ENTERPRISE RISK MANAGEMENT (ERM) SERTA PERANAN INTERNAL AUDIT DALAM *ENTERPRISE RISK MANAGEMENT (ERM)*

Kurniawati, SE,M.Ak
Dosen Universitas Bunda Mulia
e-mail : kurniawati@bundamulia.ac.id

ABSTRACT *Risk is embedded in business environment. A well established company must be aware and manage risks to be within company's acceptable risk level to achieve the goals of sustainable growth and enhance value of the company. In the late of 2001, US had been shocked by some corporate scandals in USA, such as Enron, WorldCom, Adelphia, etc. As a response of corporate scandals, US released Sarbanas-Oxley Act (SOA) as a law in 2002 that has had a major impact on worldwide enterprises and particularly those with securities registered through the Securities and Exchange Commission (SEC). SOA established major new regulatory rules for public accounting firms, financial auditing standards, and corporate governance. Risk management as one of important elements from Good Corporate Governance (GCG) has evolved from risk management traditional to Enterprise Risk Management (ERM). ERM presents an enterprise-wide approach that eliminates traditional barriers between functions, departments, divisions within an organization. ERM facilitates detection of the major risks to the company and identification of improvement opportunities. ERM as a process needs internal audit function to give an assurance ERM process is implemented effectively.*

Keywords **:** *Enterprise Risk Management, Risk Management, Internal Audit, Good Corporate Governance*

PENDAHULUAN

Kebutuhan akan pentingnya *risk management*

Risiko merupakan suatu hal yang tidak terpisahkan dari dunia bisnis. Perusahaan yang baik bukanlah perusahaan yang selalu menghindari risiko tetapi perusahaan yang ”*aware*” terhadap risiko dan berusaha mengelola risiko tersebut secara efektif sampai tingkat/batasan yang dapat ditolerir oleh perusahaan. Sejalan dengan perkembangan dunia usaha, risiko yang dihadapi saat ini sudah lebih kompleks lagi, saling terkait dan dan memiliki potensi dampak yang lebih besar. Untuk itulah pentingnya identifikasi serta pengelolaan risiko secara efektif sejak dini sehingga ”kejutan-kejutan” semacam itu tidak lagi berdampak besar bagi keberlangsungan usaha karena sudah dilakukan mitigasi atas risiko tersebut sebelumnya.

Menurut Hamilton (2003), salah satu faktor penting yang menyebabkan terjadinya berbagai skandal kasus perusahaan – perusahaan besar di Amerika Serikat seperti kasus Enron, Worldcom, Adelphia dan sebagainya adalah lemahnya sistem pengendalian internal dan *risk management*. Sebagai respon atas maraknya berbagai kasus yang terjadi tersebut maka diterbitkanlah *Sarbanas-Oxley Act* (SOA) yang menekankan akan pentingnya pengendalian internal, *risk management* dan *good governance*. Di Indonesia sendiri, para regulator seperti Bappepam, Bank Indonesia, Menteri Negara BUMN mengeluarkan peraturan yang mengharuskan perusahaan *go public*, bank umum dan Badan Usaha Milik Negara untuk menerapkan *Good Corporate Governance (GCG)*. Untuk mewujudkan GCG yang baik maka salah satu implementasi prinsip transpransi dalam GCG yang harus dipenuhi adalah *risk management*. Penerapan *risk management* oleh perusahaan bertujuan untuk mengidentifikasi risiko – risiko perusahaan, mengukurnya dan mengatasinya pada level toleransi tertentu.

Berdasarkan uraian diatas, maka timbulah kebutuhan akan pentingnya pelaksanaan *risk management* secara efektif yang dalam prakteknya mungkin saja dilakukan atas dasar kesadaran perusahaan itu sendiri atau mungkin juga karena paksaan dari para regulator.

