting the COSO's standpoint that prefers to place ERM framework as not a serial processes where one component causes the next is necessary, as this is conflicting with practical viewpoint. COSO's argument may be regarded as not stepping down to earth. This paper argues that such ERM project start up should thoroughly consider the cultural background and natural context of an organization such as said by Funston (Funston, 2003);

> "The ERM process begins with an evaluation of the context or environment in which the organization operates, its strategy for achieving its objectives, its organizational culture, and its appetite for risk. Understanding the external operating environment and the organization's business objectives and strategies is an essential first step in understanding the business conditions and the nature of the risks the organization may face.

Extracted from several precious experiences of conducting risk management project in a couple companies, we argue that organization culture and internal environment is a key element of initiating the risk management project. Not only just like that, ERM implementation projects somehow require the organization to turn around their old-fashioned culture into the new one, such as said by Ballou and Heitger (Ballou, Brian; dan L. Heitger; 2005); "ERM requires ownership by executives, careful oversight by directors, and a cultural shift at most organizations. That makes the initial implementation of the framework the biggest challenge before the process can reach its potential".
The success of culture shifting would drive the next succes in ERM implementation, and we believe that this critical component is not exchangeable or cannot be substituted by other steps like sugested by COSO.

Without disseminating, injecting and organizing behviours, attitudes and apptitutes necessary for a risk aware environment throughout the organization, at first stage of development, the risk awareness behaviour may only be sensed or touched only by those in high layer of organization. Or worse, a not-so-well organized cultivation of risk may lead to different perception amongst decision makers themselves, which in turn, will hinder the company to grow up the required culture of risk awareness across the organization. The cultural setting of ERM needs organization members to take risks

ownership in their areas of responsibility, as they are the business owners. This is a bit challenge towards most organizations in which the "top management driven" type organization would be irrelevant, such as Ballou and Heitger said (Ballou, Brian; dan L. Heitger; 2005);

> "The ERM framework can be expanded, including an eventual cascading of the framework throughout other levels of the organization as senior management becomes comfortable with the culture the framework creates. Part of that cultural change requires that people throughout the organization take ownership of risk management.

So it is obvious that the principles of risk awareness should be grasped, sensed and internalized by all organization members without exception. Management should demonstrate their commitment to the ERM initiative to all employees and become a role model to them. Otherwise, public might see it only as a signal that an organization is only following trends. Thus, executives should ensure that a firm-wide risk management culture is developed, even though initial rollouts of the framework might not involve every aspect of the organization.

Alternative Practical Solutions

Rather than getting busy with any debates incurred about "risk" and "optimum balance", something that might be deemed as too academic, we better emphasize our concern towards what Anthony Marshal mentions as the impact of "negligence" (Marshall, Anthony; 2004). This is a more practical approach in treating exposures that a company might be challenged by, rather than trying to cover any types of risks. Liability arises from fault. If there is no fault, there is no liability. If there is no negligence, there is no fault. But common law requirements or stakeholders expectations create a duty for business to exercise a "reasonable care"; a controlable threshold where some acceptable treatments should be in place to overcome certain predictable exposures, no matter that if they strike you afterwards. Natural disasters such as hurricanes are legally referred to as "acts of God," thus eliminating legal liability for any damages incurred. If a healthy tree is uprooted and flies into a moving car, it's an act of God. Who could an injured person sue claiming fault? But "reasonable care" mandates – for example – a hotelier to exercise some adequate treatments for their guests safety and security against hurricane or typhoon, so they won't be suddenly blown away with the first heavy gust of wind. For example, it's not "reasonable" to keep the hotel's outside playground open during a blustery day or when the sky is overcast as the hurricane signal, or else, to encourage or promote beach activities during that one. Those requirements remain steadfast, through and after the storm anyway.