Konsep *Enterprise Risk Management*

Risiko merupakan suatu kata yang tidak asing di teling kita. Secara umum risiko dapat didefinisikan sebagai berikut :

*"Suatu **ketidakpastian** akan kondisi di masa yang akan datang, yang jika hal itu terjadi, dapat memberikan **dampak negatif** terhadap pencapaian **tujuan** yang telah ditetapkan."*

Pada dasarnya istilah *risk management* bukan merupakan istilah baru. Konsep *risk management* tradisional sudah lebih dulu dikenal terutama di kalangan institusi keuangan seperti perusahaan asuransi, dan bank. Konsep *risk management* tradisional tersebut lebih menitikberatkan pada perlindungan terhadap aset – aset fisik dan keuangan perusahaan (*physical & financial assets*). Misalnya, bagaimana mengurangi risiko terjadinya pencurian terhadap harta perusahaan, risiko bencana alam, risiko kredit macet, risiko tingkat suku bunga

yang berfluktuasi dan sebagainya. Pendekatan *risk management* tradisional ini sekarang sudah mulai ditinggalkan karena memiliki keterbatasan yaitu mengelola risiko secara terpisah dan berbeda-beda dalam suatu organisasi, padahal risiko – risiko yang ada kebanyakan bersifat ”*interdependent*” dan tidak dapat dikelola secara sendiri – sendiri. Selain itu dengan adanya pendekatan terpisah – pisah seperti itu maka pihak manajemen tidak dapat melihat suatu laporan atas risiko secara keseluruhan. Untuk memperbaiki kelemahan tersebut maka muncul istilah ”*integrated risk management*” atau ”*holistic risk management*” yang pada hakekatnya konsep ini membicarakan tentang suatu konsep risiko secara keseluruhan. Sebagai sebuah konsep baru, berbagai pihak berupaya untuk mendefinisikan konsep tersebut dan salah satunya adalah organisasi praktisi akuntan dan auditor keuangan yang cukup berpengaruh dan tergabung dalam *The Committee of Sponsoring Organizations of the Treadway Commission* (**COSO**) menerbitkan suatu konsep kerangka pengelolaan risiko perusahaan secara keseluruhan & terintegrasi yang dikenal dengan nama ***”COSO Enterprise Risk Management”*** **(COSO ERM).**

Berikut ini definisi COSO tentang ERM seperti yang dikutip oleh Robert R.Moeller dalam bukunya yang berjudul *“COSO Enterprise Risk Mangement : Understanding the New Integrated ERM Framework”* :

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

Dari definisi diatas, maka terlihat jelas perbedaan antara pendekatan *risk management* tradisional dengan pendekatan ERM yaitu :

1. Proses dan sistem dari ERM bersifat komprehensif, integratif, dan lintas divisional. Pada manajemen risiko tradisional, risiko dikelola secara parsial (*silo-based*)
2. Tujuan dari ERM lebih bersifat strategis yaitu pencapaian tujuan perusahaan secara keseluruhan yang lebih baik dan pada akhirnya menciptakan, menambah, dan atau melindungi nilai perusahaan dengan cara memasukkan

proses ERM dalam penetapan strategi perusahaan, mengidentifikasi peluang-peluang yang ada serta mengidentifikasi dan mengelola risiko sampai batasan yang ditetapkan oleh perusahaan. Pada manajemen risiko tradisional, tujuan terbatas pada mitigasi risiko pada kegiatan atau unit bisnis tertentu saja.

Kerangka ERM COSO

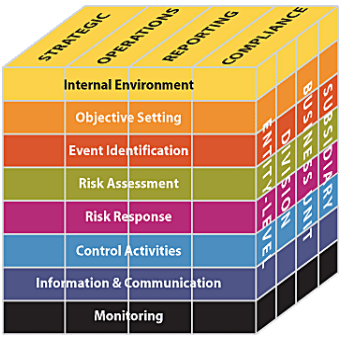
Dalam konsepnya tersebut, COSO juga memperkenalkan 8 komponen yang saling terkait satu sama lain dimana dari komponen – komponen ini akan diturunkan menjadi suatu proses ERM di suatu organisasi. Berikut ini uraian dari kedelapan komponen tersebut :

1. Lingkungan internal (*Internal Environment*)
   Lingkungan internal meliputi : filosofi manajemen risiko, *risk appetite*, sikap dewan direksi, nilai – nilai etika dan integritas, dan struktur organisasi.
2. Penetapan Tujuan (*Objective Setting*) :
   Tujuan yang telah ditetapkan perusahaan haruslah yang mendukung misi perusahaan dan konsisten dengan *risk appetite* perusahaan.
3. Identifikasi Kejadian (*Event Identification*):
   Kejadian internal dan eksternal yang mempengaruhi pencapaian tujuan perusahaan harus diidentifikasi, dan dibedakan antara risiko dan peluang. Peluang dikembalikan (*channeled back*) kepada proses penetapan strategi atau tujuan manajemen sedangkan risiko akan dinilai dan diberikan respon oleh pihak manajemen.
4. Penilaian Risiko (*Risk Assessment*) :
   Dua unsur penting dalam penilaian risiko adalah seberapa sering kemungkinan terjadinya (*likehood*) dan seberapa besar dampaknya (*impact*) bagi pencapaian tujuan perusahaan.
5. Respon Risiko (*Risk Response*)
   Atas risiko - risiko yang telah diidentifikasi dan dianalisa tersebut, manajemen akan memilih respon terhadap risiko tersebut, apakah menghindar (*avoid*), menerima (*accept*), mengurangi (*reduce*), mengalihkan (*sharing*).
6. Kegiatan Pengendalian (*Control Activities*)

Kebijakan dan prosedur yang ditetapkan dan diimplementasikan untuk membantu memastikan respons risiko berjalan dengan efektif

7. Informasi dan komunikasi (*Information & Communication*)
   Informasi yang relevan diidentifikasi, ditangkap, dan dikomunikasikan dalam bentuk dan waktu yang memungkinkan setiap orang menjalankan tanggung jawabnya.
8. Pengawasan (*Monitoring*)
   Keseluruhan proses ERM dimonitor dan modifikasi dilakukan apabila perlu. Pengawasan dilakukan secara melekat pada kegiatan manajemen yang berjalan terus-menerus, melalui eveluasi secara khusus, atau dengan keduanya.

Penerapan komponen – komponen ERM tersebut dapat dilakukan pada *entity-level*, divisional, unit bisnis, dan/atau *subsidiary*. Hubungan antara tujuan ERM, komponen – komponen ERM dan penerapannya di berbagai tingkatan organisasi digambarkan oleh COSO dalam kubus tiga dimensi sebagai berikut :



Sumber *: Applying COSO ERM Framework – www.coso.org*

Faktor – Faktor Kunci Dalam Implementasi ERM

Untuk melaksanakan ERM di suatu organisasi maka ada beberapa faktor kunci, yang merupakan turunan dari kedelapan komponen diatas, yang perlu diperhatikan yaitu :

1. *Design* Organisasi

Sebelum ERM dibentuk maka perlu diketahui terlebih dahulu *design* dari suatu organisasi yang meliputi *Mission & Strategi objectives*. Suatu organisasi yang baik harus memiliki misi yang hendak dicapainya. Setelah misi ditetapkan, maka perlu dipikirkan *strategic objective* yang kemudian diterjemahkan ke dalam bentuk *key business objective* serta *related objectives*.