Of course the term of "reasonable care" can also be problematic when we attempt to gauge it. But that's exactly the point; we should, indeed, leave the term remains to be in

wide-range interpretation as company should determine their own operational unique parameters in accordance to pursue the most "reasonable care" to avert certain negative impacts from unpredictable events. There is no need to balance anything such as COSO's suggestion. But operational parameters may still be set up, for example; such a hotelier located at shoreline assigns their coastguards certain parameter of required time of respond to hurricane indications. However, the tolarable limit of how much time needed in order to properly be mentioned as a "reasonable care" would depend on their common sense. You may not have to know or predict how devastating the hurricane would affect you, or how the disaster trends might be, but something is firm that you are not excused to make any negligence so you just let your guests being unsafe. It is fundamentally different with the "risk appetite" term as mentioned by COSO, since risk appetite is mostly related with the level of risks you could accept. You don't need to waste your time to tabulate or identify any overreaching risks, as they've already been existing inherently in your activities. All you have to ensure is that you have already prepared yourself with any reasonable care treatments for sudden awfull impacts arising from disastrous events.

Particularly in Indonesia cases, in which most businesses are operated under uncertainty circumstance – especially due to the lack of law enforcement and unstable politic – there is actually a major risk that companies face to along the way. If risks figure had become a first priority in investment decisions, you could've imagined that nobody would invested their money in Indonesia. Many external factors influences business as a sine qua non and all of them are beyond the companies' control. All Indonesian companies were even slackening during the crisis, and some of them went to bankruptcy, they've all been being such a "normal condition" till the time. But of course, just blaming or scapegoating all losses your company suffered from crisis to the political circumstances is unfair. You should firstly assure that there was no part of negligence you had done that even haistened your company's falling down such as; you didn't play your money recklessly in forex market, or as a banker – you didn't distribute a large portion of your fund mostly to related parties, and so forth. Thus, rather than identifying and registering any potential interruptions towards your business – that might lead you to shut down your company's operation since the high exposures profile you have – you would be better to enlist any possible adverse events that controlable in nature and then set up your reasonable treatments.

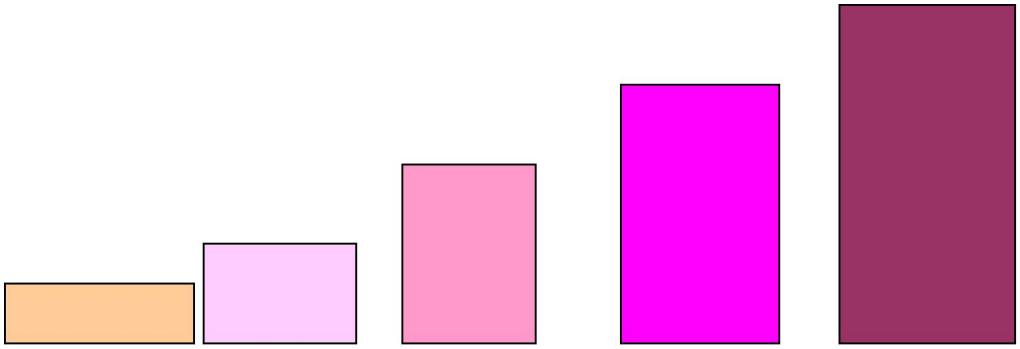
After you have measured and set up all operational parameters necessary for "reasonable treatments", the next question may arise; how are you supposed to determine the "common sense" as mentioned by the above paragraph? The answer is; it will be coming up from your length of experience in handling risks and your organizational culture maturity in risks awareness. A mature culture of certain workplace environment should gradually be developed in conjunction with organization growth. Many employees –at early initial stage of ERM introduction– may only view ERM as the latest corporate

trend that distracts them from running the business. But as the framework evolves over time, however, employees are more likely to adopt the risk awareness philosophy, especially when they see senior management and board members adopting it. As the risk management culture develops throughout the organization, each aspect of risk management can be incorporated into day-to-day operations. When the employees have already been fully aware with organizational values and culture, you won't have to make a special program to propagate or reverberate your mission, the entire employees will necessarily follow the demonstrated role model consciously. But of course, culture shifting is not just a fingertip that could be finished overnight. It requires an eagerness, impetus, clear guidance and directions as well as the firm reward and punishment scheme. Those schemes have to be consistently applied and imposed al the time.

Some facts have shown that a type of risk management model is often succesfully established in an organization with mature culture. We have gained a couple experiences in ERM projects direcly in two different companies representing different approach in ERM implementation. The first one is a company – one of the biggest conglomerates in Indonesia – that has long been running the business in the country for decades and having a robust culture of ethical business and corporate control awareness. Its achievement is proven by several prizes awarded in the fields of internal control and corporate governance both Nationally and Internationally. During the involvement, the author was observing how the company successfully established and incorporated the ERM into their system. Although some problems noted, nevertheless, we can still gain a good lesson from this company who has successfully developed their own ERM genuinely from its resources, by its own effort, and without too much external consulting.

What they had done during implementation was basically much helped by the fact that each person in organization had already had a fervent mindset of risks awareness. The company's system has also been well prepared for any types of most recent management techniques, as they have already had a definite and measurable KPIs matrix, clear targets and guidance, published code of ethics, a self-developed original management system, and so forth, while their business lines are indeed very profitable. All layers of organization have been familiar with continous changes. That's why, the project team could successfully register risks configuration till the bottom-line level by fascilitating the revolving directive interviews and brainstorming meetings amongst the staff at bottom-line; those whom are not regarded as business owners under COSO's framework such as cashiers, mechanics, salespersons, etc. And please note that they didn't use the COSO's framework. But the message is clear; all of those achievements are not attained at a wink, they need experience and patience.

Figure 2
Control Environment Development



• Control by owner • Instinctive indicators • Reliance on eye-watching • Individual control program • Dependence on quality of owner • Internal Auditor doesn't exist.	• Minimum Internal Controls • Instinctive indicators • Reliance on Internal Audit Function • Individual control program • Dependence on quality of people and individual habits • Internal Auditor as "*a policeman*"	• Complete & strict SOP and regulation • Financial historical indicators • Reliance on system • Authoritative control program • Dependence on quality of management • Internal Auditor as "*a consultant*"	• Code of Ethics & SOP developed • Comprehensive indicators – BSC/ RM • Reliance on value system • Participative control program • Dependence on quality of system • Internal Auditor as "*a facilitator*"	• GCG & BPR for SOP • Predictive analysis & leading indicators • Reliance on corporate culture • Cross-functional control program • Dependence on quality of participation and awareness • Internal Auditor as "*a partner*"

We cannot expect a certain company makes a big leap to ERM without familiarity with management techniques evolution such as TQM, Malcolm Baldridge, or leading and lagging indicators in Balance Scorecard for example. We're not able to discuss a risk awareness without adequate versatility and knowledge of internal control, or good corporate governance, or something else. This is – in our opinion – the exact backbone of what so called "internal environment" required for ERM. And an organization needs a time to have all those things, such as depicted on a bar graph on Figure 2.

All the above facts are fundamentally different with another company – a kind of MNC has been operating for 10 years in Indonesia – in which the author has also experienced with. In this company, the "internal environment" or organizational culture and values are not quite strong. The culture is still vascillating, and individual's behaviour or mood sometimes predominantly affects the organizational directions. The company is still looking for the most appropriate pattern of genuine values they can explore and exploit. Yes, they have already applied a Balance Scorecard application software, they have registered and discussed intensely the company-wide risk register, but still, all those parts are not synchronized each others; they've just gone through without common goals. In the

meanwhile, the ERM framework is just a kind of discourse. There is still no – amongst the staff – a common perceiveness that such risk management program should also belong to them. So we're not so surprised that the progress is static; risk register just discusses the elitist risks, and done separately by each manager responsible without a consolidation. There is no any cascading effects to employees; business is just running as usual. Within this condition, the author suggests that the company is better to devote their internal control related efforts to establish firstly the organizational culture. We can attest it later by conducting questionary research throughout all employees to find out whether the desired values have totally been accepted by them or not.