Contoh :

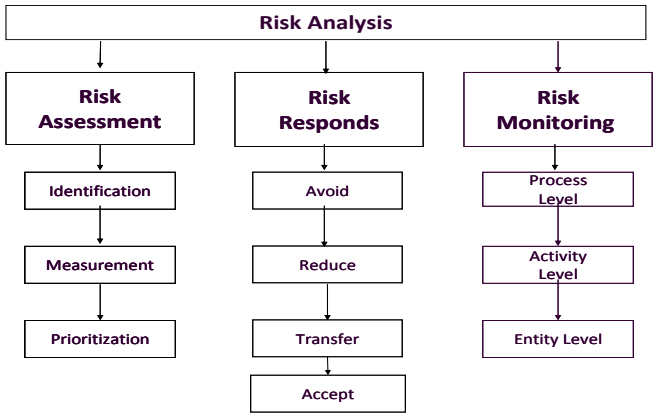
- *Mission* : Menjadi pemain yang patut diperhitungkan dalam industri minyak kelapa sawit di Indonesia.
- *Strategic Objective* : Menjadi Perusahaan No.1 di industri minyak kelapa sawit di Indonesia
- *Key Business Objective* : Selalu memberikan kualitas produk terbaik & dapat memenuhi permintaan pasar.
- *Related Objectives* :
  - Meningkatkan kualitas minyak kelapa sawit dengan batasan yang telah ditetapkan.
  - Memperluas lahan perkebunan kelapa sawit sebanyak X hektar dalam kurun waktu Y tahun
  - Menetapkan target produksi kelapa sawit sebesar Z ton per tahun

2. Menetapkan ERM

Penetapan ERM disini adalah bagaimana filosofi manajemen terhadap risiko, bagaimana budaya risiko ditanam di perusahaan tersebut, nilai – nilai etika dan integritas yang dianut perusahaan dan diperlukan juga struktur organisasi ERM.

3. Melakukan *Risk Analysis*

Yang dimaksud dengan *risk analysis* disini adalah suatu proses mengidentifikasi dan menganalisis risiko – risiko yang berkaitan dengan tujuan perusahaan yang telah ditetapkan. Adapun tahapan – tahapan yang dalam *risk analysis* ini dapat terlihat dari bagan di bawah ini :



A) *Risk Assessment*

1. Mengidentifikasi Risiko (*Identify Risks*)

   Risiko hanya dapat dinilai jika risiko tersebut telah teridentifikasi. Risiko pada dasarnya terbagi menjadi 2 kategori yaitu :

   a. Risiko bawaan (*Inherent Risk*) : risiko yang timbul karena bawaan (*nature*) dari aktivitas bisnis tersebut.

   b. Risiko sisa (*Residual Risk*) : Risiko yang tersisa setelah manajemen melakukan kontrol untuk memitigasi risiko bawaan (*inherent risk*), misalnya dengan membuat *Policy & Procedure.*

   Untuk membantu mengidentifikasi dan melengkapi risiko, maka dapat dibuat kategori – kategori atas risiko (*risk categories*). Model dari *risk categories* ini bermacam – macam dan tergantung dari kebutuhan serta sudut pandang perusahaan., misalnya : risiko strategis, risiko operasional, risiko informasi, risiko keuangan.dan lain – lain. Risiko – risiko yang telah teridentifikasi tersebut kemudian didokumentasikan ke dalam bentuk *Risk Register.*

2. Mengukur Risiko (*Measurement Risks*)

   Risiko – risiko yang telah teridentifikasi tersebut kemudian dilakukan pengukuran dengan menilai seberapa sering kemungkinan terjadinya risiko tersebut (*likelihood*) dan seberapa besar dampak yang diakibatkan dari risiko tersebut (*impact /consequences*). Untuk mengukur *likelihood* dan *impact* dari suatu risiko dapat digunakan pendekatan kuantitatif dan kualitatif.

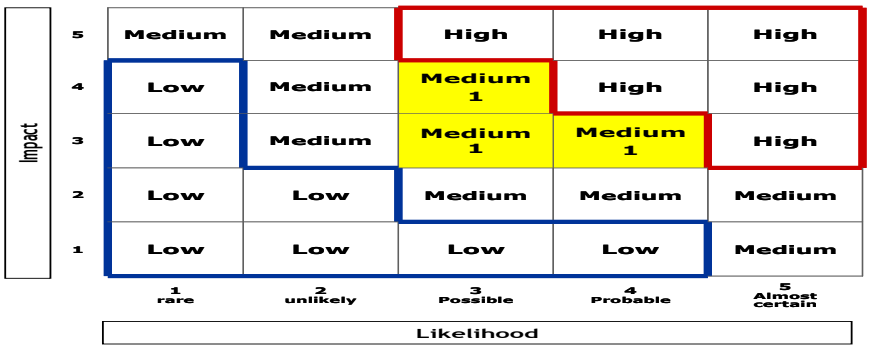
3. Membuat urutan skala prioritas atas risiko (*PrioritizationRisks*)