5. CONCLUSION

Finally, the business practitioners – are fully aware that a kind of new business tool always seize abundant curiousities and interests. This is consistent with this statement: "One concern regarding the COSO ERM framework is that its overreaching nature can appear overwhelming (meluap, berlimpah) for some organizations, particularly those that are small in size or have not previously established an ERM culture". (Ballou, Brian; Dan L. Heitger; 2005):

But one thing should be realized that, eventually, all decisions are yours. Regardless some problematic issues as pointed out above, truly, not every organization is even looking to implement ERM. "Given the size and nature of certain companies, it may not be cost beneficial to migrate to an ERM process," Jackson says, as quoted from Chapman (Chapman, 2003). "They can, however, still assure the board and stakeholders that the control environment is effective, because it is possible to have an effective internal control environment without enterprise risk management." The original control model may remain to serve these organizations. Even less, there are also some other prime determinants that may unexpectedly affect the implementation of ERM in an organization. So don't copy and paste right the way the new concept because of the trend, the companies must be convinced firstly that this ERM model is really needed by their organization. Such irrational imitative behaviour may cause unnecessary sporadic treatment that will charge the company for nothing.

REFERENCES

Alijoyo, F. Antonius; 2002; *Risk Management's Role in Corporate Governance*; Panel Discussion on Corporate Governance: "Accelerating the Implementation of Good Corporate Governance through Boards Independence"

Ballou, Brian and Dan L. Heitger; 2005; *A Building-block Approach for Implementing COSO's Enterprise Risk Management—Integrated Framework: Here is A Way Organizations of All Sizes, Cultures, and Risk Experiences Can Apply the Framework Without Becoming Overwhelmed by It*; Management Accounting Quarterly; IMA Banham, Russ; 2003; *Fear Factor: Sarbanes-Oxley Offers One More Reason to Tackle Enterprise Risk Management – Special Report ERM*; CFO: Magazine for Senior Financial Executives

Banham, Russ; 2003; *Fear Factor: Sarbanes-Oxley Offers One More Reason to Tackle Enterprise Risk Management – Special Report ERM*; CFO: Magazine for Senior Financial Executives

_____2004; *Enterprising Views of Risk Management: Businesses Can Use ERM to Manage a Wide Variety of Risks*; Journal of Accountancy; AICPA

Chapman, Christy; 2003; *Bringing ERM into Focus: a New COSO Study Provides Some Much-Needed Clarity and Structure to The Fluid Topic of Enterprise Risk Management – Committee of Sponsoring Organizations of the Treadway Commission Report on Enterprise Risk Management*; Internal Auditor; IIA

COSO; 2004; *Enterprise Risk Management – Integrated Framework, Executive Summary*; COSO

Funston, Rick; 2003; *Creating a Risk-Intelligent Organization: Using Enterprise Risk Management, Organizations Can Systematically Identify Potential Exposures, Take Corrective Action Early, and Learn From Those Actions to Better Achieve Objectives*; Internal Auditor; IIA

Loher, Diedre D. and Richard M. Stohl; 2005; *Not Quantifiable*; Internal Auditor; IIA

Longman:2005,*Dictionary of Contemporary English,* Pearson Education Limited,England.

Marshall, Anthony; 2004; *"Acts of God" can be tempered with risk management - Consultant's Corner*; Hotel and Motel Management; Advanstar Communications, Inc.

PricewaterhouseCoopers; ———; *COSO Releases Enterprise Risk Management — Integrated Framework;* Principles-Based Framework for Managements and Boards to Comprehensively Manage Risks to Objectives

The Institute of Internal Auditor (a); 2004; *Applying COSO's Enterprise Risk Management — Integrated Framework*; www.theiia.org, United Kingdom.

_____(b); 2004; *The Role of Internal Auditing in Enterprise-wide Risk Management* ,www.theiia.org, United Kingdom.

Walker, Paul L., William G. Shenkir and Thomas L. Barton; 2003; *ERM in Practice: Examples of Auditing's Role in Enterprise Risk Management Efforts at Five Leading Companies Shed Light on How This New Paradigm Is Impacting Audit Practitioners*; Internal Auditor; IIA.