   Setelah risiko – risiko tersebut dinilai, maka dilakukan proses membandingkan risiko yang telah diukur tersebut (setelah menentukan *likelihood & impact*) dengan kriteria – kriteria risiko untuk dapat menentukan seberapa signifikan risiko tersebut (*high risk, medium risk, or low risk*). Tingkatan *high, medium* dan *low risk* sangat tergantung dari *risk appetite* dari manajemen perusahaan. Berikut ini contoh tabel yang memperlihatkan tingkatan (*level*) dari *likelihood* dan *impact*

Level	Likelihood	Explanation
5	Almost certain	Frequently
4	Probable/Likely	a couple of time
3	Possible	may not occur
2	Unlikely	are not expected to occur
1	Rare	occur only in exceptional circumstances

Level	Impact	Explanation
5	Catastrophic	Damage the whole/significant part of the organization permanently
4	High	Prevent the organization to achieve the majority part of its objectives for a long time
3	Medium	Prevent the organization to achieve some of its objectives for limited period
2	Low	Cause inconvenience, however will not affect the achievement of significant objectives
1	Very Low	Cause minor inconvenience and will not affect the achievement of significant objectives

Berikut ini contoh gambar yang memperlihatkan *Risk Mapping* (pemetaan risiko)



B) Risk Responds

Setelah dilakukan *risk mapping* atas risiko bawaan tersebut maka langkah selanjutnya adalah melakukan tanggapan atas risiko – risiko tersebut. Secara umum ada 4 jenis *risk responds* yaitu :

a. *Avoidance / Terminate* : menghindari /menghilangkan suatu situasi atau kegiatan yang dapat menimbulkan terjadinya risiko tersebut

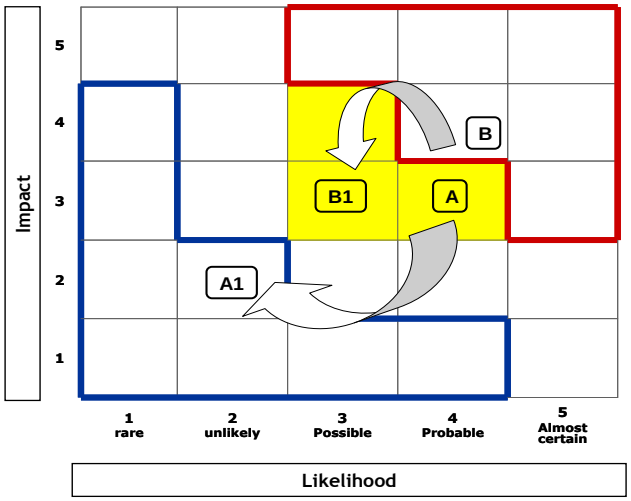
b. *Reduce /Treat*: meminimalkan risiko dengan cara membuat serangkaian aktivitas pengendalian (*Control activities*) misal : membuat *Standard Operating Procedures* (SOP) , melakukan teknologi informasi yang terintegrasi, dan sebagainya. Aktivitas pengendalian ini ada yang bersifat pencegahan (*preventive*), mendeteksi (*detective*) atau memperbaiki (*corrective*)

c. *Transfer* : Memindahkan risiko tersebut ke pihak ketiga lainnya. Misal : manajemen suatu perusahaan rental mobil memutuskan untuk melakukan transfer risiko pencurian, kecelakaan atas mobil – mobil yang disewakannya kepada pihak ketiga yaitu pihak asuransi.

d. *Acceptance* : Menerima risiko tersebut tanpa perlu melakukan tindakan apapun. Hal ini biasanya dilakukan karena nilai dari risiko itu dibawah batas toleransi risiko.

Setelah dilakukan tanggapan atas risiko-risko tersebut maka langkah selanjutnya adalah melakukan penilaian kembali atas risiko yang telah dimitigasi sehingga didapatlah nilai sisa dari risiko (*Residual Risk*). Berikut ini adalah contoh dari *risk register* & *risk mapping*

No	Kategori Risiko	Deskripsi Risiko	Inherent		Risk Response	Jenis kontrol	Deskripsi kontrol	Residual	
			L	I				L	I
A	Risiko Operasional	Barang usang atau sudah *expired date*	4	3	Reduce	Preventive Detective Corrective	-Menerapkan sistem FIFO -Melakukan cek melalui sistem utk mengidentifikasi barang - barang yang akan segera *expired date* dalam 3 bulan ke depan -Atas barang - barang yang akan *expired date* dlm waktu satu bulan ke depan dijual secara diskon	2	2
B	Risiko Operasional	Ketidaktersediaan barang pada saat dibutuhkan *(stockout)*	4	4	Reduce	Preventive Detective Corrective	-Menerapkan analisa persediaan dgn menerapkan Economic Order Quantity (EOQ) -Bagian inventory melakukan pemeriksaan secara mingguan mengenai barang - barang yang akan habis dalam beberapa minggu ke depan -Dalam hal yang sangat mendesak, maka dapat dilakukan pembelian barang *tanpa melalui PO procedure* dgn syarat - syarat yg tertentu	3	3



Keterangan :

Dari gambar tersebut terlihat bahwa terjadi penurunan tingkat risiko dimana untuk:

- Risiko A ke A1 : dari nilai *inherent risk* yang berada di titik *medium1* setelah ditetapkan kontrol maka nilai *risk residual-nya* menjadi turun ke titik *low level.*
- Risiko B ke B1 : dari *inherent risk* yang berada di titik *high risk* setelah ditetapkan kontrol maka nilai *risk residual*-nya menjadi turun ke titik *medium1*.

Setelah risiko – risiko berhasil diidentifikasi dan dianalisa maka hasilnya harus dikomunikasikan ke seluruh pihak sehingga masing – masing pihak memahami peranan mereka dalam ERM. Hasil – hasil dari risiko tersebut dapat diinformasikan & dikomunikasikan misalnya dalam bentuk *risk profile* yang didalamnya berisi risiko – risiko kunci, *responds* yang terkait serta kontrol – kontrol kunci untuk mengendalikan risiko - risiko tersebut.

C) Risk Monitoring

Untuk dapat memastikan proses ERM berjalan efektif maka dibutuhkan pengawasan (*monitoring*) baik di tingkat proses, aktivitas maupun entitas. Pengawasan ini dapat dilakukan melalui kegiatan :

- *On going monitoring*

  Misal : Salah satu faktor kunci tercapainya tujuan dari suatu pelayanan rumah sakit adalah waktu tunggu yang tidak lama. (misal : untuk proses registrasi tidak boleh lebih dari 5 menit). Untuk itu diperlukan suatu alat yang dapat

membantu mengukur waktu tunggu setiap pasien dan dari alat tersebut dapat ditarik data rata – rata waktu tunggu tersebut. Laporan waktu tunggu itu dibuat setiap minggunya sebagai salah satu bentuk dari *ongoing monitoring* atas risiko waktu tunggu yang lama.

- *Separate evaluations*

  Salah satu pihak yang dapat melakukan *separate evaluations* ini adalah internal auditor pada saat melakukan penugasannya. Dimana dari hasil penugasannya tersebut internal auditor dapat :

  - Mengevaluasi apakah kontrol yang telah ditetapkan oleh manajemen itu benar – benar efektif untuk meminimalkan risiko. Internal auditor dapat membantu merekomendasikan kontrol yang sekiranya dapat lebih membantu meminimalkan risiko.
  - Mengevaluasi apakah kontrol yang telah ditetapkan itu benar – benar dijalankan atau tidak. Karena jika tidak dijalankan maka ini akan berdampak terhadap hasil penilaian atas risiko yang telah ditetapkan sebelumnya. Jadi ada kemungkinan nilai *residual risk* yang tadinya berada dalam kategori *"low risk"* ternyata setelah dilakukan internal audit ada kemungkinan menjadi *"high / medium risk"* karena kontrolnya tidak dijalankan.
  - Memberikan masukan adanya risiko – risiko yang belum teridentifikasi sebelumnya.

Peranan Internal Audit dalam ERM

Seiring dengan perubahan – perubahan yang terjadi dalam tata kelola perusahaan , maka *Institute Internal Auditor* (IIA) sebagai institusi professional dunia internal auditor melakukan redefinisi dari internal audit sebagai berikut :

> *"Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, discipline approach to evaluate and improve* ***the effectiveness of risk management****, control, and governance processes"* (Sawyer, et.al.,2003).

Dari redefinisi diatas terlihat jelas bahwa internal auditor berperan dalam memperbaiki/meningkatkan efektivitas dari *risk management.* Selain itu juga peranan internal audit dalam *risk management* juga tertuang dalam beberapa *section* dari *"Standards for the Profesional Practice of Internal Auditing"* yang diterbitkan IIA antara lain di section 2010, dimana Chief Audit Executive (CAE) diberi mandat uuntuk menetapkan perencanaan audit atas dasar risiko (*risk-based plans*) untuk menentukan prioritas perencanaan audit dan section 2110 – dimana kegiatan internal audit harus memonitor dan mengevaluasi keefektifan dari manajemen risiko dan sistem pengendalian. Standar – standar diatas sudah terlebih dahulu ada sebelum diterbitkannya COSO ERM, akan tetapi pada saat itu (sebelum COSO ERM diterbitkan) masih banyak internal auditor yang tidak memberikan perhatian terhadap *risk management* sehingga memunculkan berbagai kasus besar di dunia bisnis. Dengan adanya COSO ERM maka dapat dijadikan sebagai alat yang efektif untuk membantu internal auditor dalam melakukan perencanaan audit berdasarkan risiko (*risk based - plans*). Sehubungan dengan penerbitan COSO ERM, IIA memberikan respon-nya dengan menerbitkan suatu tulisan yang berkaitan dengan peranan internal auditor dalam ERM *"The Role of Internal Auditing in Enterprise-wide Risk Management"*, September 29,2004 sebagai berikut :

1. Memberikan keyakinan pada *design* dan efektivitas proses manajemen risiko
2. Memberikan keyakinan bahwa risiko telah dievaluasi dengan benar
3. Mengevaluasi proses manajemen risiko
4. Mengevaluasi pelaporan mengenai status dari risiko-risiko kunci (*key risks*) dan pengendaliannya.
5. Meninjau pengelolaan risiko – risiko kunci, termasuk efektivitas dari pengendalian dan respons lain terhadap risiko – risiko tersebut.

Peranan Internal Audit yang dapat dilakukan hanya pada tahap awal penerapan manajemen risiko korporasi (bilamana penerapan manajemen risiko sudah berjalan, internal audit tidak boleh melakukan hal-hal berikut) :

1. Memberikan fasilitasi proses identifikasi dan penilaian atas risiko kepada pemilik risiko di organisasi.
2. Memberikan fasilitasi proses pengelolaan risiko kepada pemilik risiko di organisasi
3. Melakukan koordinasi aktivitas ERM
4. Melakukan konsolidasi pelaporan atas risiko
5. Memastikan dan mengembangkan kerangka kerja ERM yang sesuai dengan kebutuhan organisasi.
6. Membangun perintis awal yang akan bertanggung jawab dalam penerapan ERM selanjutnya di organisasi.
7. Mengembangkan strategi pengelolaan risiko di organisasi dan mendapatkan persetujuan Direksi maupun dewan Komisaris atas strategi yang telah dikembangkan

Peranan yang tidak boleh dilakukan oleh Internal Audit (disarankan untuk dilakukan oleh unit manajemen risiko sebagai unit yang independen) :

- Menetapkan batasan dan selera risiko (*risk appetite*)
- Terlibat dalam proses *risk management*
- Melakukan validasi atas risiko yang telah teridentifikasi dan terukur
- Melakukan pengambilan keputusan *risk respond*
- Menerapkan *risk respond* dengan mengatasnamakan manajemen
- Mengambil bentuk pertanggungjawaban atas penerapan manajemen risiko

KESIMPULAN

ERM merupakan sebuah konsep baru yang merupakan perkembangan dari konsep *risk management* tradisional. Dengan adanya konsep ERM ini, maka diharapkan suatu organisasi dapat melihat risiko secara komprehensif, integratif, dan lintas divisional. Selain itu ERM diharapkan dapat membantu perusahaan mengurangi kejutan – kejutan serta kerugiaan yang tidak diharapkan dan melihat peluang – pleuang yang ada sehingga dapat diperoleh pencapaian tujuan perusahaan yang lebih baik dan pada akhirnya menciptakan, menambah, dan atau melindungi nilai perusahaan. Penerapan ERM juga sangat membantu internal auditor dalam

melakukan perencanaan audit (*risk based – plans*) yaitu memilih prioritas – prioritas area yang akan diaudit . ERM hanyalah suatu alat/metode yang keberhasilannya sangat ditentukan oleh peranan pihak yang mendesign kerangka ERM tersebut agar sesuai dengan yang dibutuhkan oleh perusahaan, pihak yang menjalankan proses ERM sesuai dengan koridor yang telah ditetapkan serta pihak independen dan objektif, yaitu internal auditor yang mengawasi dan memberikan penilaian apakah proses ERM telah berjalan dengan efektif. Agar dapat menjalankan fungsinya tersebut secara efektif maka diharapkan internal auditor harus membekali dirinya dengan pemahaman mengenai ERM diantaranya memahami *risk philosphy* perusahaan yang menjadi dasar penetapan *risk appetite* serta strategi mitigasi yang perlu dilakukan terhadap risiko – risiko perusahaan yang berada di luar batas *risk appetite* perusahaan. Selain itu juga internal auditor diharapkan semakin membekali dirinya dengan kemampuan – kemampuan teknis yang lebih luas lagi, jadi tidak hanya memiliki kemampuan di bidang *financial & accounting* saja, tetapi juga di bidang *information & technology* (IT), *management information system* (MIS), dan bidang – bidang lainnya.

DAFTAR PUSTAKA

Alijoyo, Antonius. (2006). *Enterprise Risk Management : Pendekatan Praktis*. Jakarta Ray Indonesia.

Anquillare, Mark (2010). *ERM Helps Manager Cross Barrier Within, Outside Company*. National Underwriter.P&C

Chambers, Andrew and Graham Rand. (2000). *The Operational Auditing Handbook, Auditing Business Process*. Baffins Lance, Chichester : John Willey & Sons, Ltd.

COSO (The Committee of Sponsoring Organizations). (2004). *Applying COSO's ERM – Integrated Framework*. www.coso.org

Crouhy, Michel ; Galai, Dan ; Mark Robert. *Essential of Risk Management*. 2006. New York : McGraw-Hill.

DeLoach, J. W. (2003). *Building Enterprise Risk Management on the Foundation Laid by Sarbanes-Oxley.*

Griffiths, David. (2006). *Risk Based Internal Auditing: Three Views on Implementation*. www.internalaudit.biz

Protiviti. (2006). *Guide to Enterprise Risk Mangement*. Protiviti Inc. www.protiviti.com